GROUP LAW ON THE SMOOTH PART OF A SINGULAR CUBIC CURVE
16/5/2010 - Topics in arithmetic geometry
Davide Calliari

In the following, we will analyse the group structure that we can put on the set of the smooth points of a singular cubic curve. We start defining the group law that we can put on this set.

0.1 The group structure on $C_{sm}(K)$

Let C an irreducible plane cubic curve, defined over a field K (this means that C is defined by an irreducible polynomial of degree three in three homogenous variables and with coefficient in K).

Our cubic C, if it is singular, has exactly one singular point over $\bar{K}$ (from Bezout's theorem). Denote with $C_{sm}(K)$ the set of all the smooth K-points of C, and suppose that this set is not empty.

Definition 1. *For any two points $p, q \in C_{sm}(K)$, we define the following* composition law*: $p \circ q$ is the point obtained intersecting $C_{sm}(K)$ with the K-line that passes through p and q (the tangent line if $p = q$).*

This point $p \circ q$ is uniquely determined by p and q and cannot be singular (from Bezout theorem). Furthermore, the following properties of $\circ$ are straightforward: $p \circ q = q \circ p$ and $p \circ (p \circ q) = q$ for any $p, q \in C_{sm}(K)$.

Definition 2. *Fix now a K-rational point O in $C_{sm}(K)$. Define the* abelian group law *on $C_{sm}(K)$ in this way:*

$$p + q \coloneqq O \circ (p \circ q)$$

for any $p, q \in C_{sm}(K)$.

Proof. We will prove now that the previous definition satisfies the axioms of an abelian group law. Suppose $p, q, s \in C_{sm}(K)$.

- The commutativity holds:

$$p + q = O \circ (p \circ q) = O \circ (q \circ p) = q + p$$

- The neutral element is O:

$$p + O = O + p = O \circ (O \circ p) = p$$

- The inverse of p is defined by $-p \coloneqq (O \circ O) \circ p$:

$$p + (-p) = O \circ (p \circ (p \circ (O \circ O))) = O \circ (O \circ O) = O$$

- The associativity holds: this is the most hardest point. We start observing that, for $p, q, s \in C_{sm}(K)$, saying that $s = p + q$ (i.e. $s = O \circ (p \circ q)$) is the same as saying that there are two K-lines l and t, such that l passes through $p, q, p \circ q$, and t passes through $O, p \circ q, s$. If $l(x), t(x)$ are the respective linear forms over $C_{sm}(K)$, then $l(x)$ has zeroes in $p, q, p \circ q$, while $t(x)$ has zeroes in $O, p \circ q, s$. This means that there exists a rational function over $C_{sm}(K)$, defined by $g(x) := \frac{l(x)}{t(x)}$, that has two zeroes in p and q and that has two poles in s and O. In terms of the divisors over $C_{sm}(K)$, we have that

  $$(p) + (q) \approx (s) + (O)$$

  (recall that the set of the divisors $Div(C_{sm}(K))$ is the free abelian group generetad by formal sums $\sum_{p \in C_{sm}(K)} n_p(p)$, where $n_p \in \mathbb{Z}$; for D_1, D_2 divisors on $C_{sm}(K)$, $D_1 \approx D_2$ if and only if there is a rational function over $C_{sm}(K)$ with associated divisor $D_1 - D_2$).

  Now saying that $(p + q) + r = s$ is then equivalent in the language of divisors to $(p + q) + (r) \approx (s) + (O)$ and $(p) + (q) \approx (p + q) + (O)$, and so it is also equivalent to

  $$(p) + (q) + (r) \approx (s) + 2(O)$$

  We have the same result for $p + (q + r) = s$. This proves the associativity.

□

0.2 Singular cubic curve with K-rational singular point

Consider now an irreducible cubic curve in the Weierstrass model

$$C : zy^2 + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $a_i \in K$. Take $O := [0 : 1 : 0]$, the neutral element of our group law on $C_{sm}(K)$. Suppose that C is singular and that the (unique) singular point is defined over K. It is easy to show that this point can never be O. Because the singular point has coordinates in K, we can move it in the origin of our plane, namely in $[0 : 0 : 1]$. We get the following equation for C:

$$zy^2 + bxyz + cx^2z = x^3$$

with $b := a_1, c := -a_2$.

The group structure varies with the kind of tangents that the singular point has. Here we can define the tangent complex at the singular point $p = [p_1, p_2, p_3]$ by $\sum_{i=1}^{3} p_i \frac{\partial f}{\partial x_i}(x_1, x_2, x_3) = 0$, where f is the equation of our cubic curve.

In our case then, the tangent complex at the singular point $[0 : 0 : 1]$ satisfies the equation

$$y^2 + bxy + cx^2 = 0$$

It's not hard to see that, if we define s_1, s_2 as the two roots in $\bar{K}$ of the polynomial $t^2 + bx + c$, we have $y^2 + bxy + cx^2 = (y - s_1x)(y - s_2x)$, . Hence the splitting behaviour into lines of $y^2 + bxy + cx^2 = 0$ over K, depends exactly on what kind of roots $t^2 + bx + c$ has. Precisely the following cases can happen:

Definition 3. *1. C is of* nodal type*: $t^2 + at + b$ has two distinct solutions in K, the complex tangent consists of two distinct lines defined over K.*

2. *C is of* cuspidal type*: $t^2 + at + b$ has one double root in K, the complex tangent consists of one double line defined over K.*

3. *C is of* twisted type*: $t^2 + at + b$ is irreducible over K. In particular:*

   3a) *C is of* twisted nodal type*: $t^2 + at + b$ has two distinct solutions in some quadratic extension of K but not in K. This means that the tangent complex consists of two distinct lines that are defined in some quadratic extension of K, but not in K.*

   3b) *C is of* twisted cuspidal type*: $t^2 + at + b$ has one double solution in some quadratic extension of K but not in K. This means that the tangent complex consists of a double line that are defined in some quadratic extension of K, but not in K. This case can only happen in characteristic 2 (and furthermore the field has not to be perfect, in particular not finite).*

Observation 1. *We will now specify some facts concerning what can happen in the definition above.*

- *If* $\mathrm{char}(K) \neq 2$*, we can obtain the solutions of $t^2 + at + b$ (in some quadratic extension of K) using the resolutive formula for quadratic equations:*

$$t_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

  If we have a double root, then it has to be $t = -\frac{b}{2}$, and so it must live in K. This implies that in characteristic different from 2 the twisted cuspidal case cannot happen.

- *If* $\mathrm{char}(K) = 2$*, the polynomial $t^2 + at + b$ has two distinct roots (in its splitting field over K) if and only if $a \neq 0$.*

  Indeed, let $\bar{t}$ a root of $t^2 + at + b$. Then $\bar{t} + a$ is the other solution of the polynomial:

$$(t + \bar{t})(t + \bar{t} + a) = (t + \bar{t})^2 + a(t + \bar{t}) = t^2 + \bar{t}^2 + at + a\bar{t} = t^2 + at + b$$

  The two solutions are distinct if and only if $a \neq 0$. Furthermore, they belongs to the same quadratic extension of K.

We will now state the main result of this section.

Theorem 1. *Let C an irreducible singular cubic curve, defined over a field K. Assume that the singular point of C is defined over K.*

1. *If C is of nodal type, $C_{sm}(K)$ is isomorphic to $K^\times$.*

2. *If C is of cuspidal type, $C_{sm}(K)$ is isomorphic to K^+.*

3. *If C is of twisted nodal type, $C_{sm}(K)$ is isomorphic to the elements of norm 1 of some quadratic extension of K (subgroup of the multiplicative group of that extension).*

4. *If C is of twisted cuspidal type (that implies* $\mathrm{char}(K) = 2$*), $C_{sm}(K)$ is isomorphic to* $\{(\alpha, \beta) \in K^2 : \alpha^2 = \beta + b\beta^2\}$.

Proof. We start from a cubic curve C of equation $x^3 = (y^2 + axy + bx^2)z$: it has the singular point in the origin $[0 : 0 : 1]$, and also only the point $O = [0 : 1 : 0]$ lies on the line at infinity $z = 0$ (observe that this O is a flex point: $O = O \circ O$, because $z = 0$ is its tangent).

First, we define the following map:

$$\begin{array}{rcl} \mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\} & \longrightarrow & C_{sm}(K) \\ [\lambda : m] & \longmapsto & [(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m :\ \lambda^3] \end{array}$$

This correspondence is obtained intersecting the smooth points $C_{sm}(K)$ of our cubic curve, with the pencil of projective lines over K through the singular point, namely the lines $\lambda y = mx$, with $\lambda, m \in K$ not both zero. Each line (except the K-rational tangents at the singular points) determines exactly one point on $C_{sm}(K)$, using Bezout's theorem. We obtain then the above correspondence between the set of projective lines through the origin (written as points of a $\mathbb{P}^1(K)$), with the smooth points of the cubic.

By this observation, it is then clear that the inverse of this map has to be:

$$\begin{array}{rcl} C_{sm}(K) & \longrightarrow & \mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\} \\ [x : y : z] & \longmapsto & [x : y] \end{array}$$

We will now formally show that the two maps are bijections, one the inverse of the other. Indeed,

$$[x : y : z] \longmapsto [x : y] \longmapsto \left[(y^2 + axy + bx^2)x :\ (y^2 + axy + bx^2)y :\ x^3\right] =$$

$$= \left[(y^2 + axy + bx^2)x :\ (y^2 + axy + bx^2)y :\ (y^2 + axy + bx^2)z\right] = [x : y : z]$$

and

$$[\lambda : m] \longmapsto \left[(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m :\ \lambda^3\right] \longmapsto$$

$$\longmapsto \left[(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m\right] = [\lambda : m]$$

We have obtained a well defined bijection from $C_{sm}(K)$ to $\mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}$.

Observation 2. *In the particular case of $K = \mathbb{F}_q$ finite field, from this map, we directly obtain the number of K-rational smooth points of our singular cubic curve:*

- *if C is of nodal type, we get*

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 2 = q - 1$$

- *if C is of cuspidal type, we get*

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 1 = q$$

- *if C is of twisted type, we get*

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 0 = q+1$$

Now we will see what happens in each case.

1. Suppose C of nodal type: then there are $s_1, s_2 \in K$ two distinct zeroes of the equation $t^2+at+b=0$. Notice that $[1:s_1]$, $[1:s_2]$ represent the inclinations of the two tangents at the singular point. With these assumptions, we can write the equation of C as

$$x^3 = (y - s_1x)(y - s_2x)z$$

We have already seen that we have a bijection between $C_{sm}(K)$ and $\mathbb{P}^1 \setminus \{[1:s_1],[1:s_2]\}$. To define a (group) isomorphism between $C_{sm}(K)$ and $K^\times$, we continue defining another map:

$$\begin{array}{rcl} \mathbb{P}^1 \setminus \{[1:s_1],[1:s_2]\} & \longrightarrow & K^\times \\ [\lambda : m] & \longmapsto & \frac{m - s_1\lambda}{m - s_2\lambda} \end{array}$$

The meaning of this is, sort of speaking, to move one of the problematic tangent to infinity, and the other to 0. This map is clearly a bijection (it comes from a projectivity).

It remains only to prove that the composition of the two maps

$$\begin{array}{rccl} \psi : & C_{sm}(K) & \longrightarrow & K^\times \\ & [x:y:z] & \longmapsto & \frac{y - s_1x}{y - s_2x} \end{array}$$

is now a group isomorphism. Recall that the unit element of the group law over $C_{sm}(K)$ is $O = [0:1:0]$. Writing the group law additively, and using the fact that $O = O \circ u$ and $-p := (O \circ O) \circ p = O \circ p$, then by definition $p + q := O \circ (p \circ q) = -(p \circ q)$. So the definition of the group law becomes equivalent to

$$p + q + (p \circ q) = O$$

Hence, to prove that ψ is a group homomorphism, it is enough to prove that $\psi(p)\psi(q)\psi(p \circ q) = \psi(O)$, for any $p, q \in C_{sm}(K)$.

Observe that $\psi(O) = \psi([0:1:0]) = 1$. It is then sufficient to show that, fixed any line not containing the singular point, and called p, q, r the three points of intersection of it with the cubic curve, we have always that

$$\psi(p)\psi(q)\psi(r) = 1$$

To do that, we can change the variables $y \mapsto y - s_2 x$. This gives in the new variables the equation of the cubic

$$x^3 = (y - sx)yz$$

where $s := s_1 - s_2 \neq 0$, and now

$$\psi([x : y : z]) = \frac{y - sx}{y}$$

Furthermore the coordinates of the singular point and of the point at infinity are not changed. Now we don't have nonsingular points on the line $y = 0$, so we can pass to the affine coordinate system obtained sending that line at infinity: we get that the lines $z = \alpha x + \beta$, with $\beta \neq 0$, are all the lines that intersect the cubic curve but that do not contain the singular point. The affine equation of the curve is now become $x^3 = (1 - sx)z$ and $\psi([x : 1 : z]) = \frac{1-sx}{1}$.

We want to show that, for the three points of intersection of the line $z = \alpha x + \beta$ with the cubic curve, that are $p_i = [1 : \alpha x_i + \beta : x_i]$ such that $x_i^3 = (1 - sx_i)(\alpha x_i + \beta)$ $(i = 1, 2, 3)$, we have that

$$\psi(p_1)\psi(p_2)\psi(p_3) = 1$$

equivalently

$$(1 - sx_1)(1 - sx_2)(1 - sx_3) = 1$$

Observing that the x_i are solution of $x^3 = (1 - sx)(\alpha x + \beta) = -s\alpha x^2 + (\alpha - s\beta)x + \beta$, then

$$x_1x_2x_3 = \beta \qquad x_1x_2 + x_1x_3 + x_2x_3 = s\alpha - \beta \qquad x_1 + x_2 - x_3 = -s\alpha$$

We get

$$(1 - sx_1)(1 - sx_2)(1 - sx_3) = 1 - s(x_1 + x_2 + x_3) + s^2(x_1x_2 + x_1x_3 + x_2x_3) - s^3x_1x_2x_3 =$$

$$= 1 - s(-s\alpha) + s^2(s\beta - \alpha) - s^3\beta = 1 + s^2(\alpha - \alpha) + s^3(\beta - \beta) = 1$$

as wanted.

We have proved that ψ is a group isomorphism between $C_{sm}(K)$ and $K^\times$.

2. Suppose C of cuspidal type: then there exists $s \in K$ the unique zero of the equation $t^2 + at + b = 0$. Notice that $[1 : s]$ represents the inclination of the double tangent at the cusp. With these assumptions, we can write the equation of C as

$$x^3 = (y - sx)^2$$

We have already seen that we have a bijection between $C_{sm}(K)$ and $\mathbb{P}^1 \setminus \{[1 : s]\}$. To define a (group) isomorphism between $C_{sm}(K)$ and K^+, we continue defining another map:

$$\begin{array}{rcl} \mathbb{P}^1 \setminus \{[1:s]\} & \longrightarrow & K^+ \\ [\lambda : m] & \longmapsto & \frac{\lambda}{m-s\lambda} \end{array}$$

Sort of speaking, we have moved the inclination of the tangent at infinity. This map is clearly a bijection (it comes from a projectivity).

It remains only to prove that the composition of the two maps

$$\begin{array}{rccl} \varphi : & C_{sm}(K) & \longrightarrow & K^+ \\ & [x:y:z] & \longmapsto & \frac{x}{y-sx} \end{array}$$

is now a group isomorphism. As before, it is enough to prove that $\varphi(p)+\varphi(q)+\varphi(p \circ q) = \varphi(O)$, for any $p, q \in C_{sm}(K)$. Observe that now $\varphi(O) = \varphi([0:1:0]) = 0$. So it is sufficient to show that, fixed any line not containing the singular point, if we call p, q, r the three points of intersection of it with the cubic curve, we have

$$\varphi(p) + \varphi(q) + \varphi(r) = 0$$

To do that, we can change the variables as $y \mapsto y - sx$. This gives, in the new variables, the equation of the cubic curve

$$x^3 = y^2 z$$

and now

$$\varphi([x:y:z]) = \frac{x}{y}$$

Furthermore the coordinates of the singular point and of the point at infinity are not changed. Now we don't have smooth points on the line $y = 0$, so we can pass to the affine coordinate system obtained sending that line at infinity: we get that the lines $z = \alpha x + \beta$, with $\beta \neq 0$, are all the lines that intersect the cubic curve but that do not contain the singular point. The affine equation of the curve is now become $x^3 = z$ and $\varphi([x:1:z]) = \frac{x}{1}$.

We want to show that, for the three points of intersection of the line $z = \alpha x + \beta$ with the cubic curve, that precisely are $p_i = [1 : \alpha x_i + \beta : x_i]$ such that $x_i^3 = (1 - s x_i)(\alpha x_i + \beta)$ $(i = 1, 2, 3)$, we have that

$$x_1 + x_2 + x_3 = 0$$

This follows because $x^3 = (\alpha x + \beta)$ has no term of second degree.

We have proved that φ is a group isomorphism between $C_{sm}(K)$ and K^+.

3. Suppose C of twisted nodal type: there are no solutions in K of $t^2 + at + b = 0$, but there are two distinct solution s_1, s_2 in some quadratic extension of K.

   Define $L := K(s_1, s_2) = K(s_1)$, the quadratic extension of K that is also the splitting field of our polynomial. Over L our cubic curve is of nodal type, hence we can use the point

1., to get an isomorphism $\psi : C_{sm}(L) \cong L^\times$. This implies that $C_{sm}(K) \cong \psi(C_{sm}(K)) \subseteq L^\times$. We will now see that

$$\psi(C_{sm}(K)) = \{l \in L^\times : N_{L/K}(l) = 1\}$$

One side of the inclusion is easy:

$$N_{L/K}\left(\psi([x:y:z])\right) = N_{L/K}\left(\frac{y-s_1x}{y-s_2x_2}\right) = \frac{y-s_1x}{y-s_2x_2}\cdot\sigma\left(\frac{y-s_1x}{y-s_2x_2}\right) = \frac{y-s_1x}{y-s_2x_2}\frac{y-s_2x}{y-sx_1} = 1$$

where σ is the K-automorphism that exchanges s_1 and s_2.

Viceversa, notice that the inverse of the map ψ is the map

$$\begin{array}{rccl} \psi^{-1}: & L^\times & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [(s_1-s_2)^2u(1-u) : (s_1-s_2)^2u(s_1-s_2u) : (1-u)^3] \end{array}$$

If $u = 1$, then $\psi^{-1}(1) = [0:1:0]$. If not, we can write

$$\psi^{-1}(u) = \left[(s_1-s_2)^2\frac{u}{(1-u)^2} : (s_1-s_2)^2\frac{u}{(1-s)^2}\frac{s_1-s_2u}{1-u} : 1\right]$$

Take then u an element of $L^\times$ of norm 1, precisely $u = a + bs_1 \in L^\times = K(s_1)^\times$ is such that $N_{L/K}(u) = u\cdot\sigma(u) = 1$. First, observe that $(s_1-s_2)^2 = b^2 - 4c \in K$. Secondly, we have

$$\frac{u}{(1-u)^2} = \frac{u}{1-2u+u^2} = \frac{u}{u\sigma(u)-2u+u^2} = \frac{1}{\sigma(u)+u-2} \in K$$

because $u + \sigma(u) = \mathrm{Tr}_{L/K}(u) \in K$. Finally,

$$\frac{s_1-s_2u}{1-u} = \frac{(s_1-s_2u)(1-\sigma(u)}{(1-u)(1-\sigma(u)} = \frac{s_1-s_2u-s_1\sigma(u)+s_2u\sigma(u)}{N(1-u)} =$$

$$= \frac{s_1+s_2-(s_2u)-(\sigma(s_2u)}{N(1-u)} = \frac{-b-\mathrm{Tr}(s_2u)}{N(1-u)} \in K$$

Hence $\psi^{-1}(u) \in C_{sm}(K)$ for $u \in L^\times$ of norm 1, and we have proved that:

$$C_{sm}(K) \cong \{l \in L^\times : N_{L/K}(l) = 1\} \leq L^\times$$

4. Suppose C of twisted cuspidal type: the characteristic of K has to be 2, our polynomial has to be $t^2 + b = 0$ and is irreducible over K. It has a unique solution s in some quadratic extension of K. Precisely $s \notin K$ is such that $s^2 = b$.

   Define then $L \coloneqq K(s)$.

   Over L our cubic curve is of cuspidal type: we can then use the point 2., to get an isomorphism $\varphi : C_{sm}(L) \cong L^+$. This implies that $C_{sm}(K) \cong \varphi(C_{sm}(K)) \subseteq L^+$. We will now see that

$$\varphi(C_{sm}(K)) = \left\{l = \alpha + \beta s \in L : \beta^2 = \alpha + b\alpha^2\right\}$$

One side of the inclusion is easy: consider $[x : y : z] \in C_{sm}(K)$; we have

$$\varphi([x : y : z] = \frac{x}{y + sx} = \frac{x(y + sx)}{y^2 + bx^2} = \frac{xy}{y^2 + bx^2} + s\frac{x^2}{y^2 + bx^2}$$

We can define $\alpha := \frac{xy}{y^2+bx^2}$ and $\beta := \frac{x^2}{y^2+bx^2}$. If we write $\gamma := \frac{x}{y+bx}$, we have that $\frac{y}{y+sx} = 1 + s\gamma$ and we get

$$\alpha = \gamma(1 + s\gamma) \quad \text{and} \quad \beta = \gamma^2$$

We obtain

$$\alpha^2 + \beta + b\beta^2 = \gamma^2 + b\gamma^4 + \gamma^2 + b\gamma^4 = 0$$

what we want.

For the converse, it is easy to check that the inverse of φ is the following map:

$$\begin{array}{ccc} L^+ & \longrightarrow & C_{sm}(L) \\ u & \longmapsto & [u : 1 + su : u^3] \end{array}$$

Suppose $u = \alpha + s\beta$, with $\alpha, \beta \in K$, and $\alpha^2 + b\beta^2 = (\alpha + s\beta)^2 = \beta$. Then

$$\varphi^{-1}(u) = \varphi^{-1}(\alpha + s\beta) = [\alpha + s\beta : 1 + s(\alpha + s\beta) : (\alpha + s\beta)^3] =$$

$$= \left[1 : \frac{\alpha + s\beta + s(\alpha + s\beta)^2}{(\alpha + s\beta)(\alpha + s\beta)} : (\alpha + s\beta)^2\right] = [1 : \frac{\alpha}{\beta} : \beta] \in C_{sm}(K)$$

as wanted.

□

0.3 Singular cubic curve with the singular point not defined over K

This case can happen only if the ground field K is of characteristic 2 or 3 (furthermore this field at least has not to be perfect, nor finite).

0.3.1 Case - characteristic 2, singular point not defined over K

Suppose now that our field K has characteristic 2. From the Weierstrass model

$$zy^2 + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

we get the partial derivatives $(x^2 + a_1yz + a_4z^2, z(a_1x + a_3z), y^2 + a_1xy + a_2x^2 + a_6z^2)$. It is easy to show that the only possibility to have a singular point not defined over K is that

$$a_1 = a_3 = 0$$

We can make the substitution $x \mapsto x + a_2 z$, in order to get the following equation for our singular cubic:

$$y^2 z = x^3 + b_4 x z^2 + b_6 z^3$$

with $b_4 := a_2^2 + a_2 a_4$ and $b_6 := a_2 a_4 + a_6$.

The singular point is now $[\gamma, \delta, 1]$, with $\gamma^2 = b_4$, $\delta^2 = b_6$, and γ and δ not both in K.

In all the cases, over $L' := K(\gamma, \delta)$, we can change the variables moving the singular point in $[0 : 0 : 1]$. Precisely we send $x \mapsto x + \gamma z$ and $y \mapsto y + \delta z$, obtaining the equation

$$C^0 : z y^2 = x^3 + \gamma x^2 z$$

Now the tangent complex at the singular point is $0 = y^2 + \gamma x^2 = (y + sx)^2$, for an s such that $s^2 = \gamma$. This s could be in K or in $K(\delta)$, for example. But, if $\gamma \notin K$, then $s \notin K(\gamma)$: indeed if $s = a + \gamma b \in K(\gamma)$ for some $a, b \in K$, then, taking the square $\gamma = a^2 + b_4 b^2 \in K$. In exactly the same way it's clear also that if $\gamma \notin K$ then $s \notin K(\delta)$.

We will now state the main result of this section.

Theorem 2. *Assuming what done above, we can define $L := K(s, \delta)$. We have that*

1. *if $\gamma, \delta \notin K$ and $\delta \notin K(\gamma)$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_6^2 b^4\right\}$$

2. *if $\gamma, \delta \notin K$ and $\delta \in K(\gamma)$, i.e. $\delta = \alpha + \gamma\beta$ for some known $\alpha, \beta \in K$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_4^2 \beta^4 b^4\right\}$$

3. *if $\gamma \notin K$, $\delta \in K$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^4 = b + b_4 b^2\right\}$$

4. *if $\gamma \in K$, $\delta \notin K$ and $s \notin K(\delta)$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^2 = b + \gamma b^2 + b_6 b^4\right\}$$

5. *if $\gamma \in K$, $\delta \notin K$ and $s \notin K$, but $s \in K(\delta)$, i.e. $s = \alpha + \beta\delta$ for some known $\alpha, \beta \in K$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^2 = b + b_6 \beta^2 b^2 + b_6 b^4\right\}$$

6. *if $\gamma \in K$, $\delta \notin K$ and $s \in K$, then*

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^2 = b + b_6 b^4\right\}$$

Proof. We start now in all generality, with γ, δ not both in K. Over $L = K(s, \delta)$, we have, using the notations as before,

$$\begin{array}{rccccc} \phi: & C_{sm}(L) & \longrightarrow & C^0_{sm}(L) & \longrightarrow & L^+ \\ & [x:y:z] & \longmapsto & [x+\gamma z : y+\delta z : z] & & \\ & & [x:y:z] & \longmapsto & \frac{x}{y+sx} & \end{array}$$

The composition gives, for $[x : y : z] \in C_{sm}(L)$,

$$\phi([x:y:z]) = \frac{x+\gamma z}{y+\delta z+sx+s^3 z} = \frac{(x+\gamma z)(y+\delta z+sx+s^3 z)}{y^2+b_6 z^2+\gamma x^2+\gamma b_4 z^2} =$$

$$= \frac{z(x+\gamma z)(y+\delta z+sx+s^3 z)}{x(x^2+b_4 z^2)+z(\gamma x^2+\gamma b_4 z^2)} = \frac{z(x+\gamma z)(y+\delta z+sx+s^3 z)}{(x^2+b_4 z^2)(x+\gamma z)} =$$

$$= \frac{z(y+\delta z+sx+s^3 z)}{x^2+b_4 z^2} = \frac{yz}{x^2+b_6 z^2} + \delta \frac{z^2}{x^2+b_6 z^2} + s\frac{xz}{x^2+b_6 z^2} + s^3 \frac{z^2}{x^2+b_6 z^2}$$

We define

$$a := \frac{yz}{x^2+b_6 z^2}, \quad b := \frac{z^2}{x^2+b_6 z^2}, \quad c := \frac{xz}{x^2+b_6 z^2}, \quad d := \frac{z^2}{x^2+b_6 z^2}$$

If $[x : y : z] \in C_{sm}(K)$, these elements are in K.

Define furthermore

$$l := \frac{z}{x+\gamma z}$$

Now $+\gamma l = \frac{x}{x+\gamma z}$, and then we obtain the formulas

$$b = d = l^2 \quad \text{and} \quad c = l(1+\gamma l)$$

Furthermore, using the equation of the cubic curve $y^2 z + x^3 + b_4 x z^2 + b_6 z^3 = 0$, we can write $\frac{y^2}{(x+\gamma z)^2} l + (1+\gamma l)^3 + b_4(1+\gamma l) l^2 + b_6 l^3 = 0$. This implies $\frac{y^2}{(x+\gamma z)^2} l = 1 + \gamma l + b_6 l^3$ and so $\frac{y}{x+\gamma z} = \frac{1}{\sqrt{l}} + s + \delta l$. Finally we have

$$a = l\frac{y}{x+\gamma z} = \sqrt{l} + sl + \delta l^2$$

In the following, we will analyze all the cases.

1. Suppose $\gamma, \delta \notin K$ and $\delta \notin K(\gamma)$. We know furthermore that $s \notin K(\gamma, \delta)$. Then we can write each element u of $L = K(s, \delta)$ as

   $$u = k_1 + k_2\delta + k_3 s + k_4\gamma + k_5 s^3 + k_6\delta s + k_7\delta\gamma + k_8\delta s^3$$

   for some uniquely determined $k_i \in K$, $i = 1, ..., 8$.

Before, we have shown that, for $[x : y : z] \in C_{sm}(K)$,

$$\phi([x : y : z]) = a + b\delta + cs + ds^3$$

with $a = \sqrt{l} + sl + \delta l^2$, $b = d = l^2$, $c = l + \gamma l^2$.
From this, we have $a^2 = l + \gamma l^2 + b_6 l^4 = c + b_6 b^2$, and so

$$c = a^2 + b_6 b^2$$

We can then define the following map:

$$\begin{array}{ccc} L^+ & \longrightarrow & K^2 \\ u = k_1 + k_2\delta + k_3 s + k_4\gamma + k_5 s^3 + k_6\delta s + k_7\delta\gamma + k_8\delta s^3 & \longmapsto & (k_1, k_2) \end{array}$$

If we restrict the domain to $\phi(C_{sm}(K))$, the map has image in $\left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_6^2 b^4\right\}$. Indeed, for $a + b\delta + cs + ds^3 \in \phi(C_{sm}(K))$ as before, we have that

$$a^4 = \left(\sqrt{l} + sl + \delta l^2\right)^4 = l^2 + b_4 l^4 + b_6^2 l^8 = b + b_4 b^2 + b_6^2 b^4$$

Using the relations shown above, we can define the inverse map in this way:

$$\begin{array}{ccc} \left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_6^2 b^4\right\} & \longrightarrow & \phi(C_{sm}(K)) \\ (a, b) & \longmapsto & a + b\delta + (a^2 + b_6 b^2)s + bs^3 \end{array}$$

It is clear from before, that between this two sets, the two maps are one the inverse of the other (once we know the surjectivity). It's very easy to show also that they are groups isomorphisms, if we give to $\left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_6^2 b^4\right\}$ the usual sum induced by K^+. We only need to know that the image of this map lies really in $\phi(C_{sm}(K))$, in order to conclude that $C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_6^2 b^4\right\}$ as groups.

Recall that

$$\begin{array}{cccccc} \phi^{-1} : & L^+ & \longrightarrow & C^0_{sm}(L) & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [u : 1 + su : u^3] & \longmapsto & [u + \gamma u^3 : 1 + su + \delta u^3 : u^3] \end{array}$$

If $u = 0$, $\phi^{-1}(u) = [0 : 1 : 0]$. If not we can write $\phi^{-1}(u) = \left[\frac{u^2+\gamma u^4}{u^4} : \frac{u+su^2+\delta u^4}{u^4} : 1\right]$.

Suppose $a, b \in K$ such that $a^4 = b + b_4 b^2 + b_6^2 b^4$, and take $u = a + b\delta + (a^2 + b_6 b^2)s + bs^3$. Then $u^2 = a^2 + b_6 b^2 + \gamma b$ and $u^4 = b$. Then

$$\phi^{-1}(u) = \left[\frac{a^2 + b_6 b^2}{b} : \frac{a}{b} : 1\right]$$

that belongs to $C_{sm}(K)$, what we wanted.

2. Suppose $\gamma, \delta \notin K$ and $\delta = \alpha + \gamma\beta \in K(\gamma)$, for some known $\alpha, \beta \in K$. Then we can write each element u of $L = K(s, \delta) = K(s)$ as

$$u = k_1 + k_2 s + k_3 \gamma + k_4 s^3$$

for some uniquely determined $k_i \in K$, $i = 1, ..., 4$.

Before, we have shown that, for $[x : y : z] \in C_{sm}(K)$,

$$\phi([x : y : z]) = a + b\delta + cs + ds^3$$

with $a = \sqrt{l} + sl + \delta l^2$, $b = d = l^2$, $c = l + \gamma l^2$. Now

$$\phi([x : y : z]) = a + b(\alpha + \gamma\beta) + cs + ds^3 = (a + \alpha b) + cs + \beta b\gamma + ds^3$$

We then define

$$a' := a + \alpha b = \sqrt{l} + sl + \delta l^2 + \alpha l^2 = \sqrt{l} + sl + (\beta\gamma) l^2$$

and

$$b' := \beta b = \beta l^2 = \beta d$$

We have that $a'^2 = l + \gamma l^2 + \beta^2 b_4 l^4 = c + \beta^2 b_4 d^2$, hence

$$c = a'^2 + \beta^2 b_4 d^2$$

Then we can define the following map:

$$\begin{array}{ccc} L^+ & \longrightarrow & K^2 \\ u = k_1 + k_2 s + k_3 \gamma + k_4 s^3 & \longmapsto & (k_1, k_4) \end{array}$$

If we restrict the domain to $\phi(C_{sm}(K))$, the map has image in $\left\{(a, d) \in K^2 : a^4 = d + b_4 d^2 + b_4^2 \beta^4 d^4\right\}$. Indeed, for $u = a' + cs + b'\gamma + ds^3 \in \phi(C_{sm}(K))$ as before, we have that

$$a'^4 = \left(\sqrt{l} + sl + \beta\gamma l^2\right)^4 = l^2 + b_4 l^4 + \beta^4 b_4^2 l^8 = d + b_4 d^2 + b_4^2 \beta^4 d^4$$

(observe also that $b_4^2 \beta^4 = b_6^2 + \alpha^4$).

Using the relations shown above, we can define the inverse map in this way:

$$\begin{array}{ccc} \left\{(a', d) \in K^2 : a'^4 = d + b_4 d^2 + b_4^2 \beta^4 d^4\right\} & \longrightarrow & \phi(C_{sm}(K)) \\ (a', d) & \longmapsto & a' + (a'^2 + \beta^2 b_4 d^2) s + \beta d\gamma + ds^3 \end{array}$$

It is clear from before, that between this two sets, the two maps are one the inverse of the other (once we know that the map is surjective). It's very easy to show also that they are two groups isomorphisms if we give to $\left\{(a, b) \in K^2 : a^4 = b + b_4 b^2 + b_4^2 \beta^4 b^4\right\}$ the usual sum induced by K^+. We only need to see that the image of this map lies really

in $\phi(C_{sm}(K))$, in order to conclude that $C_{sm}(K) \cong \left\{(a,b) \in K^2 : a^4 = b + b_4b^2 + b_4^2\beta 4b^4\right\}$ as groups.

Recall that

$$\begin{array}{rccl} \phi^{-1}: & L^+ & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [u + \gamma u^3 : 1 + su + \delta u^3 : u^3] \end{array}$$

If $u = 0$, then $\phi^{-1}(u) = [0 : 1 : 0]$. If not we can write $\phi^{-1}(u) = \left[\frac{u^2+\gamma u^4}{u^4} : \frac{u+su^2+\delta u^4}{u^4} : 1\right]$.

Suppose $a, b \in K$ such that $a^4 = b+b_4b^2+b_4^2\beta^4b^4$, and take $u = a+(a^2+\beta^2b_4b^2)s+\beta b\gamma+bs^3$. Then $u^2 = a^2 + \beta^2b_4b^2 + b\gamma$ and $u^4 = b$. Then

$$\phi^{-1}(u) = \left[\frac{a^2 + \beta^2b_4b^2}{b} : \frac{a + \alpha b}{b} : 1\right]$$

that belongs to $C_{sm}(K)$, what we wanted.

3. Suppose $\gamma \notin K$, but $\delta \in K$. We know also that then $s \notin K(\gamma)$.

   In the previous point 2), we have never really used the fact that $\delta \notin K$, equivalently we have never supposed that $\beta \neq 0$. Hence, in this case, $\delta = \alpha$ (so $\beta = 0$), and so

   $$C_{sm}(K) \cong \left\{(a,b) \in K^2 : a^4 = b + b_4b^2\right\}$$

4. Suppose $\gamma \in K$, $\delta \notin K$ and $s \notin K(\delta)$. Then we can write each element u of $L = K(s, \delta)$ as

   $$u = k_1 + k_2\delta + k_3s + k_4s\delta$$

   for some uniquely determined $k_i \in K$, $i = 1, ..., 4$.

   Before, we have shown that, for $[x : y : z] \in C_{sm}(K)$,

   $$\phi([x : y : z]) = a + b\delta + cs + ds^3$$

   with $a = \sqrt{l + sl + \delta l^2}$, $b = d = l^2$, $c = l + \gamma l^2$. Observe that, since $\gamma \in K$ then $l \in K$. Now

   $$\phi([x : y : z]) = a + b\delta + (c + \gamma d)s$$

   We define then

   $$c' = c + \gamma d = l + \gamma l^2 + \gamma l^2 = l$$

   Furthermore we have that

   $$c'^2 = l^2 = b$$

   So we can define the following map:

   $$\begin{array}{ccc} L^+ & \longrightarrow & K^2 \\ u = k_1 + k_2\delta + k_3s + k_4\delta s & \longmapsto & (k_1, k_3) \end{array}$$

If we restrict the domain to $\phi(C_{sm}(K))$, the map has image in $\left\{(a,c') \in K^2 : a^2 = c' + \gamma c'^2 + b_6 c'^4\right\}$. Indeed, for $u = a + c'^2 + \delta + c's \in \phi(C_{sm}(K))$ as before, we have that

$$a^2 = \left(\sqrt{l} + sl + \delta l^2\right)^2 = l + \gamma l^2 + b_6 l^4 = c' + \gamma c'^2 + b_6 c'^4$$

Using the relations shown above, we can define the inverse map in this way:

$$\begin{array}{ccc} \left\{(a,c') \in K^2 : a^2 = c' + \gamma c'^2 + b_6 c'^4\right\} & \longrightarrow & \phi(C_{sm}(K)) \\ (a,c') & \longmapsto & a + c'^2\delta + c's \end{array}$$

It is clear from before, that between this two sets, the two maps are one the inverse of the other (once we know that the map is surjective). It's very easy to show also that they are two groups isomorphisms if we give to $\left\{(a,b) \in K^2 : a^2 = b + \gamma b^2 + b_6 b^4\right\}$ the usual sum induced by K. We only need to see that the image of this map lies really in $\phi(C_{sm}(K))$ in order to conclude that $C_{sm}(K) \cong \left\{(a,b) \in K^2 : a^2 = b + \gamma b^2 + b_6 b^4\right\}$ as groups.

Recall that

$$\begin{array}{rccc} \phi^{-1}: & L^+ & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [u + \gamma u^3 : 1 + su + \delta u^3 : u^3] \end{array}$$

If $u = 0$, then $\phi^{-1}(u) = [0:1:0]$. If not we can write $\phi^{-1}(u) = \left[\frac{u^2+\gamma u^4}{u^4} : \frac{u+su^2+\delta u^4}{u^4} : 1\right]$.

Suppose $a, b \in K$ such that $a^2 = b + \gamma b^2 + b_6 b^4$, take $u = a + b^2\delta + bs$. Then $u^2 = b$ and $u^4 = b^2$. Then

$$\phi^{-1}(u) = \left[\frac{b + \gamma b^2}{b^2} : \frac{a}{b^2} : 1\right]$$

that belongs to $C_{sm}(K)$, what we wanted.

5. Suppose $\gamma \in K$, $\delta \notin K$ and $s \notin K$, but $s = \alpha + \beta\delta \in K(\delta)$, for some $\alpha, \beta \in K$ known. Then we can write each element u of $L = K(s,\delta) = K(\delta)$ as

$$u = k_1 + k_2\delta$$

for some uniquely determined $k_1, k_2 \in K$.

Before, we have shown that for $[x:y:z] \in C_{sm}(K)$,

$$\phi([x:y:z]) = a + b\delta + cs + ds^3$$

with $a = \sqrt{l} + sl + \delta l^2$, $b = d = l^2$, $c = l + \gamma l^2$. Observe that, since $\gamma \in K$ then $l \in K$. Now

$$\phi([x:y:z]) = a + b\delta + (c + \gamma d)(\alpha + \beta\delta) = a + \alpha(c + \gamma d) + (b + \beta(c + \gamma d))\delta$$

We define then

$$b' := b + \beta(c + \gamma d) = b + \beta l = l^2 + \beta l$$

and

$$a' := a + \alpha(c + \gamma d) = a + \alpha l = \sqrt{l} + sl + \delta l^2 + \alpha l^2 = \sqrt{l} + \delta(l^2 + \beta l) = \sqrt{l} + \delta b'$$

Hence we have $a'^2 = l + b_6 b'^2$ and so

$$l = a'^2 + b_6 b'^2$$

Then we can define the following map:

$$\begin{array}{ccc} L^+ & \longrightarrow & K^2 \\ u = k_1 + k_2\delta & \longmapsto & (k_1, k_1^2 + b_6 k_2^2) \end{array}$$

If we restrict the domain to $\phi(C_{sm}(K))$, the map has image in $\left\{(a', l) \in K^2 : a'^2 = l + b_6\beta^2 l^2 + b_6 l^4\right\}$. Indeed, for $u = a' + b'\delta \in \phi(C_{sm}(K))$ as before, we have that

$$a'^2 = l + b_6 b'^2 = l + b_6\beta^2 l^2 + b_6 l^4$$

Using the relations shown above, we can define the inverse map in this way:

$$\begin{array}{ccc} \left\{(a', l) \in K^2 : a'^2 = l + b_6\beta^2 l^2 + b_6 l^4\right\} & \to & \phi(C_{sm}(K)) \\ (a', l) & \mapsto & a' + (\beta l + l^2)\delta \end{array}$$

It is clear from before, that between this two sets, the two maps are one the inverse of the other (once we know that the map is surjective). It's very easy to show also that they are two groups isomorphisms if we give to $\left\{(a, b) \in K^2 : a^2 = b + b_6\beta^2 b^2 + b_6 b^4\right\}$ the usual sum induced by K. We only need to see that the image of this map lies really in $\phi(C_{sm}(K))$ in order to conclude that $C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^2 = b + b_6\beta^2 b^2 + b_6 b^4\right\}$ as groups.

Recall that

$$\begin{array}{rccc} \phi^{-1} : & L^+ & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [u + \gamma u^3 : 1 + su + \delta u^3 : u^3] \end{array}$$

If $u = 0$, then $\phi^{-1}(u) = [0 : 1 : 0]$. If not we can write $\phi^{-1}(u) = \left[\frac{u^2+\gamma u^4}{u^4} : \frac{u+su^2+\delta u^4}{u^4} : 1\right]$.

Suppose $a, b \in K$ such that $a^2 = b + b_6\beta^2 b^2 + b_6 b^4$, and take $u = a + (\beta b + b^2)\delta$. Then $u^2 = b$ and $u^4 = b^2$. Then

$$\phi^{-1}(u) = \left[\frac{b + \gamma b^2}{b^2} : \frac{a + \alpha b}{b^2} : 1\right]$$

that belongs to $C_{sm}(K)$, what we wanted.

6. Suppose $\gamma \in K$, $\delta \notin K$ and $s \in K$.

   In the previous point, we have never really used the fact that $s \notin K$, equivalently we have never supposed that $\beta \neq 0$. Hence, in this case, $s = \alpha$ (so $\beta = 0$), and so

$$C_{sm}(K) \cong \left\{(a, b) \in K^2 : a^2 = b + b_6 b^4\right\}$$

□

0.3.2 Case - characteristic 3, singular point not defined over K

Suppose now that our field K has characteristic 3. From our Weierstrass model $zy^2+a_1xyz+a_3yz^2 = x^3+a_2x^2z+a_4xz^2+a_6z^3$, we can change the variables with $y \mapsto \frac{1}{2}(y-a_1x-a_3z)$, obtaining the equation

$$y^z = x^3 + b_2x^2z + b_4xz^2 + b_6z^3$$

with $b_2 \coloneqq a_2 + a_1^2$, $b_4 \coloneqq a_4 - a_1a_3$, $b_6 \coloneqq a_6 + a_3^2$.

The partial derivatives are $(z(-b_2x+b_4z); yz; -y^2+x(b_2x-b_4z))$, and it is not difficult to see that the only case for which the singular point is not defined over K, can happen when

$$b_2 = b_4 = 0$$

We get then the equation

$$y^2z = x^3 + b_6z^3$$

Hence we have the singular point in $[\gamma : 0 : 1]$, where $\gamma \notin K$ is such that $\gamma^3 = -b_6$.

Theorem 3. *With the assumptions done above, define $L \coloneqq K(\gamma)$. We have that*

$$C_{sm}(K) \cong \left\{a + b\gamma \in L : a^3 = b + b_6b^3\right\}$$

Proof. Over $L = K(\gamma)$, we can move the singular point to the origin with the change the variables $x \mapsto x - \gamma z$, getting the curve in the new variables

$$C^0 : y^2z = x^3$$

Hence we have

$$\begin{array}{cccccc} \phi & C_{sm}(L) & \longrightarrow & C^0_{sm}(L) & \longrightarrow & L^+ \\ & [x:y:z] & \longmapsto & [x-\gamma z : y : z] & & \\ & & & [x:y:z] & \longmapsto & \frac{x}{y} \end{array}$$

The composition gives, for $[x : y : z] \in C_{sm}(L)$,

$$\phi([x:y:z]) = \frac{x-\gamma z}{y} = \frac{x}{y} - \gamma\frac{z}{y}$$

Now, if $[x : y : z] \in C_{sm}(K)$, then from the equation of the cubic we get

$$\left(\frac{x}{y}\right)^3 - \frac{z}{y}\frac{y^2}{y^2} + b_6\left(\frac{z}{y}\right)^3 = 0$$

It follows that $\phi([x : y : z]) \in \{a + b\gamma \in L : a^3 + b_6b^3 + b = 0\}$.

For the converse, we take $u = a + \gamma b \in L$ such that $a^3 + b_6b^3 + b = 0$, equivalently $(a+\gamma b)^3 = -b$. Now

$$\begin{array}{rccc} \phi^{-1}: & L^+ & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [u + \gamma u^3 : 1 : u^3] \end{array}$$

In our case, $[u + \gamma u^3 : 1 : u^3] = [a + \gamma b + \gamma(-b) : 1 : -b] = [a : 1 : -b] \in C_{sm}(K)$. Hence we have proved the other inclusion and we have finished. □