Cubic Curves

Luciana Marconi and Mara Mittelholzer

3. October 2023

Contents

1 Introduction to cubic curves

In this section we will give an introduction to cubic curves and show that it exists a group law for these objects.

1.1 Definitions and notation

Definition 1.1. *A **cubic curve** in the plane is the zero set of a polynomial of degree three in two variables. A general cubic curve is of the form*

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \qquad (1)$$

*where $a, b, c, d, e, f, g, h, i, j \in \mathbb{C}$. We say that a cubic curve is **rational** if the coefficients of its equation are rational numbers.*

Definition 1.2. *A **homogeneous** polynomial is a polynomial in three variables whose nonzero terms have all the same degree. We will use the convention to write a polynomial with lowercase variables and its homogeneous form with uppercase variables. So, the equation (1) becomes*

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

Example 1.3. *A famous example for a cubic is*

$$x^3 + y^3 = 1$$

or in its homogeneous form $X^3 + Y^3 = Z^3$.

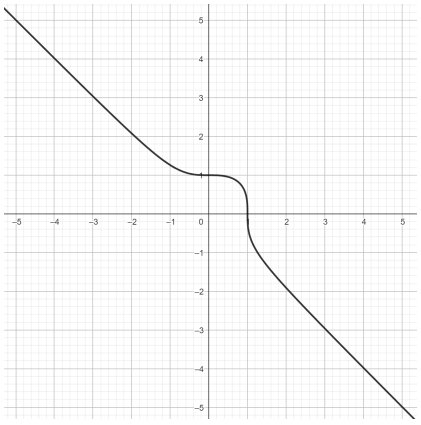

Figure 1: Example of a cubic curve : $x^3 + y^3 = 1$ from [3].

Definition 1.4. *Let C be a cubic curve. Let*

$$\begin{array}{rccc} * : & C \times C & \to & C \\ & (P, Q) & \mapsto & P * Q \end{array}$$

*define the **composition of two points** on C. It is intuitively correct, that a line meets the cubic three times counted with multiplicity. So, $P * Q$ is defined as the third intersection point on C of the line going through P and Q.*

We want to have a closer look at the composition of all points of a cubic curve, that is why we introduced the above general Definition 1.4. Later in this seminar one will focus particularly on the rational points of a rational cubic curve. However this general Definition 1.4 restricted on the rational points will still be well-defined (see Theorem 1.5).
Note, that there is no known method that is guaranteed to determine, in a finite number of steps, whether a given rational cubic has a rational point. Hence its existence is always just assumed in this script.

Theorem 1.5. *The composition $*$ is a well-defined operation on $C(\mathbb{Q})$, the set of all rational points on a rational cubic curve.*

Proof. Since the line connecting P and Q is a rational line that intersects with a rational cubic the three intersection points are the roots of a cubic equation with rational coefficients. Since two roots are rational per assumption the third intersection point $P * Q$ must be rational too.
Also, if you take the tangent line of a rational point P you can think of it as going twice through the point P and $P * P$ will be again a rational point.
□

Remark 1.6. *Repeating $*$ on more rational points and its intersection point will generate more rational points. So, one of the goals of this seminar will be to prove* ***Mordell's Theorem*** *that states the following:*
If C is a non-singular rational cubic curve, then there is a finite set of rational points such that all other rational points can be obtained by repeatedly drawing lines and taking intersections.

Theorem 1.7. *Introducing two properties that are going to be useful later on:*

- *(Bezout's theorem). Two cubic curves always meet in nine points.*
- *Let C, C_1 and C_2 be cubic curves. Suppose that C goes through eight of nine intersection points of C_1 and C_2. Then C must also go through the ninth intersection point.*

For Bezout's Theorem you can find the proof in Appendix $A.4$ of [1]. The proof of the second property is available in Chapter 1.2 (page 10f.) of [1].

1.2 Group structure of C

Unfortunately, $(C, *)$ does not form a group, since we can not find an identity element. But we can define another operation that satisfies the group axioms.

Definition 1.8. *Let C be a cubic curve and $\mathcal{O} \in C$ a point on it. We define the binary operation as*

$$\begin{array}{rccc} + : & C \times C & \to & C \\ & (P, Q) & \mapsto & \mathcal{O} * (P * Q) \end{array}$$

where $*$ denotes the composition defined in Definition 1.4. The operation is illustrated in Figure 2. [1]

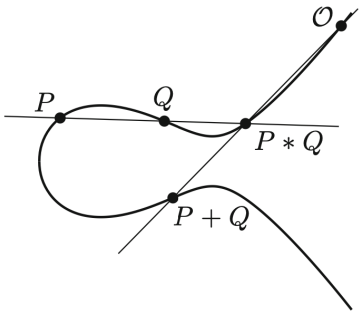

Figure 2: The + operation on C.

We will show in section 3 that this operation is well-defined by giving an explicit formula for it.

Theorem 1.9. *Let C be a cubic curve and $\mathcal{O} \in C$ a point on it. Then $(C, \mathcal{O}, +)$ is an abelian group.*

Proof. Commutativity: It is easy to see that + is commutative. Since the line through P and Q is the same as the line through Q and P, it follows $P * Q = Q * P$. So it also holds

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P.$$

Identity Element: Given $P \in C$, the line through P and $\mathcal{O}$ intersects C in the points $P, \mathcal{O}$ and $P * \mathcal{O}$. So it follows that the third point on the intersection of C and the line through $P * \mathcal{O}$ and $\mathcal{O}$ must be P. Since P was arbitrary and by the commutativity it holds that $\mathcal{O}$ is the identity element, i.e.

$$\forall P \in C : P + \mathcal{O} = \mathcal{O} + P = P.$$

In Figure 3 we can see geometrically that $\mathcal{O}$ acts as the identity element.

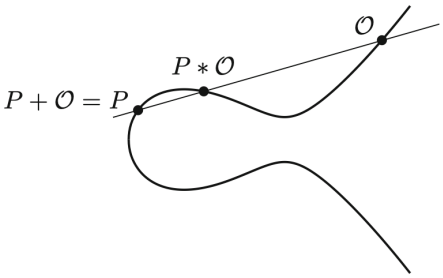

Figure 3: $\mathcal{O}$ acts as the identity element.

Inverse elements: We can construct the inverse of an arbitrary $Q \in C$ as follows (see Figure 4): Let S be the additional point on the intersection of C and the

[1] If no other sources are given, the Figures are from [1].

tangent line to the cubic on $\mathcal{O}$, i.e. $S = \mathcal{O} * \mathcal{O}$. Then we join Q and S and we claim that

$$-Q = Q * S = Q * (\mathcal{O} * \mathcal{O}).$$

It is easy to check this claim:

$$\begin{aligned} Q + (-Q) &= \mathcal{O} * (Q * (-Q)) \\ &= \mathcal{O} * S \\ &= \mathcal{O} \end{aligned}$$

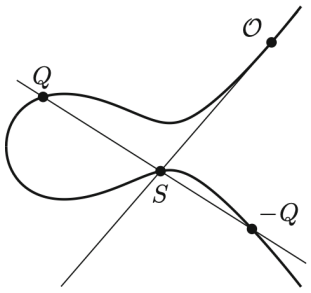

Figure 4: Construction of an inverse element.

Associativity: Let $P, Q, R \in C$. We have to show that

$$(P + Q) + R = P + (Q + R).$$

Claim (without proof): It suffices for the associativity to show that

$$(P + Q) * R = P * (Q + R).$$

So, we only need to show that the equality $(P + Q) * R = P * (Q + R)$ holds: To get $(P + Q) * R$, first construct $P * Q$ and then take the third intersection point of the line going through $P * Q$ and $\mathcal{O}$. Then take the line going through $P + Q$ and R. Similarly, for $P * (Q + R)$ you construct $Q * R$ and $Q + R$.
Now, as seen in the picture 5 each of these points

$$\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R, Q + R \in C$$

lies on one of the dashed and one of the solid lines. If we consider the dashed lines as three linear equations, by multiplying them together, we get a cubic equation with the solution set being the union of the three dashed lines. The same holds for the three solid lines. So, now there are two cubic curves that intersect in the eight listed points plus one point, denoted as X in the picture. The goal is to show that their last intersection also lies on the original cubic curve C. We apply the second property of Theorem 1.7 and take for C_1 the union of the three dashed and for C_2 the union of the three solid lines. As seen before, C goes through the eight listed points above and so it follows that X the intersection of the two highlighted lines must lie on C as well. Hence it follows that $(P + Q) * R = P * (Q + R)$.

□

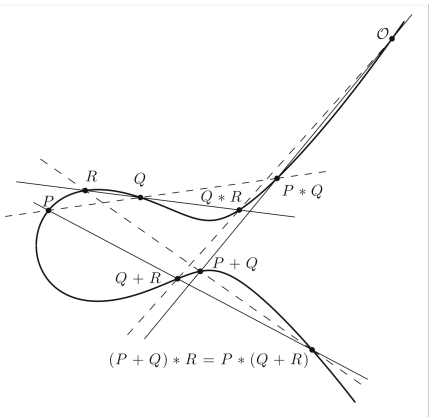

Figure 5: Sketch to visualize the associativity of $+$.

Remark 1.10. *As seen in Theorem 1.9, $(C, \mathcal{O}, +)$ forms an abelian group for any $\mathcal{O} \in C$. Choosing any other $\mathcal{O}' \in C$ as the identity element results in a new group $(C, \mathcal{O}', +')$ with the same structure as before. Specifically, the map*

$$\begin{array}{lll} (C, \mathcal{O}, +) & \to & (C, \mathcal{O}', +') \\ P & \mapsto & P + \mathcal{O}' \end{array}$$

is an isomorphism with the following new addition law:

$$P +' Q := P + Q - \mathcal{O}'.$$

2 Weierstrass normal form and singularities

Later in this script we want to give an explicit formula for the addition operation. To get a formula that is as simple as possible we will introduce now the Weierstrass normal form.

2.1 Weierstrass normal form

Definition 2.1. *A cubic is in **Weierstrass normal form** if it is of the form*

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

with $a, b, c \in \mathbb{C}$.

We want to find an algorithm that transforms a general cubic into Weierstrass normal form. This allows us to later just focus on curves in this normal form.

Now we sketch the way how the transformation works. We start with a cubic curve C in the projective plane (see section 3.1) and assume that there is an element $\mathcal{O} \in C$ which is rational and C is non-singular. Then we are proceed as follows:

1. Change the coordinates such that $\mathcal{O}$ lies at the point $[1, 0, 0]$.

2. Find the tangent T_1 of C at $\mathcal{O}$ and change the coordinates such that T_1 is the line where $Z = 0$ holds.

3. Let $Q = \mathcal{O} * \mathcal{O}$ (we assume $Q \neq \mathcal{O}$). Then find the tangent T_2 of C at Q. Change the coordinates again such that T_2 is the line where $X = 0$ holds.

4. Take any line T_3 that goes through $\mathcal{O}$ such that $T_3 \neq T_1$ and change the coordinates such that T_3 is the line where $Y = 0$ holds.

An illustration of the first 4 steps is shown in Figure 6.

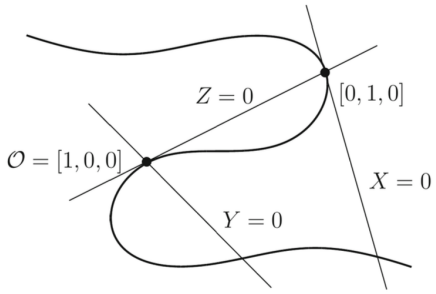

Figure 6: First steps of the transformation.

5. Choose the axes as described in the steps 1 to 4 and define

$$x = \frac{X}{Z} \quad \text{and} \quad y = \frac{Y}{Z}.$$

6. Without working out the details we tell you that at the end the equation for C takes the form

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

Multiply with x and get

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex.$$

Renaming xy as y gives

$$y^2 + (ax + b)y = cx^3 + dx^2 + ex.$$

Replace y by $y - \frac{1}{2}(ax + b)$ to get

$$y^2 = \text{ cubic in } x.$$

7. In case that λ, the leading coefficient of the cubic in x, is not 1, we can replace x and y by λx and $\lambda^2 y$ and divide by λ^4 to get a normal form. If one wants to get rid of the x^2 term in the cubic, replace x by $x - \alpha$ for an appropriate choice of α.

Now we have a sketch of how to transform a general cubic equation into Weierstrass normal form. Since the transformation of the coordinates and its inverse are rational functions, there is a bijection of the rational points on the general cubic and on its Weierstrass normal form. So the problem of finding rational points on the initial form of C is the same as finding the rational points on the Weierstrass normal form of C. Since the transformation is a group homomorphism, the group structures of a cubic curve and its transform are not the same but connected through the transformation.

There is an example of a transformation of a cubic in Appendix B of [1].

Definition 2.2. *A cubic curve of the form $y^2 = f(x) = x^3 + ax^2 + bx + c$ is called an **elliptic curve** if $f(x)$ has distinct roots. A general cubic curve is called an elliptic curve if its transform into the Weierstrass normal form is an elliptic curve.*

Remark 2.3. *An important remark is that for any curve of the form $y^2 = f(x) = x^3 + ax^2 + bx + c$, $f(x)$ having distinct roots is equivalent to the curve being non-singular. Look at the examples in Figure 7 to get an idea how curves in Weierstrass normal form look like. They all have the form $y^2 = x^3 + ax + b$ and one can easily see that the case $a = b = 0$ has a singularity and is therefore not an elliptic curve. All the other examples are elliptic curves.*

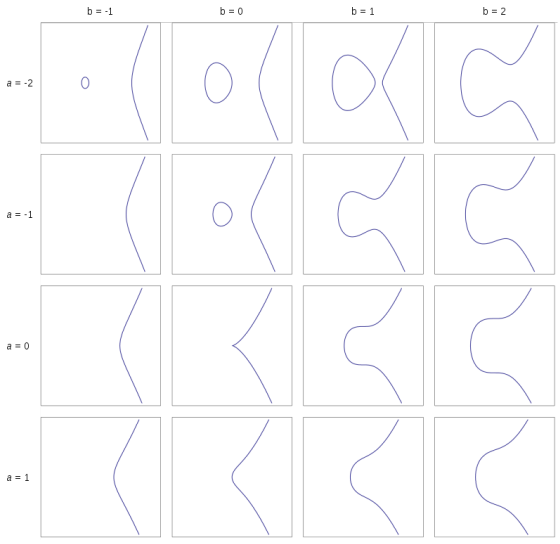

Figure 7: Cubic curves of the form $y^2 = x^3 + ax + b$ from [2].

2.2 Singular cubics

As mentioned in the last section, singular cubes are excluded in the definition of elliptic curves. But why do we distinguish between these two cases? This comes from the fact that singular cubics and non-singular cubics have different

behaviours. Studying rational points on a singular cubic is much easyer than studying rational points on a non-singular cubic, as we will see in this section.

There are three possible pictures of singular cubics which depend on whether f has a double root or triple root. In case that f has a double root, the typical equations are

$$y^2 = x^2(x+1) \quad \text{and} \quad y^2 = x^2(x-1).$$

They are illustrated in the Figures 8 and 9. If f has a triple root, then we consider the equation (see Figure 10)

$$y^2 = x^3.$$

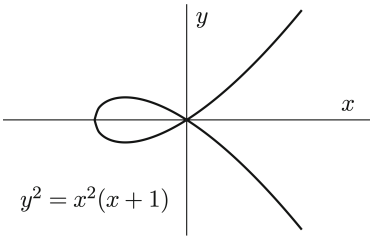

Figure 8: A singular cubic with distinct tangent directions.

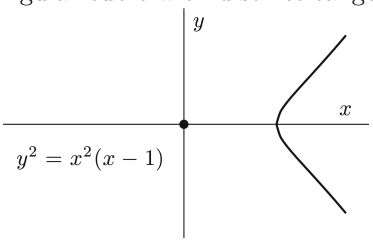

Figure 9: A singular cubic with an isolated singular point.

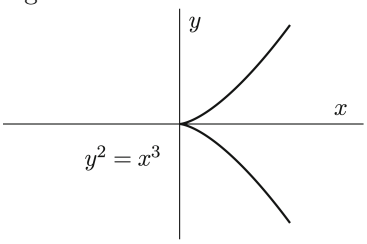

Figure 10: A singular cubic with a cusp.

Rational points on singular cubics are trivial to analyse:
If we look at the singular cubic $y^2 = x^2(x+1)$ and let $r = \frac{y}{x}$, then we get

$$r^2 = x + 1$$

and from this follows

$$x = r^2 - 1 \quad \text{and} \quad y = r^3 - r.$$

So if r is any rational number, then we obtain a rational point (x, y) on the cubic with these equations. And also the other way around, if we first have a rational point $(x, y) \neq (0, 0)$ on the cubic, we will get a rational number $r = \frac{y}{x}$. These functions are inverses of each other and defined for all points but the singularity $(0, 0)$. This is how we get all rational points on the curve.
Analogously, we can find similar equations for $y^2 = x^2(x - 1)$ with $r = \frac{y}{x}$:

$$x = r^2 + 1 \quad \text{and} \quad y = r^3 + r.$$

The curve $y^2 = x^3$ is even simpler to describe, take

$$x = t^2 \quad \text{and} \quad y = t^3.$$

The rational solutions of $y^2 = x^3$ are exactly of the form (t^2, t^3) for $t \in \mathbb{Q}$.

3 Explicit Formulas for the Group Law

3.1 The projective plane

For now, we will focus on points on a non-singular cubic curve. First start with the Weierstrass normal form

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

Now, to describe an explicit formula for the addition law, we need to introduce the projective plane. This will be done, by giving an intuitive understanding of the projective plane (see Figure 11). The projective plane is a regular plane with one additional line added to it. To us, only one point, denoted as $\mathcal{O}$, is important: It is the point where all vertical (to x) lines will "meet" at infinity. The point $\mathcal{O}$ is non-singular and is counted as a rational point belonging to the given cubic curve C. As the notation suggests, we will take the point $\mathcal{O}$ as the identity element of the group $(C, \mathcal{O}, +)$.

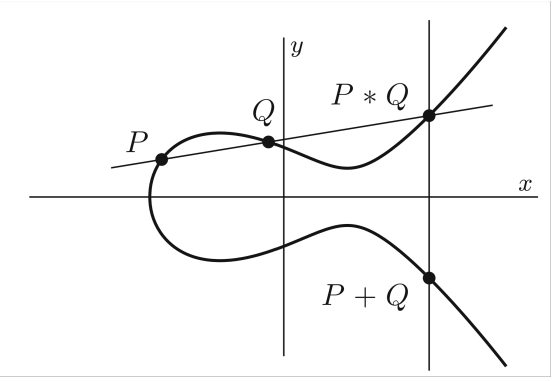

Figure 11: intuitive sketch of the projective plane

(For those who would like a more rigorous definition of the projective plane are asked to look at the first two sections of Appendix A of [1].)
The projective plane visualizes well that every line meets the cubic in three points:

- (Special case.) The line at infinity meets the cubic at the point $\mathcal{O}$ three times.
- The lines vertical to the x-axis go through the cubic twice and once through the point $\mathcal{O}$.
- The lines non-vertical to the x-axis go through the cubic in the regular plane three times.
- The lines that meet the cubic in complex points will be excluded for now.

3.2 The addition formula for distinct points in Weierstrass form

The geometrical idea of the addition in Weierstrass form is equal to the one introduced at the beginning for an arbitrary cubic curve (see Definition 1.8). Note that the sum of two points P, Q is easier to compute since a cubic curve in Weierstrass form is symmetric about the x-axis. Hence after having the intersection point $P * Q$ you just reflect it about the x-axis.
Similarly, to find the negative point $-P$ of a given point P you just reflect it about the x-axis.

3.3 Explicit formula to compute $P + Q$

To efficiently develop an explicit formula, the points on a given cubic curve C need to be written as coordinates: Set

$$P = (x_1, y_1), \quad Q = (x_2, y_2), \quad P * Q = (x_3, y_3).$$

It follows from Subsection 3.2 that $P + Q = (x_3, -y_3)$, the point that we want to compute. Now assume that $(x_1, y_1), (x_2, y_2)$ are given.

1. Look at the equation of the line joining (x_1, y_1) to (x_2, y_2):

$$y = \lambda x + \nu, \text{ where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

2. To get the third intersection point of the line with the cubic curve C, substitute $y = \lambda x + \nu$ into the equation (in Weierstrass form) of the curve:

$$(\lambda x + \nu)^2 = y^2 = x^3 + ax^2 + bx + c.$$

3. Rearranging everything and because a cubic equation has three roots, it follows:

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

4. Comparing the coefficients of the x^2 terms on either side results in:

$$a - \lambda^2 = -x_1 - x_2 - x_3.$$

5. Hence the following explicit formula for $P + Q$ holds:

$$P + Q = (x_3, y_3) = (\lambda^2 - a - x_1 - x_2, -(\lambda x_3 + \nu)).$$

3.4 The duplication formula

Now we want to focus on the special case $P + Q$ where $P = Q$ and we define $2P := P + P$.

We can not calculate the line through P and P as in section 3.3, since λ is not well-defined in this case. Instead, we take the tangent to C at $P = (x_0, y_0)$. From the relation $y^2 = f(x)$ we get

$$\lambda = \frac{dy}{dx}\Big|_{P=(x_0,y_0)} = \frac{f'(x_0)}{2y_0}$$

The tangent has then the form $y = \lambda x + \nu$, where $\nu = y_0 - \lambda x_0$.

The same calculation as before leads to

$$2(x_0, y_0) = (x_0, y_0) + (x_0, y_0) = (\lambda^2 - a - 2x_0, -\lambda(\lambda^2 - a - 2x_0) - \nu).$$

By plugging in the terms for λ and ν and using the relation $y_0^2 = f(x_0)$ we get

$$x - \text{coordinate of } 2(x_0, y_0) = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}.$$

We can do the same for $y' =$ the $y-$coordinate of $2(x_0, y_0)$:

$$y' = \frac{x_0^6 + 2ax_0^5 + 5bx_0^4 + 20cx_0^3 + (20ac - 5b^2)x_0^2 + (8a^2c - 2ab^2 - 4bc)x_0 + 4abc - b^3 - 8c^2)}{8y_0^3}.$$

These formulas can be used to prove some facts about rational points on cubic curves, for example in the proof of Mordell's Theorem.

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] Tos Wikipedia user, *Elliptic curve*, URL: `https://en.wikipedia.org/wiki/Elliptic_curve`.

[3] Geogebra user, URL: `https://www.geogebra.org/calculator`