Exercises for algebraic curves

Christophe Ritzenthaler

February 18, 2019

1 Exercise Lecture 1

1.1 Exercise

Show that $V = \{(x, y) \in \mathbb{C}^2 \text{ s.t. } y = \sin x\}$ is not an algebraic set.

Solutions. Let us assume that V is algebraic and let us consider its intersection with the line $Y = 0$. This is also an algebraic set and consist of infinitely many isolated points. Each point is an irreducible component but one should be able to write $V \cap V((Y))$ as a finite sum: contradiction.

1.2 Exercise

If V is a algebraic set and $P \notin V$ a point, show that there exists a polynomial F such that $F(x) = 0$ for all $x \in V$ and $F(P) = 1$.

Solutions. Consider $I = I(V)$ and $J = I(V \cup \{P\})$. Since $V \circ I$ is injective $J \subsetneq I$. Consider $F_0 \in I \setminus J$. By definition $F_0(x) = 0$ for all $x \in V$ and $F_0(P) \neq 0$. Let $F = F_0/F_0(P)$.

1.3 Exercise

1. Let $F(x, y, z)$ be a homogeneous polynomial of degree d over a field k. Show (Euler relation)

$$x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z} = d \cdot F(x, y, z)$$

   (hint: take partial derivative of $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$ with respect to λ and then $\lambda = 1$).

2. If d is coprime to the characteristic of k, show that the projective set $C : F = 0$ is singular at $P_0 = (x_0 : y_0 : z_0)$ if and only if

$$\left(\frac{\partial F}{\partial x}(P_0), \frac{\partial F}{\partial y}(P_0), \frac{\partial F}{\partial z}(P_0)\right) = (0, 0, 0).$$

3. If P_0 is not singular, an equation of the tangent at P is
$$\frac{\partial F}{\partial x}(P_0)x + \frac{\partial F}{\partial y}(P_0)y + \frac{\partial F}{\partial z}(P_0)z = 0.$$
4. Study the singularities of $C_1/\mathbb{C} : y^2z = x^3$ over $\mathbb{C}$..

Solutions.

1. Derive the composition of $g : \lambda \mapsto (\lambda x, \lambda y, \lambda z)$ with $F : (x, y, z) \mapsto F(x, y, z)$. One has
$$\partial(F \circ g)/\partial\lambda = (\partial F/\partial x, \partial F/\partial y, \partial F/\partial z) \cdot {}^t(\partial\lambda x/\partial\lambda, \partial\lambda x/\partial\lambda, \partial\lambda x/\partial\lambda)$$
which gives the result. The second equality is straitforward.
2. Let choose an affine space containing the point. We can assume that $z_0 \neq 0$. The point is singular if and only if $\partial F(x, y, z)/\partial x = \partial F(x, y, z)/\partial y = 0$ at $(x_0, y_0, 1)$. If it is so, then $\partial F(x, y, z)/\partial z = 0$ since $F(x_0, y_0, z_0) = 0$. Conversely if at a point the three partial derivative are zero, since d is not zero, then F is zero and the point is on the curve.
3. An affine equation of the tangent at $(x_0 : y_0 : 1)$ is
$$y - y_0 = -\frac{\partial F/\partial x}{\partial F/\partial y}(x_0, y_0, 1)(x - x_0).$$
Developing one gets
$$\partial F/\partial x(P_0)x + \partial F/\partial y(P_0)y - (x_0\partial F/\partial x(P_0) + \partial F/\partial y(P_0)y_0) = 0.$$
The last term is $\partial F/\partial z(P_0)$ en after homogenizing one gets the result.
4. The partial derivative are $(-3x^2, 2yz, y^2)$. The point $(0 : 0 : 1)$ is the unique singularity.

1.4 Exercise

Let V be the projective variety defined by $Y^2Z - (X^3 + Z^3) = 0$. Show that the map $\phi : V \to \mathbb{P}^2$ given by $(X : Y : Z) \mapsto (X^2 : XY : Z^2)$ is a morphism.

Solutions. The map is apparently not defined at $P = (0 : 1 : 0)$. But $Z \equiv \frac{X^3}{Y^2 - Z^2} \pmod{I(V)}$. So we get that
$$(X^2 : XY : Z^2) = \left(X^2 : XY : \frac{X^6}{(Y^2 - Z^2)^2}\right) = \left(X : Y : \frac{X^5}{(Y^2 - Z^2)^2}\right)$$
and this last expression evaluate at P is $(0 : 1 : 0)$.

1.5 Exercise

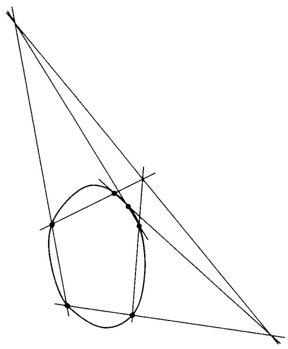
Show the following result:

If two projective plane curves C_1, C_2 of degree n intersect in exactly n^2 points and that there exists a irreducible curve D of degree $m < n$ containing mn of these points, then there exists a curve of degree at most $n - m$ containing the $n(n - m)$ residual points.

To do so, let F_1, F_2, G the equations of C_1, C_2 and D and $p = [a : b : c]$ be a point of D which is not in $C_1 \cap C_2$. Show that there exists a linear combination of F_1 and F_2 containing p. Conclude using Bézout.

One can use this to prove the following corollary (Pascal mystical hexagon): The opposite sides of a hexagon inside an irreducible conic meet in three collinear points.

Figure 1: Pascal mystical hexagon



Solutions. We wish that $\alpha F_1(a, b, c) + \beta F_2(a, b, c) = 0$ which is always possible. Let $R = \alpha P_1 + \beta P_2$. Since p is a point of D different from $C_1 \cap C_2$, R and D intersect in at least $nm + 1$ points. This is possible only if $V(D)$ has a common component with $V(R)$. As D is irreducible we get that $G|R$. Let $U = R/G$. V(U) defines a curve of degree at most $n - m$ and one can check easily that $U(q) = 0$ for all $q \in C_1 \cap C_2$.
Consider for C_1 and C_2 the two curves of degree 3 union of the 3 non-adjacent sides and for $V(D)$the irreducible conic. The 9 intersection points are the 6 points on the conic and the 3 intersection points of the opposite sides. The previous result says that these 3 points are on a curve of degree $3 - 2 = 1$.

2 Exercise Lecture 2

2.1 Exercise

Let $C = V(F) \subset \mathbb{P}^2$ be a dimension 1 affine variety over k. Let $P \in C$ be a smooth point. We are going to show that $\overline{k}[C]_P$ is a discrete valuation ring and that if $L = V(aX + bY + c)$ is any line through P which is not tangent to C at P, then its image in $\overline{k}[C]_P$ is a uniformizer at P

1. Show that by a change of variables we can assume that $P = (0,0)$ that $Y = 0$ is the tangent at P and that $L = V(X)$.
2. Show that $\mathcal{M}_P = (X, Y)$
3. Show that $F = YG - X^2H$ where $G = a +$ higher terms with $a \neq 0$ and $H \in \overline{k}[X]$.
4. Conclude that $\mathcal{M}_P = (X)$.

Solutions.

1. By a translation, we can assume that $P = (0,0)$. Now given two distinct line $aX + bY = 0$ and $cX + dY = 0$ (the tangent), the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible. This change of variables sends the two lines on $X = 0$ and $Y = 0$.
2. By definition $\mathcal{M}_P = \{f \in \overline{k}[X,Y]/F \text{ s.t. } f(P) = 0\}$. In particular $f(P) = 0$ if and only if any representative in $\widetilde{f} \in \overline{k}[X,Y]$ is such that $\widetilde{f}(0,0) = 0$, *i.e.* is in the ideal (X, Y, F). By the correspondence between the ideals of $\overline{k}[X,Y]$ and of $\overline{k}[X,Y]/F$ we see that $\mathcal{M}_P = (X, Y)$.
3. This is equivalent to say that the lowest terms of F is aY which is the case since $Y = 0$ is the tangent.
4. $G(P) \neq 0$ so $G \notin \mathcal{M}_P$ and is therefore invertible. We can write $Y = X^2H/G$ so $\mathcal{M}_P = (X)$.

2.2 Exercise

Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves and $f \in \overline{k}(C_2)^*, P \in C_1$. Prove that

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

Solutions. Locally around $Q = \phi(P)$, we can write $f = ut_Q^{\operatorname{ord}_Q(f)}$ where t_Q is a uniformizer at Q and u is non-zero at Q. So

$$\operatorname{ord}_P(\phi^* f) = \underbrace{\operatorname{ord}_P(\phi^* u)}_{=0} + \operatorname{ord}_Q(f) \cdot \underbrace{\operatorname{ord}_P(\phi^* t_Q)}_{=e_\phi(P)}.$$

2.3 Exercise

We give a proof of residue theorem[1] in the case of $C = \mathbb{P}^1$ over an algebraically closed field k.

1. Consider a rational fraction $P(X)/Q(X)$. Show that one can write P/Q as a sum of terms of the form $c(X-a)^n$ with $c \in k^*, a \in k$ and $n \in \mathbb{Z}$. By linearity, one can restrict to one of these cases.

2. Show for each cases that the formula holds.

Solutions. Using partial fraction decomposition we can decompose P/Q as a polynomial plus a sum of such terms. Now, these expressions are also a basis for polynomials so we can express the polynomial in this basis as well.

A differential $\omega = P/Qdt$ can be decomposed as a sum of $(t-a)^n dt$. At all affine points $P = (b:1)$ we have that $(t-a)^n dt = (t-b+(b-a)^n d(t-b)$. If $b-a \neq 0$ then ω is regular at P and the residue is 0. When $b = a$ and $n = -1$, then the residue is 1. Now at $P = (1:0)$, using that $dt = -t^2 d(1/t)$, we see that $(t-a)^n dt = -t^{n+2}(1-a/t)^n d(1/t)$ which residue is 0 unless $n = -1$ and then the residue is -1. The formula is then proved.

3 Exercise Lecture 3

3.1 Exercise

Prove that a curve C has genus 0 iff there exists two distinct points $P, Q \in C$ such that $(P) \sim (Q)$.

Solutions. Let us assume that C has genus 0. By Riemann-Roch theorem we get that for any $P \in C$, $\ell(P) = 2$ ($\ell(\kappa - P) = 0$ since this is a negative degree divisor). This means that there exists a non-constant function f such that $P + \operatorname{div} f \geq 0$. Since f is non constant, it has a pole and this must be P. As the degree of $\operatorname{div} f$ is zero it has only one zero Q. This means that $P - Q = \operatorname{div} f$ hence $(P) \sim (Q)$. Conversely, if this is the case, then let us consider $\phi : C \to \mathbb{P}^1$ the morphism induced by f and h the function x/z. From previous exercise, we get that

$$1 = \operatorname{ord}_P(f) = e_\phi(P) \cdot \underbrace{\operatorname{ord}_{(0:1)}(x/z)}_{=1},$$

hence $e_{\phi(P)}$ is 1. As P is the only point over $(0:1)$ (since it is the only zero of f), it means that $\deg \phi = 1$ and it is therefore an isomorphism.

[1] For any differential $\omega \in \Omega_C$ $\sum_{P \in C} \operatorname{Res}_P(\omega) = 0$.

3.2 Exercise

Let $\phi : C_1 \to C_2$ a non-constant morphism between curves.

1. Show that $g_{C_1} \geq g_{C_2}$.
2. Prove that if there is equality then $g = 0$ or ($g = 1$ and ϕ is unramified) or ($g \geq 2$ and ϕ is an isomorphism).

Solutions. The first item is a direct consequence of Riemann-Hurwitz theorem since $\deg \phi > 0$ and $\sum e_\phi(P) - 1 \geq 0$. For the second item, we can rewrite letting $g_{C_1} = g_{C_2} = g$

$$(2g-2)(1-\deg \phi) \geq \sum e_\phi(P) - 1 \geq 0.$$

If $2g - 2 > 0$ *i.e.* $g > 1$ then this is possible only if $\deg \phi = 1$ *i.e.* ϕ is an isomorphism. If $g = 1$ then we get that $\sum e_\phi(P) - 1 \geq 0$ hence $e_\phi(P) = 1$ for all P. The morphism ϕ is unramified.

3.3 Exercise

Let k be an algebraically closed field. Let C be a curve of genus $g_C > 1$ and G be the group of automorphisms of C. It is known that this is always a finite group. In the first part of this exercise, we are going to prove this result when C is hyperelliptic and the characteristic of k is different from 2.

We write $C : Y^2 = f(X)$ where f is of degree $2g_C + 2$ (a singular model for C). Recall that isomorphisms of hyperelliptic curves are of the form

$$g : (X,Y) \mapsto \left(\frac{aX+b}{cX+d}, \frac{eY}{(cX+d)^{g+1}}\right)$$

with $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$ and $e \in k^*$. We denote $\widetilde{g}$ the induces automorphism of $\mathbb{P}^1$ given by $(X : Z) \mapsto (aX + bZ : cX + dZ)$ and we therefore have a surjective morphism from G to $\widetilde{G} = \{\widetilde{g},\ g \in G\}$.

1. Show that the kernel of this morphism is generated by the hyperelliptic involution ι.

Hence in order to prove that G is finite, it is enough to prove that $\widetilde{G}$ is. Let $\widetilde{g} \in \widetilde{G}$.

2. Show that the $2g+2$ points $(x_i, 0) \in C$ where x_i are the roots of f are the fixed points of ι.
3. Show that $\widetilde{g}$ permutes the points $Q_i = (x_i : 1)$.
4. Show that an automorphism of $\mathbb{P}^1$ which fixes 3 distinct points is the identity.

5. Conclude that there exists an injective morphism from $\widetilde{G}$ into Sym_{2g+2} and that $\#G \leq 2(2g+2)!$.

6. Describe briefly how to compute the elements of G given a factorization of f.

We now come back to the case where C is not necessarily hyperelliptic and we assume that G is finite. We assume also that the characteristic of k does not divide $\#G = n$.

We know that there exists a curve D/k and a morphism $\phi : C \to D$ separable of degree n such that for all $Q \in D$, $\phi^{-1}(Q) = \{g(P),\ g \in G\}$, where $P \in C$ is any point such that $\phi(P) = Q$ (the curve D is the "quotient" of C by G and in particular $\phi \circ g = \phi$ for all $g \in G$). Let $P \in C$ be a point with ramification index $e_\phi(P) = r$.

7. Show that $\phi^{-1}(\phi(P))$ consists of exactly n/r points, each of ramification index r.

Let $P_1, \ldots, P_s$ be a maximal set of ramification points of C lying over distinct points of D and let $e_\phi(P_i) = r_i$.

8. Show that Riemann-Hurwitz formula implies
$$\frac{2g_C - 2}{n} = 2g_D - 2 + \sum_{i=1}^{s} 1 - \frac{1}{r_i}.$$

9. As $g_C \geq 2$, then the left side is > 0. Show that if $g_D \geq 0$, $s \geq 0$, $r_i \geq 0$ are integers such that
$$2g_D - 2 + \sum_{i=1}^{s} 1 - \frac{1}{r_i} > 0$$
then the minimal value of this expression is $1/42$.

10. Conclude that $n \leq 84(g_C - 1)$.

Solutions.

1. Clearly ι is in the kernel as it is the identity on the x-coordinate. Conversely a map which is the identity on the x-coordinate is of the form $(x, y) \mapsto (x, ey)$. if we want to preserve C, we see that $e^2 = 1$ so this is the hyperelliptic involution.

2. The hyperelliptic involution is given by $(x, y) \mapsto (x, -y)$ hence the points such that $y = 0$ are fixed. Then these are the zeros of f. Note that as the degree of f is even the points at infinity are not fixed by the involution.

3. Recall that an automorphism g commutes with the hyperelliptic involution ι. Hence if P is a fixed point of ι then $g\iota(P) = g(P) = \iota g(P)$ so $g(P)$ is a fixed point as well. This implies that $\widetilde{g}$ permutes the points Q_i.

4. We know that an automorphism $(x : z) \mapsto (ax + bz : cx + dz)$ of $\mathbb{P}^1$ maps three points on any three points, so we can assume that these three points are $0, 1\infty$. The first condition impose $b = 0$, the last one $d = 0$ and the second one $a = c$ not equal to 0 so this is the identity.

5. We have an action of any element of $\widetilde{G}$ on the points Q_i. This action is faithful since there are more than 3 Q_i. So the maps of $\widetilde{G}$ into Sym_{2g+2} is injective.

6. We fix a choice of 3 roots of f and we consider the automorphism of $\mathbb{P}^1$ which sends them to any three other roots of f. We then check that this automorphism maps also the remaining roots on other roots. If this is the case we see that $(cx + d)^{2g+2} f((ax + b)/(cx + d)) = \alpha \cdot f$ and we let $e = \sqrt{\alpha}$. We then get a list of all automorphisms in this way.

7. Let P and P' be two points in the fiber. There exists $g \in G$ such that $g(P) = P'$. Since g is of degree 1 and so nowhere ramified $\operatorname{ord}_{g(P)} g^{-1*} t_P = \operatorname{ord}_P t_P = 1$ so $g^{-1*} t_P = v t_{g(P)}$ where v is non zero at $g(P)$. Now by definition $\phi^* t_{\phi(P)} = u t_P^{e_\phi(P)}$ so since $\phi g = \phi$,

$$\phi^* t_{\phi(P)} = g^{-1*} \phi^* t_{\phi(P)} = g^{-1*} u g^{-1*} t_P^{e_\phi(P)} = (g^{-1*} uv) t_{g(P)}^{e_\phi(P)}.$$

But $\phi^* t_{\phi(P)} = w t_{g(P)}^{e_\phi(g(P))}$ so we get that $e_\phi(P') = e_\phi(P)$. Using Proposition 3.2.1 allows to conclude that there are n/r such points in the fiber.

8. Riemann-Hurwitz formula says that $2g_C - 2 = n(2g_D - 2) + \sum_Q e_\phi(P) - 1$. The last sum can be group into fibers with index of ramification r_i which appears n/r_i times so we get $2g_C - 2 = n(2g_D - 2) + \sum_{i=1}^{s} \frac{n}{r_i}(r_i - 1)$. Dividing by n gets the result.

9. Clearly if $g_D \geq 2$ then the sum is greater than $2 > 1/42$. If $g_D = 1$ since the sum is strictly positive, one of the $r_i > 1$ so at least 2 and the sum is greater than $1/2 > 1/42$. So we can assume that $g_D = 0$ so $s - 2 > \sum 1/r_i$ and therefore $s > 2$. As soon as $s \geq 5$ then the sum is greater than $1/2$. So let us look at the cases $s = 3$ and $s = 4$. For $s = 4$, we have $2 - \sum 1/r_i$ which we want to be as small as possible, so this gives (by a greedy algorithm we start with r_i as small as possible and increases keeping the condition of positivity),

$2 - 1/2 - 1/2 - 1/2 - 1/3 = 1/6 > 1/42$. In the case $s = 3$, we have $1 - 1/2 - 1/3 - 1/7 = 1/42$.

10. We have seen that in all cases in the minimum is $1/42$, so $2g_C - 2 \geq n/42$ hence $n \leq 84(g_C - 1)$.