Solutions assignment I

Problem 1

Consider the cubic curve $E: \ y^2 = x^3 + ax + b$, where $x^3 + ax + b$ has distinct zeros. The closure of E in the projective plane contains one extra point, which we denote by O, the point at infinity. Without using the Riemann-Roch theorem prove that for every integer $n > 0$ the dimension of $L(nO)$ equals n and display a basis of this space. (Hint: functions in $L(nO)$ are regular on the affine part of E; what are the orders of x, y at O?)
Solution. In class we showed that x has a pole of order two at O and y a pole of order 3. Notice that functions in $L(nO)$ are regular on the affine part of E, hence given by polynomials in x, y. Since $y^2 = x^3 + ax + b$. The space of functions regular on the affine part of E is spanned by x^m ($m = 0, 1, 2, 3, \ldots$) and yx^m ($m = 0, 1, 2, \ldots$). Clearly the pole order of x^m at O is $2m$, an even number, and the pole order of yx^m at O equals $2m + 3$, an odd number. So the pole order of these functions are distinct, hence these functions are linearly independent. A basis for $L(nO)$ is given by $1, x, x^2, \ldots, x^{[n/2]}$ and $y, yx, \ldots, yx^{[(n-3)/2]}$. Hence the dimension of $L(nO)$ equals $[n/2] + 1 + [(n-3)/2] + 1 = n$.

Problem 2

Let C be a smooth projective algebraic curve. A birational isomorphism from C to itself is called an automorphism. The automorphism group of C is denoted by $\mathrm{Aut}(C)$.

1. Suppose the genus of C is 0. Show that $\mathrm{Aut}(C)$ is isomorphic to the group $GL(2, k)$ modulo scalars. (Hint: Notice that C is isomorphic to $\mathbb{P}^1$ and that rational functions on $\mathbb{P}^1$ can be considered as rational maps from $\mathbb{P}^1$ to itself)

2. Suppose the genus of C is 1 and write C in standard Weierstrass form $y^2 = x^3 + ax + b$. Show that if $ab \neq 0$, then $\mathrm{Aut}(C)$ is generated by the translations $P \mapsto P + Q$ with a fixed $Q \in C$ and the involution $(x, y) \mapsto (x, -y)$. (Hint: If s is in $\mathrm{Aut}(C)$, then there exists a translation T so that Ts fixes the point at infinity). Suppose $ab = 0$, write down a set of generators for $\mathrm{Aut}(C)$. In these problems you may only use basic

definitions and the result of problem (1). So no standard theorems on elliptic curves, you are proving one of them.

Solution

1. We determine $\mathrm{Aut}(\mathbb{P}^1)$. Any rational map is of the form $f(t)/g(t)$ with $f, g \in k[t]$. Suppose that $f/g \in \mathrm{Aut}(\mathbb{P}^1)$. Then, with finitely many exceptions, for any $a \in k$ the equation $f(t)/g(t) = a$ has precisely one solution. Hence $f(t) - ag(t) = 0$ has one solution for almost all $a \in k$. We conclude that f, g have degree at most degree 1 and that at least one of them is non-constant. Write $f(t) = at + b, g(t) = ct + d$. Notice that non-constantness of $f(t)/g(t)$ implies $ad - bc \neq 0$. Conversely any rational map $t \mapsto (at + b)/(ct + d)$ has an inverse, namely $(dt-b)/(-ct+a)$. Associate the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the automorphism $(at + b)/(ct + d)$. Then one easily checks that the matrix of composition of two automorphisms equals the product of the matrices of the automorphisms. Hence $\mathrm{Aut}(C)$ and $GL(2, k)/k^*$ are isomorphic.

2. We use the following general remark. Let $f \in k(C)$ and let $\phi \in \mathrm{Aut}(C)$. Then the functions f and $f \circ \phi$ have the same degree, simply because ϕ does nothing than to move around the poles of f.

   According to the hint we can restrict ourselves to an automorphism ϕ that fixes the point O, the point at infinity. Let $\phi(x, y) = (f_1(x) + yf_2(x), g_1(x) + yg_2(x))$. Since O is sent to O the components of ϕ are regular on the affine part of E, hence they are polynomial in x, y. We now apply our remark to the function x. Note that $x\circ\phi$ is $f_1(x)+yf_2(x)$. Since $x \circ \phi$ has degree 2 we conclude that f_1 is of the form $px + q$ with $p, q \in k$ and $f_2 = 0$. Similarly $g_1 + yg_2$ has degree 3 hence $g_2 = r \in k$ and $g_1 = sx + t$ with $s, t \in k$. Furthermore,

   $$(ry + sx + t)^2 = (px + q)^3 + a(px + q) + b,$$

   hence

   $$r^2y^2 + 2(rx + t)y + (rx + t)^2 = (px + q)^3 = a(px + q) = b.$$

   Note that $y^2 = x^3 + ax + b$. By comparison of the coefficients of y on the left and right hand side we conclude that $sx + t \equiv 0$. So we are left with

   $$r^2(x^3 + ax + b) = (px + q)^3 + a(px + q) + b.$$

Comparison of coefficient of x^2 yields $0 = 3p^2q$. As $p \neq 0$ we conclude that $q = 0$. Hence

$$r^2(x^3 + ax + b) = p^3x^3 + apx + b.$$

Comparison of the coefficients now yields

$$r^2 = p^3, \quad ar^2 = ap, \quad r^2b = b.$$

If $ab \neq 0$ the third equation gives $r^2 = 1$, hence $r = \pm 1$ and the second $p = r^2 = 1$. Hence the only non-trivial automorphism is $(x, y) \mapsto (x, -y)$.

When $b = 0$ we have $a \neq 0$, otherwise the curve is singular. From the first and second equation we derive $r^2 = p^3$ and $p = r^2$. Hence $r = i^k, p = i^{2k}$ where $i^2 = -1$ and $k = 0, 1, 2, 3$.

When $a = 0$ we have $b \neq 0$. From the first and third equation we derive $r^2 = p^3, r^2 = 1$. Hence $r = \pm 1$ and $p = \omega^k$ with $k = 0, 1, 2$ and ω is a primitive third root of unity.

Problem 3, Hindry/Silverman A.4.2

Recall that a smooth projective curve C of genus $g \geq 2$ is called hyperelliptic if there exists a double covering $\pi : C \to \mathbb{P}^1$. Let C be a hyperelliptic curve.

1. Show that C has an affine model U given by an equation of the form $y^2 = F(x)$ where $F(x)$ is a polynomial with distinct roots.

2. Let $g = [(\deg(F) - 1)/2]$ and let $F^*(u) = u^{2g+2}F(u^{-1})$. Show that the equation $v^2 = F^*(u)$ also defines a smooth affine model U' of C.

3. More precisely, show that there is an isomorphism $V \to V'$ given by

$$(x, y) \mapsto (u, v) = (x^{-1}, yx^{-g-1})$$

   where $V = \{(x, y) \in U \mid x \neq 0\}$ and $V' = \{(u, v) \in U' \mid u \neq 0\}$. Prove that C is isomorphic to the curve obtained by using this map to glue U and U' together.

4. Let U and U' be as above and define the map

$$\phi : U \to \mathbb{P}^{[\deg(F)/2]+1}, \qquad (x, y) \mapsto (1 : x : \ldots : x^{[\deg(F)/2]} : y).$$

Prove that ϕ is an embedding. Prove that the Zariski-closure of $\phi(U)$ in $\mathbb{P}^{[\deg(F)/2]+1}$ is smooth, hence isomorphic to C.

5. Prove that the map $\pi : C \to \mathbb{P}^1$ is ramified at exactly $2g + 2$ points. Use the Riemann-Hurwitz formula to deduce that C has genus g. If C is given by the affine model $y^2 = F(x)$ with $\pi(x, y) = x$, identify the ramification points.

6. Prove that the set $\{x^j dx/y \mid j = 0, 1, \ldots, g-1\}$ is a basis for the space of regular differential forms on C.

Solution

1. Denote the rational function giving the degree 2 map $\pi : C \to \mathbb{P}^1$ by x. Since x has degree 2, the extension $k(C)/k(x)$ has degree 2. Hence $k(C) = k(x, y)$ where y satisfies a quadratic equation over $k(x)$. By a suitable choice of y we arrive at a quadratic equation of the form $y^2 = G(x)$, where $G \in k[x]$. Write $G(x) = F(x)H(x)^2$, where F is a square-free polynomial. Replace y by $yH(x)$ to obtain $y^2 = F(x)$, an equation of the desired form.

   For a singular point (x_0, y_0) in the affine part the equations $y_0^2 = F(x_0)$, $0 = F_x(x_0)$, $y_0 = 0$ are satsfied. Hence $y_0 = 0$ and $F(x_0) = F_x(x_0) = 0$, i.e. x_0 is double zero of F. The latter is impossible, so we conclude that the affine curve U is smooth.

2. If in the equation $y^2 = F(x)$ we replace x by $1/u$ and y by v/u^{g+1}, then we obtain $v^2 = u^{2g+2}F(1/u) = F^*(u)$, another affine model of C. That this model U' is smooth follows from the fact that F^* has no double zeros. This is because F has no double zeros.

3. One easily checks that the rational function $V \to V'$ is an isomorphism. The functions are regular on V and the inverse function $(u, v) \mapsto (x, y) = (1/u, v/u^{2g+2})$ is regular on V'. Let W the Zariski open subset of C on which x is regular. Then clearly W is isomorphic to U. Let W' be the open subset of C where $u = 1/x$ is regular. Then W' is isomorphic to U'. Notice also that the union of W and W' is all of C

(at any point $P \in C$ either x or $1/x$ is regular) and the intersection $W \cap W'$ is compatible with the gluing of U and U'.

4. This problem is a correction for the wrongly stated question in Hindry/Silverman. However this correction turns out to be harder than I thought when $\deg(F)$ is odd. Instead we consider the embedding

$$\phi : U \to \mathbb{P}^{g+1}, \quad (x, y) \mapsto (1, x, x^2, \ldots, x^{g+1}, y).$$

The solution for the harder problem needs an adaptation when $\deg(F)$ is odd.

Notice that at any point $P = (x_P, y_P) \in U$ either $x - x_P$ is a local parameter (when $y_P \neq 0$) or y is a local parameter (if $y_P = 0$). Since x and y both occur linearly in $(1, x, x^2, \ldots, x^{g+1}, y)$ the image $\phi(U)$ has a well-defined tangent at every point. We extend ϕ to the whole curve C by choosing an extension on U' as follows,

$$\phi : (u, v) \mapsto (u^{g+1}, \ldots, u, 1, v) \sim (1, u^{-1}, \ldots, u^{-g-1}, vu^{-g-1}).$$

The latter equals $(1, x, \ldots, x^{g+2}, y)$ in the original x, y-coordinates. For the same reason as before the image $\phi(U')$ is smooth. Clearly ϕ now defines a birational isomorphism between two smooth curves, hence ϕ is an isomorphism.

5. The map $C \to \mathbb{P}^1$ is a morphism. For any $a \in k$ the equation $y^2 = F(a)$ in y has either two solutions (when $F(a) \neq 0$) or one solution $y = 0$ when $F(a) = 0$. To find $\pi^{-1}(\infty)$ we change to u, v coordinates and we need to solve $v^2 = F^*(0)$ in v. When $F^*(0) = 0$ there is one solution, and two solutions otherwise. Notice that $F^*(0) = 0$ if and only if F has odd degree. The number of ramification points (all of order 2) is thus $\deg(F)$ if $\deg(F)$ is even and $\deg(F) + 1$ if $\deg(F)$ is odd. In all cases the number is $2g + 2$. We now apply Hurwitz formula to $\pi : C \to \mathbb{P}^1$ where g_C is the genus of C:

$$2g_C - 2 = -4 + (2g + 2)(2 - 1).$$

Hence $2g_C - 2 = 2g - 2$ nad we see that $g_C = g$.

6. Notice that any form $x^j dx/y$ is regular on U. This is clear when $y \neq 0$, when $y = 0$ we use $2ydy = F_x dx$ to find $x^j dx/y = 2x^j dy/F_x$. And F_x is nonvanishing in the points with $y = 0$.

For any $0 \leq j < g$ the form $x^j dx/y$ is also regular on U' as can be seen by using the u, v coordinates. We get $x^j dx/y = -u^{g-j-1} du/v$. By the same arguments as above this is regular on U'.

It remains to show that the forms are linarly independent. Choose $a \in k$ such that $F(a) \neq 0$ and $b \in \overline{k}$ such that $b^2 = F(a)$ It suffices to show that $(x-a)^j dx/y$ are linearly independent. Since $x - a$ is a local parameter at the point (a, b) we see that $(x-a)^j dx/y$ has vanishing order precisely j. Hence these forms are k-linear independent.