Seminar on Elliptic Curves

Cubic curves

Silvio Barandun & Florian Held

ETH Zürich

29th September 2020

Table of contents

1. Introduction

2. Weierstrass Normal Form

3. Explicit Formulas for the Group Law

Introduction

Introduction

Projective space

- The complex projective plane $\mathbb{P}^2$ is $\mathbb{C}^3 \setminus \{0\}$ mod $x \quad x; \quad 2\ \mathbb{C}$
- Equivalence classes are denoted by $[x : y : z]$ for $x; y; z\ 2\ \mathbb{C}$
- $\mathbb{C}^2$, ! $\mathbb{P}^2$ by $(x; y)$ 7! $[x : y : 1]$
- Polynomial in $\mathbb{P}^2$ need to be homogeneous:

$$aX^3 + bY + c\ 2\ \mathbb{C}[X; Y] \quad \text{becomes} \quad aX^3 + bYZ^2 + cZ^3\ 2\ \mathbb{C}[X; Y; Z]$$

Introduction

Definition (Cubic curve)

A cubic curve C $\mathbb{P}^2$ is the zero set of a polynomial of degree three in three variables.

- General form

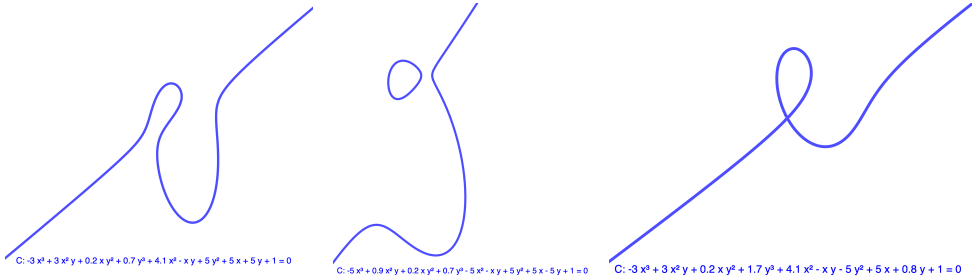
$$C : aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0:$$

  for some $a; b; c; d; e; f; g; h; i; j \ 2$ C.
- Projective space is important for later results. We will jump between $\mathbb{C}^2$ and $\mathbb{P}^2$

Introduction

Some examples

Remark that picture show the real point of the curves



(a) (b) (c)

Figure: Some examples of cubic curves

Towards a group law

First binary operation

We define by $\grave{}(P;Q)$ the line joining P and Q
Let C be a cubic curve

$$: C \quad C \; ! \; C$$
$$(P;Q) \; 7! \; P \quad Q = \grave{}(P;Q) \setminus C \quad fP;Qg$$

Well-defined:

One element $\grave{}(P;Q) \setminus C$ is a system of a linear and a cubic equation, so has three solutions in P^2 with multiplicity!

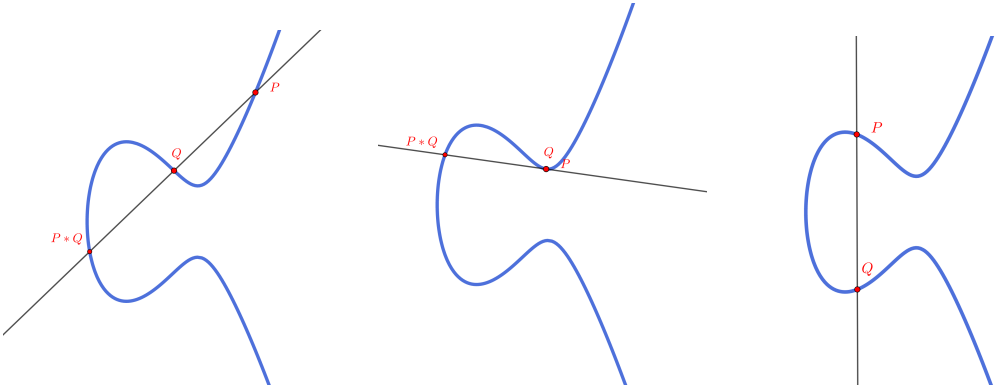
$P \quad P$ $\grave{}(P;P)$ is the tangent to C at P

Duplicates We do allow duplicates in the notation: $fA;B;Bg \quad fA;Bg = fBg$

Note that sends rational points to rational points.

$P \quad Q$

Some examples



(a) General (b) Tangent (c) Need of P^2

Figure: Some examples of $P \quad Q$

Towards a group law

Geometry

Let C be a cubic curve and $e \in C$ a point on it. We define the binary operation

$$\begin{aligned} + : C \quad C &\to C \\ (P, Q) &\mapsto e \quad (P \quad Q) \end{aligned}$$

A group law

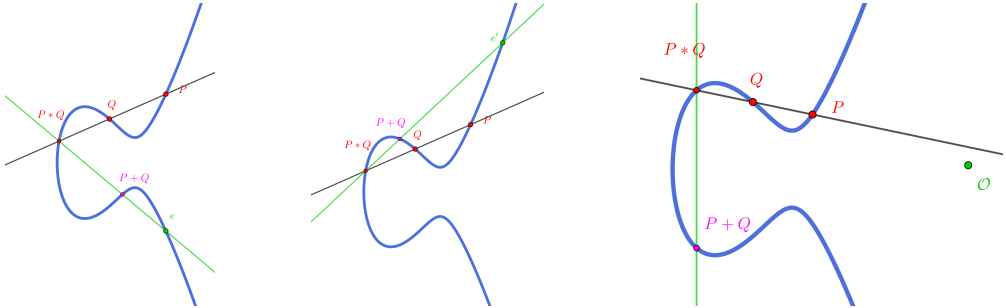
Lemma

Let C be a cubic curve and $e \in C$ a point on it. Then $(C; e; +)$ forms an abelian group.

- Convention: $(C; O; +)$ for $O = [0 : 1 : 0]$ is not a loss of generality

A group law

Some examples



(a) $P + Q$ (b) $P +' Q$ (c) $P +_{\text{std}} Q$

Figure: Some examples of $P + Q$ for di erent e's

Proof

Easy part

Well-de ned: Follows from well-de niteness of

Commutativity: `(P; Q) = `(Q; P), so P Q = Q P. Thus P + Q = Q + P

Proof

Example Commutativity

Figure: Commutativity

Proof

Easy part

Well-de ned: Follows from well-de niteness of

Commutativity: `(P;Q) = `(Q;P), so P Q = Q P. Thus P + Q = Q + P

O: Notice that `(P;O) = f P;O;P Og impliesO (P O) = P

P: Idea: P = P (O O) di cult to picture since it's in [x : y : 0].

Proof

ExampleO

Figure: Neutral element $\mathcal{O}$

Preliminary results

Lemma (Bezout)

Let $C_1; C_2$ be two cubics (in $\mathbb{P}^2$) having no irreducible components in common. Then C_1 and C_2 intersect in nine points counting multiplicity.

Proposition (Intersection points of cubics)

Let $C; C_1; C_2$ be three cubics (in $\mathbb{P}^2$). If C goes through eight of the nine intersection points of C_1 and C_2 then C goes through the ninth intersection point as well.

Proof

Tedious part

Associativity: Really just a sketch here.

Enough to show
$\grave{}(Q; P + R) \setminus \grave{}(R; P + Q) \quad C$
$\grave{}(O; P + Q); \grave{}(P; R); \grave{}(Q; P + R)$
$\grave{}(O; P + R); \grave{}(P; Q); \grave{}(R; P + Q)$ give us six linear equation two cubics C_1 and C_2

By Proposition C goes through the nine points $C_1 \setminus C_2$, so we're done.

Figure: Associativity

Weierstrass Normal Form

Motivation

The question of rational points on conics is solved (Capter 1.1) example of the unit circle:

Figure: Projection from $(0;1)$ to the line $y = 1$

Motivation

To work with rational points on a elliptic curve we bring it into an easier form while keeping track of it's rational points. The general form

$$C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0:$$

becomes

$$C^0 : y^2 = x^3 + a^0x^2 + b^0x + c^0$$

with all coe cients in C

Motivation

Visual example of a transformation

Figure: $x^3 + y^3$ $a = 0$ and it's transformed $y^2 = x^3 - 432a^2$ for $a = 0.047304$

The projective transformation

We need to work in the projective plane $\mathbb{P}^2$ and thus change to homogeneous coordinates

We assume a rational Point O, that the curve is non singular and choose new ax depending on O

The projective transformation

with new axes the cubic takes the form

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

after multiplying by x, a renaming xy as y' and completing the square we arrive a
the desired form

Transforming $x^3 + y^3 \quad a = 0$ into the normal form leads to $y^2 = x^3 \quad 432a^2$

De nition of elliptic curve

De nition (Elliptic curve)

A cubic curve of the form $y^2 = f(x) = x^3 + ax^2 + bx + c$ is called elliptic curve if f has distinct roots. A general cubic curve is called elliptic if it's transform into Weierstras normal form is an elliptic curve.

Note that being non-singular is equivalent to having distinct roots.

A visual tour of elliptic curves

Figure: curves of the form $y^2 = x^3 + ax + b$

About singular cubics

Why do elliptic curves only include non-singular cubics?

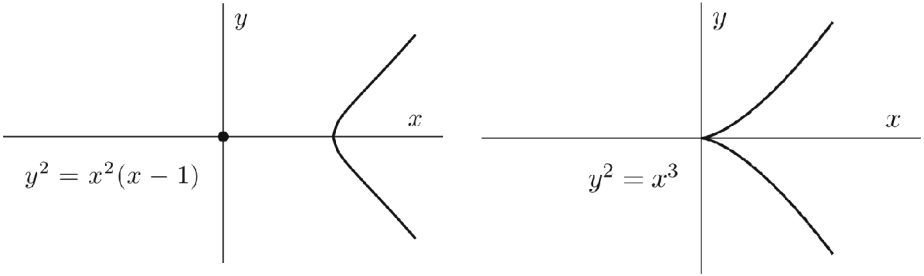


Figure: singular cubics with double and triple root

Explicit Formulas for the Group Law

The cubic we work with

- Weierstrass makes life easier
- We will work with cubics of the form

$$C^{\emptyset} : Y^2 = X^3 + aX^2 + bX + c \quad ! \quad Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

- $Z = 0$ leads $X^3 = 0$ so the only point at infinity is $O = [0 : 1 : 0]$!
- Geometrical observations:
  - Every line meets C in exactly three points
  - C is symmetric with respect to $Y = 0$, in particular vertical lines meet C twice in C^2 one once in O.
  - In particular for $P = (x_1; x_2)$ we get $P = (x_1; \quad x_2)$.

Weierstrass cubic

Starting point

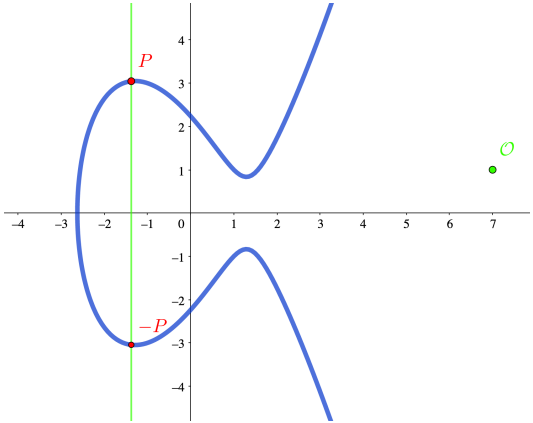


Figure: Weierstrass cubic and P

Derivation of the explicit Formula

Part 1

- Let $P_1 = (x_1; y_1)$, $P_2 = (x_2; y_2)$ and let's denote $P_1 \quad P_2 = (x_3; y_3)$, $P_1 + P_2 = (x_3; \quad y_3)$
- $`(P_1; P_2) = f(x; y) : y = \quad x + \quad)g$ with $\quad = \frac{y_2 \quad y_1}{x_2 \quad x_1}$ and $\quad = y_1 \qquad x_1$.
- $C \setminus `(P_1; P_2)$:

$$Y^2 = (\quad X + \quad)^2 = X^3 + aX^2 + bX + c$$
$$(\ ) \quad 0 = X^3 + (a \qquad ^2)X^2 + (b \quad 2 \quad)X + (c \qquad ^2)$$

- The three roots of this polynomial must be $x_1; x_2; x_3$:

$$X^3 + (a \qquad ^2)X^2 + (b \quad 2 \quad)X + (c \qquad ^2) = (X \quad x_1)(X \quad x_2)(X \quad x_3)$$

Derivation of the explicit Formula

Part 2

$$X^3 + (a \quad ^2)X^2 + (b \quad 2 \quad)X + (c \quad ^2) = (X \quad x_1)(X \quad x_2)(X \quad x_3)$$

- $a \quad ^2 = \quad x_1 \quad x_2 \quad x_3$, $x_3 = \quad ^2 \quad a \quad x_1 \quad x_2$ but also $y_3 = \quad x_3 +$

$$(x_1; y_1) + (x_2; y_2) = \quad ^2 \quad a \quad x_1 \quad x_2; \quad (\quad ^2 \quad a \quad x_1 \quad x_2)$$

with $= \frac{y_2 \quad y_1}{x_2 \quad x_1}$ and $= y_1 \quad x_1$

Derivation of the explicit Formula

Reality check

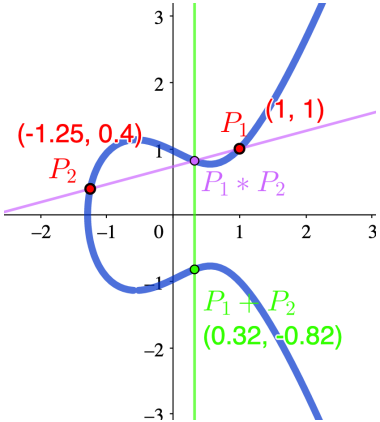


Figure: Concrete example of $P_1 + P_2$

$$= \frac{1127}{1200} \quad P_1 = (1;1) \quad P_2 = \quad \frac{5}{4}; \frac{2}{5}$$

$$C : Y^2 = X^3 \quad X +$$

$$= \frac{\frac{2}{5} \quad 1}{\frac{5}{4} \quad 1} = \frac{4}{15}$$

$$= 1 \quad \frac{4}{15} = \frac{11}{15}$$

$$x_3 = \frac{4^2}{15^2} \quad 1 + \frac{5}{4} = \frac{289}{900} = 0{:}32\overline{1}$$

$$y_3 = \frac{2674}{3375} = 0{:}818\overline{962}$$

The duplication formula

For adding a point P to itself the formula from before doesn't work, that is the reason for choosing as the slope of the tangent at P on the curve. With the same calculation as before we get:

$$\text{Let } 2(x;y) = (x;y) + (x;y) = (x';y')$$

Then:

$$(x';y') = \quad ^2 \quad a \quad 2x; \quad (\quad ^2 \quad a \quad 2x)$$

Where

$$= \frac{f'(x)}{2y} \text{ and } \quad = y \qquad x$$

The duplication formula

And more explicitly: $x' =$

$$\frac{x^4 \quad 2bx^2 \quad 8cx + b^2 \quad 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

And: $y' =$

$$\frac{x^6 + 2ax^5 + 5bx^4 + 20cx^3 + (20ac \quad 5b^2)x^2 + (8a^2c \quad 2ab^2 \quad 4bc)x + 4abc \quad b^3 \quad 8c^2}{8y^3}$$

References I

[1] *Elliptic curve*. https://en.wikipedia.org/wiki/Elliptic_curve. Accessed: 2020-09-25.

[2] *How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form*. https://web.archive.org/web/20200928185302/https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/Matsuura-projective_transformation.pdf. Accessed: 2020-09-28.

[3] Trinity Mecklenburg. *Elliptic Curves*. https://scholarworks.lib.csusb.edu/etd/186. Accessed: 2020-09-25.

[4] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 2015.