Lecture 08

Jose Capco (jcapco@risc.jku.at)

C_f in the first example of Example 2 of the last lecture is an *elliptic curve*. This is defined more generally (which would include fields of any characeristics).

In its full generality an elliptic curve is a just a smooth plane curve in $\mathbb{P}^2$ with a K-rational point. But we will have a standard form for the equation of the curve. We will express this form and define the curve after the following motivational Theorem.

Theorem 1. Let C be a smooth cubic curve in $\mathbb{P}^2(K)$ and suppose that C has a non-flex K-rational point (i.e. a point P such that the tangent line at that point meets C at another point). By change of coordinates, C defined by say an equation

$$b_0x^3 + b_1x^2y + b_2x^2z + b_3xy^2 + b_4xyz + b_5xz^2 + b_6y^3 + b_7y^2z + b_8yz^2 + b_9z^3 = 0$$

can be brought to a smooth cubic affine plane curve (in the affine chart $z \neq 0$) defined by equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and if $\operatorname{char} K \nmid 6$ then it can be further brought to a smooth affine curve defined by equation of the form

$$y^2 = x^3 + ax + b$$

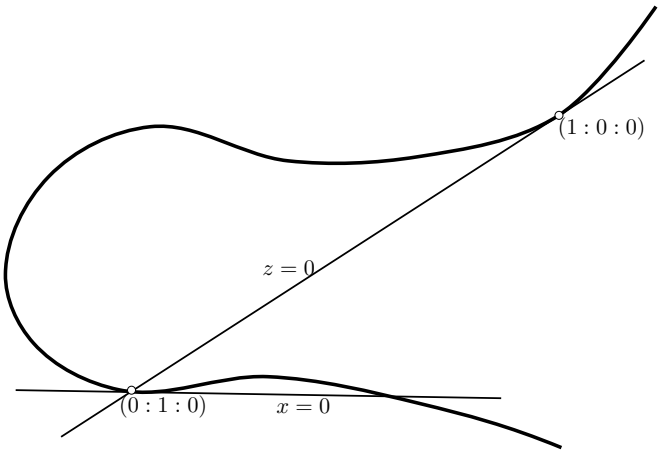

Figure 1: idea of the proof in theorem: bring point P to $(1 : 0 : 0)$, it's tangent to $z = 0$, the second intersection point of $z = 0$ to $(0 : 1 : 0)$ and the tangent of $(0 : 1 : 0)$ to $x = 0$.

Proof. Assume that $(p_x : p_y : p_z) \in C$ and without loss of generality let $p_x \neq 0$. Then ...

Step 1.) We bring this point to $(1 : 0 : 0)$ by applying the following $\mathbb{P}^2$-automorphism

$$\phi_1 : \begin{cases} x' &= x \\ y' &= p_xy - p_yx \\ z' &= p_xz - p_zx \end{cases}$$

renaming x', y', z' to x, y, z yields the defining equation of the new curve

$$c_1x^2y + c_2x^2z + c_3xy^2 + c_4xyz + c_5xz^2 + c_6y^3 + c_7y^2z + c_8yz^2 + c_9z^3 = 0$$

The coefficient of x^3 is 0 because $(1 : 0 : 0)$ is a point of this curve. We work with this new curve.

Step 2.) We notice that $c_2z + c_1y = 0$ is the tangent line of the curve at $(1:0:0)$[1]. We want to keep the point $(1:0:0)$ but move it's tangent line to $z = 0$, so we make a transformation ϕ_2 (almost similar to rotating the curve about $(1:0:0)$) so that the tangent line becomes $z = 0$, this is an affine transformation, so it is a $\mathbb{P}^2$-automorphism i.e.

$$\text{if } c_2 \neq 0 \ \phi_2 : \begin{cases} x' &= x \\ y' &= y \\ z' &= c_2z + c_1y \end{cases} \qquad \text{if } c_2 = 0 \ \phi_2 : \begin{cases} x' &= x \\ y' &= z \\ z' &= y \end{cases}$$

after renaming x', y', z' to x, y, z this will yield the new curve defined by

$$d_2x^2z + d_3xy^2 + d_4xyz + d_5xz^2 + d_6y^3 + d_7y^2z + d_8yz^2 + d_9z^3 = 0$$

Notice that the coefficient of x^2y is 0 because the tangent line of $(1:0:0)$ should now be $z = 0$. We work with this new curve

Step 3.) There will be another intersection of the curve with the line $z = 0$, we can check that this is the point $(-d_6 : d_3 : 0)$ and so $d_3 \neq 0$. We apply another transformation ($\mathbb{P}^2$-automorphism) to move this point to $(0:1:0)$ while keeping the point $(1:0:0)$ and its tangent line $z = 0$ namely

$$\phi_3 : \begin{cases} x' &= d_3x + d_6y \\ y' &= y \\ z' &= z \end{cases}$$

The new curve will then be defined by a function of the form (after renaming x', y', z')

$$e_2x^2z + e_3xy^2 + e_4xyz + e_5xz^2 + e_7y^2z + e_8yz^2 + e_9z^3 = 0$$

Notice that the coefficient of y^3 is 0 because $(0:1:0)$ is now a point on the curve.

Step 4.) Now we want to transform the curve (by a $\mathbb{P}^2$-automorphism) by fixing $(1:0:0), (0:1:0)$ and the tangent line $z = 0$ of $(0:0:1)$ so that the tangent line at $(0:1:0)$ is moved to the line $x = 0$. Notice that the tangent line at $(0:1:0)$ is $e_3x + e_7z = 0$, we achieve the above by applying the following $\mathbb{P}^2$-automorphism

$$\phi_4 : \begin{cases} x' &= e_3x + e_7z \\ y' &= y \\ z' &= z \end{cases}$$

we get, after renaming, a smooth projective cubic curve defined by

$$f_2x^2z + f_3xy^2 + f_4xyz + f_5xz^2 + f_8yz^2 + f_9z^3 = 0$$

Notice that the coefficient of y^2z is 0, because $x = 0$ is the tangent line at $(0:1:0)$, furthermore $f_2 \neq 0$ because $z = 0$ is the tangent line at $(1:0:0)$ and $f_3 \neq 0$ because $x = 0$ is the tangent at $(0:1:0)$

Step 5.) Observe $z = 0$ meets this curve at only two points namely $(0:1:0)$ and $(1:0:0)$, after dividing by f_3, the curve is defined by the following equation

$$xy^2 + g_0xyz + g_1yz^2 = g_2x^2z + g_3xz^2 + g_4z^3$$

[1] we can just look at the function g, defining the curve at the affine chart $(1 : y : z)$, the tangent line is $\frac{\partial f(0,0)}{\partial y}y + \frac{\partial f(0,0)}{\partial z}z$

If we multiply the above equation by x, we get a new equation

$$x^2y^2 + g_0x^2yz + g_1xyz^2 = g_2x^3z + g_3x^2z^2 + g_4xz^3$$

which the union of our original smooth cubic curve above and the line $x = 0$. There is a birational map[2] in a sense that there is a $\phi_5 : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ defined by $\phi_5(x : y : z) = (xz : xy : z^2)$ (where it is defined). Point of indeterminacy for this map is $(0 : 1 : 0)$ and $(1 : 0 : 0)$. This 'map' collapses the *exceptional line* $x = 0$, except at $(0 : 1 : 0)$, to the point $(0 : 0 : 1)$. So the irreducible components $x = 0$ collapses to a point that belongs to our new affine curve (after multiplying by z^2) defined by

$$y'^2z' + g_0x'y'z' + g_1y'z'^2 = g_2x'^3 + g_3x'^2z' + g_4x'z'^2$$

The inverse of ϕ_5 is a rational map defined by $\phi_5^{-1}(x', y', z') = (x'^2 : y'z' : x'z')$ and its points of indeterminacy are $(0 : 1 : 0)$ and $(0 : 0 : 1)$ and exceptional line $z' = 0$. But being able to define ϕ_5 in an open set suffices as there is a Theorem in algebraic geometry that states that a birational map from a curve to another projective curve is actually an isomorphism of curves. After renaming, scaling and translating x we can work on only one affine chart U_z, because we only have one point outside U_z, in this chart we have a smooth curve defined by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

It is not really clear how the labelling $a_1, \ldots, a_6$ came about, but we will provide a possible explanation later. The above curve will now have only one point outside the chart $z \neq 0$, namely $(0 : 1 : 0)$.

Step 6.) Assume now that $\operatorname{char} K \neq 2$, we can get rid of the xy monomial by completing the square with y^2, i.e. we apply the $\mathbb{P}^2$-automorphism

$$\phi_6 : \begin{cases} x' &= x \\ y' &= y + (a_1x + a_3)/2 \end{cases}$$

After renaming variables, the new affine curve is now

$$y^2 = x^3 + h_1x^2 + h_2x + h_3$$

In literature, for field of characteristic 3, this is often written as

$$y^2 = x^3 + ax^2 + bx + c$$

Step 7.) Assuming furthermore that $\operatorname{char} K \neq 3$, we can complete the cube for x and get rid of the monomial with x^2, i.e. we apply the transformation

$$\phi_7 : \begin{cases} x' &= x + h_1/3 \\ y' &= y \end{cases}$$

and by renaming we obtain the desired result

$$y^2 = x^3 + ax + b$$

This curve will be smooth and will have only one points outside the affine chart $z \neq 0$, namely the point $(0 : 1 : 0)$.

□

[2] they are maps defined from a (Zariski) open set of $\mathbb{P}^2$ to $\mathbb{P}^2$ by some polynomials (rational map), which have an inverse rational map (so also defined in an open set of $\mathbb{P}^2$). Points where they are not defined are called *loci of indeterminacy*

Now we can define an elliptic curve

Definition. An elliptic curve is a smooth affine plane curve $C \in \mathbb{P}^2(K)$ either defined by a dehomogenized equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

called the *long Weierstrass form*, or by (if $\operatorname{char} K \neq 2$)

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0$$

called the *short Weierstrass form*. As shown in previous example, the inequality above just tells us that the curve is smooth. Since in both case above there is only one point in U_z (namely the point $(0 : 1 : 0)$ we can define an elliptic curve as an affine curve defined by one of the above equations with a point at infinity $O := (0 : 1 : 0)$.

Remark 2.

- When we reached the Weierstrass long form in the above theorem, we artifially introduced the constant a_6. From our starting point (non-flex point) this was not necessary. But one can also show that we can similarly achieve the Weierstrass long form starting from a flex. The procedure are is a bit easier, but in this case one in fact reaches a form for which we do not know if a_6 is 0. Thus we introduced a_6 to be consistent with the other construction. In fact it suffices to have a K-rational point, i.e. a smooth elliptic curve is just a cubic smooth plane curve defined by a polynomial over K that has a K-rational point. There is a technical non-issue in the proof of the Theorem that will be explained in the next lecture i.e. we inadvertently assume that $(0 : 1 : 0)$ before ϕ_5 is a non-flex point. If it is a flex point, then there is a simpler way to attain Weierstrass long form (not discussed!).
- We have seen in the last Theorem that an elliptic curve C is just a special smooth cubic curve whose defining equation, by some change of variables, is brought to a Weierstrass form. In practice, we would always want C to have K-rational points. It could happen that a smooth cubic curve defined by an equation in $f \in K[x, y]$ will not have a K-rational points, a famous example is a curve studied by Selmer in his PhD thesis (1950's): If $f(x, y) = 3x^3 + 4y^3 + 5z^3$, then $C_f(\mathbb{Q})$ is empty! For our definition of an elliptic curve we always have a K-rational point, namely O.
- There are some other forms of elliptic curves that are beneficial in proving some things. For instance we can regard an elliptic curve as a cubic curve given by an equation of the form

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

  or

  $$y^2 = x(x - e_1)(x - e_3)$$

  for distinct e_i's. Recall that from the exercises in the last session we know that the above curve is smooth for charactersitic not dividing 6 and the above also has only one point outside U_z namely $(0 : 1 : 0)$

We inadvertently used some basic concepts in intersection theory in the statement and proof of the last theorem (for instance we talked about flex point of a cubic curve). It is best, when defining group structure of elliptic curves, if we have a little bit exposure in this area. We are only interested in intersection of a line and a curve so we define these as follows

Definition. Let $P = (0, 0)$ and $f \in K[x, y]\backslash K$ such that $f(P) = 0$ and consider a line $L \subset \mathbb{A}^2$ passing P defined by an equation $l(x, y) = ax + by$. The intersection of C_f and L is solved by paramaterezing L in one variable t and finding the solution of $f(x(t), y(t)) \in K[t]$. The *intersection multiplicity/number* of the line L and C_f at point P is the order of t in $f(x(t), y(t))$. This is denoted by $I(P, L \cap C_f)$ or sometimes $I(P, l \cap f)$. We can generalize this to any point P by translating the curve and the line such that after the translation P is $(0, 0)$.

We expect that if the line is tangent to C_f then $I(P, f \cap l) \geq 2$ and if the line intersects the curve at P transversely then $I(P, f \cap l) = 1$. The above definition generalizes to any point P in the projective plain that is in the intersection of a projective plane curve $C_F \subset \mathbb{P}^2$ and a line L, we can just view this in an affine chart where P lives and use the above definition.

Example 3. Let $f(x, y) = y^2 - (x^3 + x)$ and $P = (0, 0)$

- Consider $l(x, y) = 3x + 4y$ we compute the intersection multiplicity

$$I(P, l \cap f) = \text{ord}_x(f(x, -3x/4)) = \text{ord}_x((-3x/4)^3 - (x^3 + x)) = 1$$

- Consider $l(x, y) = x$ then

$$I(P, l \cap f) = \text{ord}_y(f(0, y)) = 2$$

  the line l is tangent to f

- Consider $l(x, y) = y$ then

$$I(P, l \cap f) = \text{ord}_x(f(x, 0)) = 1$$

- Let F be the homogenization of f to $K[x, y, z]$ so $F = y^2z - (x^3 + xz^2)$. Let $Q = (0 : 1 : 0)$ and $l(x, y, z) = x - z$. Then $Q \in C_l \cap C_F$ and Q lives in the affine chart U_y. So we dehomogenize F and l in $K[x, z]$ to get $g(x, z) = z - (x^3 + xz^2)$. Now we can compute the intersection multiplicity

$$I(Q, l \cap F) = I(Q, l \cap g) = \text{ord}_x(g(x, x)) = 1$$

From the above we have Bézout theorem for lines and curves on the plane

Remark 4. For any line L and a curve C_F in the projective plane we have

$$\sum_{P \in C(\bar{K}) \cap L(\bar{K})} I(P, L \cap C_f) = \deg f$$

In particular, if C is a cubic curve and L is a line tangent to a point P of the curve then there at most one more other point $\neq P$ where L meets C.

We will usually use the letter E for an elliptic curve

Exercise 1. Given an elliptic curve E, show that O is a flex point i.e. if E is regarded as a projective plane curve and L is the tangent line at O then $I(O, E \cap L) = 3$.