Lectures on Elliptic Curves

J. W. S. CASSELS

London Mathematical Society
Student Texts **24**

Remark 1. We have not merely shown that there is a solution of $F(\mathbf{x}) = 0$, but we have found that there is one in a certain ellipsoid. This facilitates the search in explicitly given cases.

Remark 2. We have made no use of the condition of solubility in $\mathbb{Q}_p$ for $p \nmid 2f_1f_2f_3$. In fact this condition tells us nothing [cf. §3, Exercises 2, 3]. It is left to the reader to check that for any f_1, f_2, f_3 and p with $p \nmid 2f_1f_2f_3$ there is always a point defined over $\mathbb{Q}_p$ on

$$f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0.$$

Remark 3. We have also nowhere used that there is local solubility for $\mathbb{Q}_\infty = \mathbb{R}$.

Hence solubility at $\mathbb{Q}_\infty$ is implied by solubility at all the $\mathbb{Q}_p$ ($p \neq \infty$). This phenomenon is connected with quadratic reciprocity. In fact for any conic over $\mathbb{Q}$, the number of p (including ∞) for which there is not a point over $\mathbb{Q}_p$ is always even [cf. §3, Exercises 6,7]. See a book on quadratic forms (such as the author's).

§5. Exercises

1. Let

$$F(X,Y,Z) = 5X^2 + 3Y^2 + 8Z^2 + 6(YZ + ZX + XY).$$

Find rational integers x, y, z not all divisible by 13, such that

$$F(x,y,z) \equiv 0 \pmod{13^2}.$$

[*Hint.* cf. Hensel's Lemma 2 of §10.]

2. Let

$$F(X,Y,Z) = 7X^2 + 3Y^2 - 2Z^2 + 4YZ + 6ZX + 2XY.$$

Find rational integers x, y, z not all divisible by 17 such that

$$F(x,y,z) \equiv 0 \pmod{17^3}.$$

6

Cubic curves

In this section we consider curves given by

$$\mathcal{C} : F(\mathbf{X}) = F(X_1, X_2, X_3) = 0,$$

where F is a homogeneous cubic form. The case of interest is when the ground field is the rationals $\mathbb{Q}$, but our initial remarks apply to any ground field.

A point $\mathbf{x}$ on $\mathcal{C}$ is said to be *singular* when

$$\frac{\partial F}{\partial X_j}(\mathbf{x}) = 0 \qquad (j = 1,2,3).$$

If we choose co-ordinates so that $\mathbf{x} = (0,0,1)$, this is equivalent to F not containing terms in X_3^3, $X_1X_3^2$, $X_2X_3^2$.

A singular point counts with multiplicity at least 2 as an intersection with a line. More precisely, if $\mathbf{a}$, $\mathbf{b}$ are two points on the line, the general point on it is

$$\lambda\mathbf{a} + \mu\mathbf{b},$$

where the numbers λ, μ are not both 0. The intersections with $\mathcal{C}$ are given by

$$F(\lambda\mathbf{a} + \mu\mathbf{b}) = 0, \qquad (*)$$

a homogeneous cubic in λ, μ. What is claimed is that if one of the intersections is a singular point of $\mathcal{C}$ then the corresponding ratio $\lambda : \mu$ occurs as a multiple root of (*). An easy way to check this is to take $\mathbf{b} = \mathbf{x}$.

Suppose that $\mathcal{C}$ has two distinct singular points $\mathbf{x}$, $\mathbf{y}$. The line joining them cuts $\mathcal{C}$ at both $\mathbf{x}$, $\mathbf{y}$ with multiplicity ≥ 2. This can happen only if $F(\lambda\mathbf{x} + \mu\mathbf{y})$ vanishes identically, i.e. if $\mathcal{C}$ contains the whole line. If we suppose, as we shall, that $\mathcal{C}$ is *irreducible* (i.e. that F does not factorize), this cannot happen. An irreducible cubic curve has at most one singular point.

Now take the ground field to be $\mathbb{Q}$. If there is a singular point over the algebraic closure $\overline{\mathbb{Q}}$, there is at most one. By Galois theory[2] it must be defined over $\mathbb{Q}$. Hence, as we have already seen in §1, $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}$ to the line.

From now on we restrict attention to *non-singular* cubic curves, i.e. those which have non-singular points over $\overline{\mathbb{Q}}$. Let $\mathbf{a}$, $\mathbf{b}$ be rational points on $\mathcal{C}$. The line joining them meets $\mathcal{C}$ in a third point, in general distinct: it is also rational since it is given by a cubic equation, two of whose roots are rational. This process was used already by Diophantos to find new unobvious points from known obvious ones. The variant in which one takes the third point of intersection with the curve of the tangent at a rational point was, according to Weil, first noted by Newton. An older generation of mathematicians refer to these as the "chord and tangent processes".

In general, starting from one rational point $\mathbf{a}$ on $\mathcal{C}$ one obtains infinitely many by the chord and tangent processes. If this is not the case, $\mathbf{a}$ is said to be *exceptional*. For example we have

Lemma 1. *Let $a \geq 1$ be a cubic-free integer and let*

$$\mathcal{C}: \ X^3 + Y^3 - aZ^3 = 0.$$

The point $(1, -1, 0)$ is exceptional. For $a = 1$ the points $(0, 1, 1)$, $(1, 0, 1)$ are also exceptional. For $a = 2$ the point $(1, 1, 1)$ is exceptional. No other rational point is exceptional.

Proof. We first show that the given points are indeed exceptional. The tangent at $(1, -1, 0)$ is $X + Y = 0$, which meets $\mathcal{C}$ only at $(1, -1, 0)$. The other cases for $a = 1$ are similar. The tangent at $(1, 1, 1)$ for $a = 2$ is $X + Y - 2Z = 0$, which meets $\mathcal{C}$ again only at $(1, -1, 0)$.

Let $\mathbf{x} = (x, y, z)$ be a rational point other than those named. We may suppose that x, y, z are integers without common factor. The equation for $\mathcal{C}$ implies that then x, y, z are coprime in pairs.

Let $\mathbf{x}_1 = (x_1, y_1, z_1)$ be the third point of intersection, where again x_1, y_1, z_1 are integers without common factor. It may be verified[3] that

$$x_1 : y_1 : z_1 = x(x^3 + 2y^3) : -y(2x^3 + y^3) : z(x^3 - y^3)$$

Let d be the greatest common divisor of the three terms on the right hand side. If a prime p divides both x and d it must also divide y, a contradiction. Hence d divides $x^3 + 2y^3$ and $2x^3 + y^3$. It thus divides $3x^3$ and $3y^3$, so $d = 1$ or 3. Hence

$$z_1 = \pm z(x^3 - y^3) \qquad \text{or} \qquad z_1 = \pm z(x^3 - y^3)/3.$$

In either case, it is readily verified that $|z_1| > |z|$ except for the $\mathbf{x}$ listed in the enunciation. By repeating the tangent process we thus get a sequence of points $\mathbf{x}$, $\mathbf{x}_1$, $\mathbf{x}_2, \ldots$ with

$$|z| < |z_1| < |z_2| < \ldots .$$

Hence the $\mathbf{x}_j$ are distinct, and $\mathbf{x}$ is not exceptional.

§6. Exercises

1. (i) Show that the cubic curve

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

is non-singular provided that

$$4A^3 + 27B^2 \neq 0.$$

(ii) If $4A^3 + 27B^2 = 0$, find a singularity and decide whether it is a cusp or a double point with distinct tangents.

2. (i) Let

$$F(\mathbf{x}) = a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + dX_1X_2X_3,$$

where

$$a_1a_2a_3 \neq 0.$$

Show that $F(\mathbf{x}) = 0$ is non-singular provided that

$$a_1a_2a_3 + d^3 \neq 0.$$

(ii) If $a_1 = a_2 = a_3 = 1$, $d = -3$, show that any point (x_1, x_2, x_3) with $a_1^3 = x_2^3 = x_3^3 = x_1x_2x_3 = 1$ is a singularity.

[2] *For the cognoscenti.* If the ground field is not perfect, the conclusion does not necessarily hold. See *Note* at end of §9.

[3] This is essentially a special case of elegant formulae of Desboves for the chord and tangent processes. See Exercises and Formulary.

(iii) How does the result of (ii) square with the result proved in the text that a cubic curve has at most one singularity?

3. Let $F(\mathbf{x})$ be as in the previous question and suppose that $F(\mathbf{x}) = 0$ is non-singular.

(i) Let $F(\mathbf{x}) = 0$. Show that the third intersection $\mathbf{t}$ of the tangent at $\mathbf{x}$ is given by

$$t_j = x_j(a_{j+1}x_{j+1}^3 - a_{j+2}x_{j+2}^3) \quad (j = 1, 2, 3),$$

where the suffixes are taken mod 3.

(ii) Let $\mathbf{x}$, $\mathbf{y}$ be distinct points on $F(\mathbf{X}) = 0$. Show that the third intersection $\mathbf{z}$ of the line joining them is given by

$$z_j = x_j^2 y_{j+1} y_{j+2} - y_j^2 x_{j+1} x_{j+2}.$$

[Formulae of Desboves].

4. Starting with the solution $(2, -1, -1)$ of $X^3 + Y^3 + 7Z^3 = 0$, find 10 distinct solutions.

7

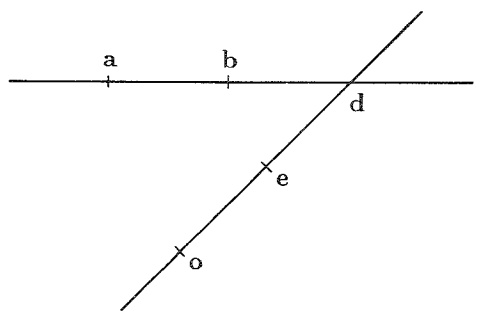
Non-singular cubics. The group law

Let $\mathcal{C}$ be a non-singular cubic curve and let $\mathbf{o}$ be a rational point on $\mathcal{C}$. We show that the set of rational points on $\mathcal{C}$ has a natural structure of commutative group with $\mathbf{o}$ as neutral element ("zero").

Hence the ground field is arbitrary, the curve $\mathcal{C}$ is defined over it; and by rational point we mean point defined over the ground field.

The group law is defined as follows. Let $\mathbf{a}$, $\mathbf{b}$ be rational points. Let $\mathbf{d}$ be the third point of intersection with $\mathcal{C}$ of the line through $\mathbf{a}$, $\mathbf{b}$. Let $\mathbf{e}$ be the third point of intersection of the line through $\mathbf{o}$, $\mathbf{d}$. Then we write

$$\mathbf{a} + \mathbf{b} = \mathbf{e}.$$



The construction has to be interpreted appropriately if two or more of the points involved coincide. For example if $\mathbf{b} = \mathbf{a}$ we take the tangent at $\mathbf{a}$.

We have to show that this operation "+" gives a structure of commutative group. Clearly

$$\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$$

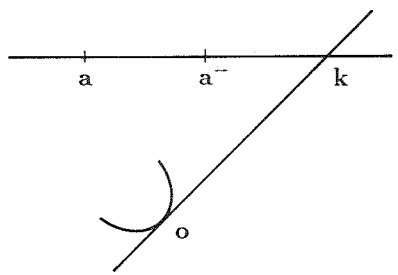
and

$$\mathbf{o}+\mathbf{a}=\mathbf{a}$$

for all $\mathbf{a}$.

Next we construct the inverse. Let the third intersection of the tangent at $\mathbf{o}$ be $\mathbf{k}$. Let $\mathbf{a}^-$ be the third intersection of the line through $\mathbf{a}$ and $\mathbf{k}$. Then by definition

$$\mathbf{a}+\mathbf{a}^-=\mathbf{o}$$

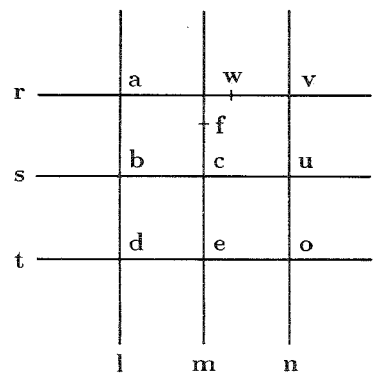


The crunch is to show that + is associative:

$$(\mathbf{a}+\mathbf{b})+\mathbf{c}=\mathbf{a}+(\mathbf{b}+\mathbf{c}).$$

We give two proofs; the first geometric, the second more fundamental.

Let $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ be given. Consider the diagram



Here $\mathbf{r}$, $\mathbf{s}$, $\mathbf{t}$, $\mathbf{l}$, $\mathbf{m}$, $\mathbf{n}$ are the names of lines and the remaining symbols are points on $\mathcal{C}$. All except $\mathbf{f}$, $\mathbf{w}$ are intersections of two of the lines. The whole figure is determined once $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{o}$ are given.

We have $(\mathbf{a}+\mathbf{b})=\mathbf{e}$, and so $(\mathbf{a}+\mathbf{b})+\mathbf{c}$ is the third intersection of the line through $\mathbf{o}$, $\mathbf{f}$. Similarly $\mathbf{a}+(\mathbf{b}+\mathbf{c})$ is the third intersection of the line through $\mathbf{o}$, $\mathbf{w}$. To prove associativity, we thus have to show that $\mathbf{f}$, $\mathbf{w}$ are not as shown but coincide with the unlabelled intersection of the lines $\mathbf{r}$, $\mathbf{m}$.

We now recall a geometrical

Lemma 1. *Let $\mathbf{x}_1,\ldots,\mathbf{x}_8$ be 8 points of the plane in general position*[4]*. Then there is a 9th point $\mathbf{y}$ such that every cubic curve through $\mathbf{x}_1,\ldots,\mathbf{x}_8$ also passes through $\mathbf{y}$.*

We briefly recall the proof of the lemma. A cubic form $F(\mathbf{X})$, $\mathbf{X}=(X_1,X_2,X_3)$ has 10 coefficients. An equation $F(\mathbf{x})=0$ imposes a linear condition on the coefficients. Passing through $\mathbf{x}_1,\ldots,\mathbf{x}_8$ imposes 8 conditions. Hence if $F_1(\mathbf{X})$, $F_2(\mathbf{X})$ are linearly independent forms through the 8 points, any other F is of the shape

$$F(\mathbf{X})=\lambda F_1(\mathbf{X})+\mu F_2(\mathbf{X}).$$

Now $F_1=0$, $F_2=0$ have 9 points in common; and clearly $F=0$ passes through them all.

Now to the application of the Lemma. Let an equation for the line $\mathbf{l}$ be $l(\mathbf{X})=0$ etc. and consider the two (reducible) cubics

$$F_1(\mathbf{X})=l(\mathbf{X})m(\mathbf{X})n(\mathbf{X})=0$$
$$F_2(\mathbf{X})=r(\mathbf{X})s(\mathbf{X})t(\mathbf{X})=0.$$

Our nonsingular cubic $\mathcal{C}$ passes through 8 of the points of intersection of $F_1=0$, $F_2=0$ and so by the Lemma must pass through the 9th. Hence $\mathbf{f}=\mathbf{w}$, as required.

We now present a second proof of the associativity of the relation "+" for points which is more basic.

A linear form $l(\mathbf{X})$ (say) does not give a meaningful function on the curve $\mathcal{C}$ because the coefficients $\mathbf{X}$ are homogeneous. On the other hand, if $t(\mathbf{X})$ is another linear form, then the quotient

$$g(\mathbf{X})=l(\mathbf{X})/t(\mathbf{X})$$

does give something meaningful. In the situation just discussed, the line

[4] This is the geometer's way of saying "such that the proffered proof works". In this case, what is needed is that the $\mathbf{x}_j$ give linearly independent conditions on the coefficients of F: so no 4 on a line and no 7 on a conic.

$l(\mathbf{X}) = 0$ passes through $\mathbf{a}$, $\mathbf{b}$, $\mathbf{d}$ and $t(\mathbf{X}) = 0$ through $\mathbf{d}$, $\mathbf{o}$, $\mathbf{e}$, all being points on $\mathcal{C}$. The function $g(\mathbf{X})$ thus has a zero $\mathbf{a}$, $\mathbf{b}$ and a pole at $\mathbf{o}$, $\mathbf{e}$. At the point $\mathbf{d}$ there is neither a zero nor a pole, as the zeros of the linear forms cancel out.

There is the notion of the order of a pole or zero at a nonsingular point of an algebraic curve which generalizes in an obvious way the notion of the order of a zero or pole of a rational function of a single variable. In our case, $g(\mathbf{X})$ clearly has simple poles at $\mathbf{a}$, $\mathbf{b}$ and simple zeros at $\mathbf{o}$, $\mathbf{e}$. The equation $\mathbf{e} = \mathbf{a} + \mathbf{b}$ is equivalent to the existence of such a function.

Similarly, the equation

$$\mathbf{x} = (\mathbf{a} + \mathbf{b}) + \mathbf{c}$$

is equivalent to the existence of a function with simple poles at $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, a double zero at $\mathbf{o}$ and a simple zero at $\mathbf{x}$. The equation

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$$

is now obvious.

This point of view shows that the group law is unchanged under birational equivalence, since it depends only on the function field of the curve. The geometer would say that $\mathbf{a} + \mathbf{b} = \mathbf{c}$ precisely when the divisor $\{\mathbf{a}, \mathbf{b}\}$ is linearly equivalent to the divisor $\{\mathbf{o}, \mathbf{c}\}$.

We conclude with an informal explanation of what is meant by saying that a nonsingular cubic curve is of genus 1. Let $r \geq 2$ and let $\mathbf{x}_1, \ldots, \mathbf{x}_r, \mathbf{y}_1, \ldots, \mathbf{y}_{r-1}$ be points on $\mathcal{C}$, for simplicity all distinct. By manipulating linear forms in $\mathbf{X}$, as we did in the construction of $g(\mathbf{X})$, one can construct a function $h(\mathbf{X})$ on the curve where only poles are simple poles at $\mathbf{x}_1, \ldots, \mathbf{x}_r$ and which has zeros at $\mathbf{y}_1, \ldots, \mathbf{y}_{r-1}$. Then $h(\mathbf{X})$ has one further zero, which is completely determined.

Contrast the position on the line. Let $c_1, \ldots, c_r, d_1, \ldots, d_r$ be any $2r$ distinct numbers. Then the function

$$\prod_j (T - d_j) \Big/ \prod_j (T - c_j)$$

has simple zeros at the d_j, simple poles at the c_j and no further zeros or poles (even at infinity).

The genus of a curve is a measure of the freedom in imposing the zeros and poles of a function. The precise statement, which we shall not need, is slightly complicated and is called the Riemann-Roch Theorem.

§7. Exercises

1. Let $\mathbf{o}$, $\mathbf{a}$ be rational points on the nonsingular cubic $\mathcal{C}$. Construct the point $-\mathbf{a}$ with respect to the group law for which $\mathbf{o}$ is the neutral element.

2. Let $\mathbf{o}$, $\mathbf{o}_1$ be rational points on the nonsingular cubic $\mathcal{C}$. Show how the group law for which $\mathbf{o}_1$ is the neutral element can be expressed in terms of that for which $\mathbf{o}$ is the neutral element.

3. Let $\mathbf{o}$, $\mathbf{a}$ be rational points on the nonsingular cubic $\mathcal{C}$ and suppose that $3\mathbf{a} = \mathbf{o}$ with respect to the group law based on $\mathbf{o}$. Let $\mathbf{b} = 2\mathbf{a}$. Show that each side of the triangle $\mathbf{o}$, $\mathbf{a}$, $\mathbf{b}$ meets the tangent to $\mathcal{C}$ of the opposite vertex at a point of $\mathcal{C}$. Take $\mathbf{o}$, $\mathbf{a}$, $\mathbf{b}$ as the triangle of reference and express this condition in terms of the coefficients of the cubic form determining $\mathcal{C}$.

4. Let $\mathcal{C}$ be the curve

$$X^3 + Y^3 - XZ^2 - YZ^2 + 7XYZ = 0$$

and let $\mathbf{x} = (x, y, z)$ be a point on $\mathcal{C}$ defined over some $\mathbb{Q}_p$. Show that $y/x \to -1$ as $\mathbf{x} \to (0, 0, 1)$ (with respect to the p-adic topology).

5. In this question everything is defined over $\mathbb{Q}_p$ for some p. Let $\mathbf{a}$ be a nonsingular point on the cubic curve

$$F(X, Y, Z) = 0$$

and let $t(\mathbf{X}) = 0$ be the tangent. Let $l(\mathbf{X}) = 0$, $m(\mathbf{X}) = 0$ be lines through $\mathbf{a}$ distinct from the tangent. Show that there are d, e, f such that

$$dl(\mathbf{X}) + em(\mathbf{X}) + ft(\mathbf{X}) = 0$$

(identically) with $d \neq 0$, $e \neq 0$. Show that

$$m(\mathbf{x})/l(\mathbf{x}) \to -d/e$$

as $\mathbf{x} \to \mathbf{a}$.

8

Elliptic curves. Canonical Form

We are concerned with algebraic curves defined up to a birational equivalence over the ground field. For genus 0 we saw that every curve is equivalent to a conic (or line). For genus 1 no such reduction to a special form or forms is possible. The situation changes when we are also given a point on the curve which is defined over the ground field (a "rational point"). It is convenient to have a special name for this situation: an *elliptic curve* is a curve of genus 1 together with the specification of a rational point on it.

As canonical form we take

$$\mathcal{C} : Y^2 = X^3 + AX + B$$

or, in homogeneous co-ordinates

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

The right hand side does not have multiple roots provided that

$$4A^3 + 27B^2 \neq 0.$$

The specified rational point $\mathbf{o}$ is the point $(X, Y, Z) = (0, 0, 1)$ at infinity.

Since the line at infinity is an inflexional tangent at $\mathbf{o}$, the group law on $\mathcal{C}$ is especially simple:

$$-(x, y) = (x, -y)$$

and $\mathbf{a} + \mathbf{b} + \mathbf{c} = \mathbf{o}$ precisely when $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ are collinear.

We shall find this choice of canonical form particularly convenient when the ground field is $\mathbb{Q}$. When the ground field is of characteristic 2 or 3, we can no longer use $\mathcal{C}$ as a canonical form but must use

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

However this is quite peripheral to our purposes and we leave it to the reader, if she wishes, to deal with these cases.

As we have not formally defined curves of genus 1, we will not give a formal proof that elliptic curves are birationally equivalent to the canonical form. In compensation we will give detailed algorithms for converting certain kinds of elliptic curves to that form. These could well be omitted at first reading.

Fact. (characteristic $\neq 2, 3$). *Any elliptic curve is birationally equivalent over the ground field to the canonical form for some A, B.*

More precisely the curve is equivalent to $\mathcal{C}$ and the equivalence takes the specified rational point $\mathbf{O}$ on it into the point at infinity on $\mathcal{C}$.

Proof for the Cognoscenti. By the Riemann-Roch theorem, the set of functions on the curve with at worst a pole of order 2 at $\mathbf{O}$ has dimension 2. Let a basis be 1, ξ. Similarly the set of functions with at worst a triple pole is of dimension 3 at $\mathbf{O}$, with basis say 1, ξ, η. Then the functions

$$\eta^2, \eta\xi, \eta, \xi^3, \xi^2, \xi, 1$$

all have at worst a pole of order 6. By the Riemann-Roch Theorem, there must be a linear relation between the 7 listed functions. The relation must involve both ξ^3 and η^2. A transformation

$$\xi \to c_1\xi + c_2$$

$$\eta \to c_3\eta + c_4\xi + c_5$$

reduces the relation to

$$\eta^2 = \xi^3 + H\xi + B$$

for some A, B.

Note for the Cognoscenti. The reason why there is no canonical form, or finite family of canonical forms for curves of genus 1 is that

$$2(g - 1) = 0 \qquad \text{for } g = 1.$$

For every other genus we can use the divisor of the differential of a function defined over the ground field to give a birational map. For example, for genus 2, there is always equivalence with some curve $Y^2 =$ sextic in X.

Particular cases. The above proof does not, in any case, usually provide a practical algorithm. We discuss some special cases. Note that it is

enough to transform the curve into the shape $\mathcal{C}$. For if it takes $\mathbf{O}$ into $\mathbf{a}$, we can make the translation $\mathbf{x} \to \mathbf{x} - \mathbf{a}$ on $\mathcal{C}$.

(i) *Cubic curve $\mathcal{D}$. Rational point $\mathbf{O}$ has inflexional tangent.* Here a linear tranformation of co-ordinates is enough, taking $\mathbf{O}$ to $\mathbf{o}$ and the tangent to be line at infinity.

For example

$$\mathcal{D} : X^3 + Y^3 + dZ^3 = 0$$

$$\mathbf{O} = (1, -1, 0).$$

Put

$$X = U + V, \qquad Y = U - V.$$

Then

$$6UV^2 = -2U^3 + dZ^3,$$

so

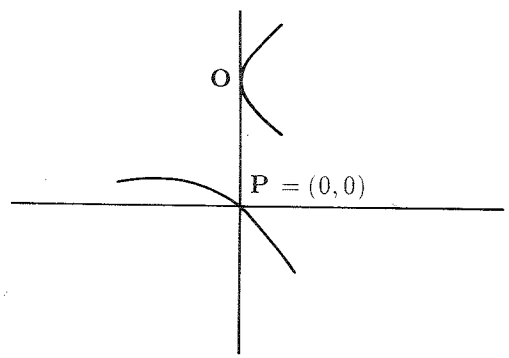
$$Y_1^2 Z_1 = X_1^3 - 2^4.3^3.d^2 Z_1^3,$$

where

$$X_1 = -6dZ, \qquad Y_1 = 6^2 dV, \qquad Z_1 = U.$$

(ii) *Cubic curve $\mathcal{D}$. Rational point $\mathbf{O}$ not on inflexional tangent*[5].

The tangent at $\mathbf{O}$ meets $\mathcal{D}$ again at a rational point $\mathbf{P}$, say. We may take an affine system of co-ordinates with $\mathbf{P}$ as origin and with the tangent as Y-axis



[5] The argument is due to Nagell: Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.* **52** (1928-9), 92-106. Older geometrical techniques (adjoint curves etc.) had shown that every elliptic curve is birationally equivalent to a cubic, but he was the first to show that it can be reduced to the canonical form.

Then the curve $\mathcal{D}$ is given by $F(X, Y) = 0$, where

$$F(X, Y) = F_1(X, Y) + F_2(X, Y) + F_3(X, Y),$$

with F_j is homogeneous of degree j.

The Y-axis meets the curve at $(0, y)$, where

$$0 = yF_1(0, 1) + y^2 F_2(0, 1) + y^3 F_3(0, 1).$$

Since the Y-axis is a tangent, we have a double root:

$$F_2(0, 1)^2 - 4F_1(0, 1)F_3(0, 1) = 0. \qquad (*)$$

Now consider the intersection of the curve with $Y = tX$. Then

$$0 = xF_1(1, t) + x^2 F_2(1, t) + x^3 F_3(1, t).$$

Discarding the solution $x = 0$, we have

$$\begin{aligned} s^2 &= F_2(1, t)^2 - 4F_1(1, t)F_3(1, t) \\ &= G(t) \qquad \text{(say)}, \end{aligned}$$

where

$$s = 2F_3(1, t)x + F_2(1, t).$$

Now $G(t)$ is a cubic by (*); and we achieve the canonical form by a linear transformation on s, t.

(iii) *Curve $\mathcal{D}$ is $Y^2 =$ Quartic in X with rational point.*

Let the rational point be (a, b). By a transformation

$$X \to \frac{1}{X - a}, \qquad Y \to \frac{Y}{(X - a)^2},$$

we may suppose that the rational point is at infinity:

$$Y^2 = f_0 + f_1 X + f_2 X^2 + f_3 X^3 + f_4 X^4,$$

where f_4 is a square. On dividing by f_4, we have without loss of generality

$$f_4 = 1.$$

We can write the right hand side as

$$G(X)^2 + H(X),$$

where

$$\begin{aligned} G(X) &= X^2 + g_1 X + g_0 \\ H(X) &= h_1 X + h_0, \end{aligned}$$

and the g_j, h_j are easily given in terms of the f_j.

The equation of the curve is now

$$(Y + G(X))(Y - G(X) = H(X).$$

Put

$$Y + G(X) = T,$$

so

$$Y - G(X) = \frac{H(X)}{T}$$

and

$$2G(X) = T - \frac{H(X)}{T}.$$

Multiply by T^2 and put $TX = S$. We get

$$2S^2 + 2g_1TS + 2g_0T^2 = T^3 - h_1S - h_0T.$$

This is readily brought to the canonical form.

(iv) *Intersection of two quadric surfaces with a rational point.*

We use homogeneous co-ordinates X, Y, Z, T and may suppose that the common rational point is $(0,0,0,1)$. The two quadric forms are thus of the shape

$$\left.\begin{aligned} Q_1 &= TL + R \\ Q_2 &= TM + S \end{aligned}\right\},$$

where L, M are linear in X, Y, Z and R, S are quadratic.

Suppose, first, that L and M are linearly dependent. Then without loss of generality $M = 0$. The intersection is

$$S(X,Y,Z) = 0, \qquad T = R(X,Y,Z)/L(X,Y,Z);$$

which is of genus 0.

Otherwise, eliminating T, we have

$$C(X,Y,Z) = LS - RM = 0,$$

where C is a homogeneous cubic. It has the rational point

$$L(X,Y,Z) = M(X,Y,Z) = 0.$$

Hence we are reduced to an earlier case.

§8. Exercises

1. Transform the following curves to canonical form:

(i) $X^3 + Y^3 + dZ^3 = 0$

(ii) $X^3 + Y^3 + Z^3 - 3mXYZ = 0$

(iii) $Y^2 - kT^2 = X^2$, $Y^2 + kT^2 = Z^2$

(iv) $X_1^2X_2 - X_1X_2^2 - X_1X_3^2 + X_2^2X_3 = 0$

2. [Difficult]. Show that the group law on

$$X^2 = Y^2 - T^2, \qquad Z^2 = Y^2 + T^2$$

with $(1,1,1,0)$ as neutral element is given by $\mathbf{x}_3 = \mathbf{x}_1 + \mathbf{x}_2$, where

$$\begin{aligned} x_3 &= x_2t_2y_1z_1 - x_1t_1y_2z_2 \\ y_3 &= y_2t_2z_1x_1 - y_1t_1z_2x_2 \\ z_3 &= z_2t_2x_1y_1 - z_1t_1x_2y_2 \\ t_3 &= t_2^2x_1^2 - t_1^2x_2^2 = t_2^2y_1^2 - t_1^2y_2^2 = t_2^2z_1^2 - t_1^2z_2^2. \end{aligned}$$

3. (i) Find all the points defined over the field $\mathbb{F}_5$ of 5 elements on each of

$$Y^2Z = X^3 + XZ^2$$
$$Y^2Z = X^3 + 2XZ^2$$
$$Y^2Z = X^3 + Z^3.$$

Check in each case that they form a group under the group law, with $(0,1,0)$ as neutral element.

(ii) As (i) but with other $\mathbb{F}_p$ and other curves

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Find an example where the group is not cyclic. Can you find an example where the group requires more than 2 generators?

4. In the curves considered below, the point at infinity is taken as neutral element for the group law.

(i) Let $Y^2 = (X-\alpha)(X^2+aX+b)$ be an elliptic curve. Show that the transformation $\mathbf{x} \to \mathbf{x} + (\alpha, 0)$ induces a fractional-linear transformation

$$T : x \to (t_{11}x + t_{12})/(t_{21}x + t_{22}).$$

Check that $T^2 : x \to x$.

(ii) Consider $Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ and let T_1, T_2, T_3 be as in (i) with $\alpha = \alpha_j$ $(j = 1,2,3)$. Show that T_1, T_2, T_3 commute and that

$$T_1T_2T_3 : x \to x.$$

(iii) Let $\mathcal{T}_j$ be the 2×2 matrix of coefficients $\left(\begin{smallmatrix} t_{11} & t_{21} \\ t_{12} & t_{22} \end{smallmatrix}\right)$ in (i) with $\alpha = \alpha_j$ $(j = 1,2,3)$. Show that

$$\mathcal{T}_1\mathcal{T}_2 + \mathcal{T}_2\mathcal{T}_1 = 0.$$

(iv) Find the fixed points of T_1 and show that they are interchanged by T_2.

5. Find a necessary and sufficient condition that a line $Y = lX + m$

should be an inflexional tangent to

$$Y^2 = X^3 + AX + B.$$

Hence find a general formula for the curves in canonical form having a rational point of order 3.

6. Find a necessary and sufficient condition that a line $Y = lX + m$ should be an inflexional tangent to $Y^2 = X(X^2 + aX + b)$.
Hence find a general formula for curves in canonical form having a point of order 6.

7. Let

$$F(X, Y, Z) = X^2Y + XZ^2 + 2Y^3 + Z^3.$$

Find a birational transformation defined over $\mathbb{Q}$ taking the curve $F = 0$ into canonical form with the point $(1, 0, 0)$ going to the point at infinity.

8. Find a birational transformation defined over $\mathbb{Q}$ taking

$$X_1^2 - 2X_2^2 + X_3^2 = 0, \quad X_2^2 - 2X_3^2 + X_4^2 = 0$$

into canonical form, with $(1, 1, 1, 1)$ going to the point at infinity.

9. Invent similar exercises to the two preceding, and solve them.

9

Degenerate laws

In this section we consider the curve

$$\mathcal{C} : Y^2 = X^3 + AX + B \tag{1}$$

when

$$4A^3 + 27B^2 = 0. \tag{2}$$

There is then precisely one singular point. We recall that if (2) does not hold, there is a group law on the curve given by[6]

$$\mathbf{a} + \mathbf{b} + \mathbf{c} = 0$$

whenever $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ are the intersection of a line with $\mathcal{C}$. We show that this continues to give a group law on the nonsingular points in the degenerate case (2), and we find out what it is.

There are two cases, the second with two subcases.

First case. Cusp. Suppose $A = B = 0$, so

$$\mathcal{C} : Y^2Z = X^3$$

with a singular point at the origin. Any line not passing through the origin can be written

$$Z = lX + mY.$$

It meets $\mathcal{C}$ where

$$X^3 - Y^2(lX + mY) = 0$$

[6] We write indifferently 0 or $\mathbf{o}$ for the neutral element of the group law.

If the three points of intersection are (x_j, y_j, z_j) $(j = 1, 2, 3)$, it follows that

$$u_1 + u_2 + u_3 = 0,$$

where

$$u_j = x_j/y_j.$$

We therefore have the additive group, the zero being the point $(0, 1, 0)$ at infinity.

Second case[7]. *Double point.* (Characteristic $\neq 2$). If not both A, B vanish, then, after a transformation $X \to X+$ constant, we have

$$\mathcal{C} : Y^2Z = X^2(X + CZ) \qquad (C \neq 0),$$

i.e.

$$(Y^2 - CX^2)Z = X^3.$$

Suppose, first, that $C = \gamma^2$ is a square. Put

$$U = Y + \gamma X, \qquad V = Y - \gamma X;$$

so $\mathcal{C}$ is given by

$$8\gamma^3 UVZ = (U - V)^3.$$

Any line not passing through the origin can be written

$$Z = lU + mV.$$

It meets $\mathcal{C}$ where

$$(U - V)^3 - 8\gamma^3 UV(lU + mV) = 0.$$

If the points of intersection are (u_j, v_j, z_j) $(j = 1, 2, 3)$, then

$$\left(\frac{u_1}{v_1}\right)\left(\frac{u_2}{v_2}\right)\left(\frac{u_3}{v_3}\right) = 1.$$

We have the multiplicative group.

Now suppose that C is not a square. Adjoin γ to the ground field, where $\gamma^2 = C$. For a point (x, y, z) on $\mathcal{C}$, put

$$\frac{y + \gamma x}{y - \gamma x} = r + s\gamma \qquad \text{(say)},$$

where

$$r^2 - s^2 C = 1. \qquad (*)$$

We now have a "twisted" multiplication law on (*). Compare the multiplication of the complex numbers $x + iy$ with $x^2 + y^2 = 1$.

[7] We shall not require the details about this case in later work.

Note for the Cognoscenti. In characteristic 2 the curve

$$\mathcal{C} : \quad Y^2Z = X^3 + AXZ^2 + BZ^3$$

is always singular. Write the equation as

$$(Y^2 - BZ^2)Z = X(X^2 + AZ^2).$$

Over a finite (or, more generally, a perfect) field, we have

$$B = \beta^2, \qquad A = \alpha^2$$

for some α, β. Then the curve is

$$(Y + \beta Z)^2 Z = X(X + \alpha Z)^2;$$

which is clearly singular.

If the ground field is not perfect, we may have an example of a singularity defined over an inseparable extension, compare footnote in §6.