Introduction to Elliptic Curves

Proving the group law of elliptic curves using the Riemann–Roch's theorem

Sirawit Pongnakintr, under the supervision of Prof. Diego Izquierdo

December 14, 2023

Bachelor of Science, École Polytechnique

Table of contents

The goal of this journey!

To prove the group law of elliptic curves using the Riemann–Roch theorem.

The goal of this journey!

To prove the group law of elliptic curves using the Riemann–Roch theorem.

Expected duration: 20 minutes

Notation

We use K to denote a field. We assume that K is perfect, i.e. all algebraic extensions of K are separable. However, we don't assume that K is algebraically closed. We denote by $\overline{K}$ the algebraic closure of K.

If we're working on dimension n, we denote by $\mathbb{A}^n$ the affine space of $\overline{K}$ of dimension n, i.e. $\mathbb{A}^n = \overline{K}^n$.

$\mathbb{P}^n$ will be the projective space of dimension n.[1]

[1] We will not go through the rigorous description here since there is no time. See appendix for details.

Curves

Algebraic set

Given a set S of polynomials in $\bar{K}[x_1, \ldots, x_n]$ and let I be the ideal generated by S. We define the (affine) algebraic set of I to be the set

$$V_I := \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

This is a subset of $\mathbb{A}^n$.

Example

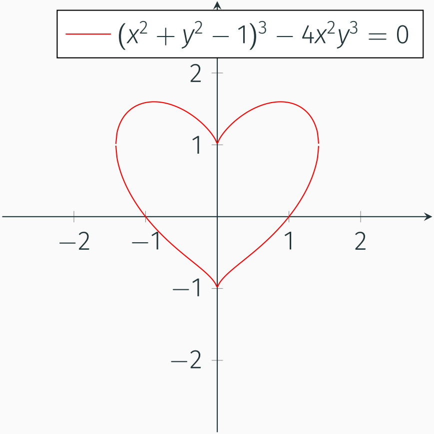


Figure 1: An affine algebraic set

Curve

A curve is a projective variety of dimension one.

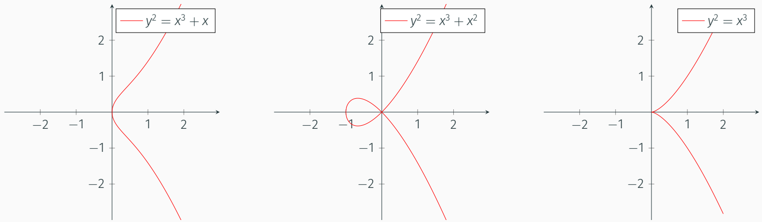


Figure 2: Curves defined as projective closures of affine algebraic sets in $\mathbb{R}^2$

Note that this doesn't mean every curve is defined on $\mathbb{P}^1$. One can define a projective variety on $\mathbb{P}^n$ that has dimension one, and that would also count as a curve.

Note

Note that here, we'll not consider the notion of "curves" in its full generality since we will not have time to go through the concept of projective set, algebraic variety, dimension and smoothness.

For now, we consider affine algebraic set that "looks like dimension one", and note that it can be extended to a projective algebraic set.

Things that are not curves!

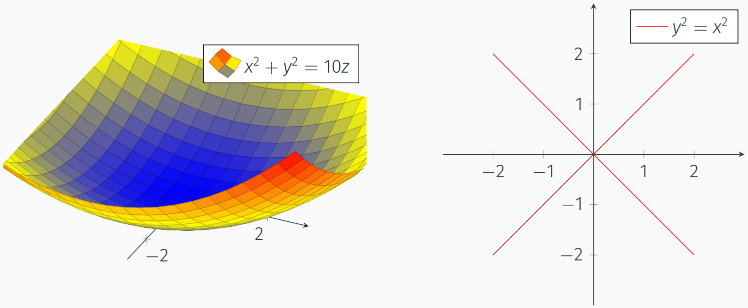


Figure 3: A surface, and an algebraic set whose ideal is not prime

The coordinate ring

For an affine variety $V \subseteq \mathbb{A}^n$, we have the affine coordinate ring:

$$\overline{K}[V] := \overline{K}[X_1, \ldots, X_n]/I(V),$$

Its function field:

$$\overline{K}(V) := \mathrm{Frac}(\overline{K}[V]).$$

Example

Suppose V is defined from the polynomial $(x^2 + y^2 - 1)^3 - 4x^2y^3 = 0$.

Then, in $\overline{K}[V]$, one sees that $(x^2 + y^2 - 1)^3$ and $4x^2y^3$ are the same object.

Analogue: p-adic valuation

The set $\mathbb{Z}$ can be localized at any prime ideal (p) as

$$\mathbb{Z}_{(p)} := \{a/b \colon a, b \in \mathbb{Z}, b \notin (p)\}.$$

Then one can observe that (p) is the unique maximal ideal in $\mathbb{Z}_{(p)}$, so there is the following natural valuation

$$\nu \colon \begin{cases} \mathbb{Z}_{(p)} & \to \mathbb{N} \cup \{\infty\} \\ x & \mapsto \max\{n \in \mathbb{N} \cup \{\infty\} \colon x \in (p)^n\}. \end{cases}$$

This is the usual p-adic valuation, i.e. if $p = 3$ then $\nu(18) = \nu(3 \cdot 3 \cdot 2) = 2$, $\nu(7) = 0$, $\nu(75) = 1$, etc.

One can extend this to $\mathrm{Frac}(\mathbb{Z}_{(p)}) = \mathbb{Q}$ as $\nu(a/b) = \nu(a) - \nu(b)$ for all $a, b \in \mathbb{Z}_{(p)}$. It is not hard to check that this is well-defined.

Localization at a point

Let C be a curve in $\mathbb{P}^n$, and let $P \in C$ be a point on it. We define the ideal M_P as

$$M_P := \{f \in \bar{K}[V] \colon f(P) = 0\}.$$

It is a maximal ideal because the function

$$\phi\colon \begin{cases} \bar{K}[V]/M_P & \to \bar{K} \\ f & \mapsto f(P) \end{cases}$$

is an isomorphism between a quotient of a ring by an ideal to a field.

Now we can "localize" the coordinate ring as

$$\bar{K}[V]_P := \{F \in \bar{K}(V) \colon F = f/g \text{ for some } f, g \in \bar{K}[V] \text{ with } g(P) \neq 0\}.$$

The discrete valuation

One can check that $\bar{K}[V]_P$ is a principal ideal domain with a unique maximal ideal, which is M_P. (admitted here)

Then, we define the following object, called the order of f at P, denoted by $\mathrm{ord}_P(f)$, defined as the image of the function

$$\mathrm{ord}_P\colon \begin{cases} \bar{K}[V]_P & \to \mathbb{N} \cup \{\infty\} \\ f & \mapsto \max\{n \in \mathbb{N} \cup \{\infty\} : f \in M_P^n\}. \end{cases}$$

at f, with the convention that the maximum of an infinite subset of the naturals is ∞.

One can extend this valuation to $\mathrm{Frac}(\bar{K}[V]_P) = \bar{K}(V)$ as $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$. We can check that it is a well-defined function $\mathrm{ord}_P\colon \bar{K}(V) \to \mathbb{Z} \cup \{\infty\}$.

An example

Consider the curve $y^2 = x^3 + x$. Consider $P = (0, 0)$. The ideal M_P is generated by x and y. The ideal M_P^2 is generated by x^2, xy and y^2, but $x = y^2 - x^3$ so it can be generated by y^2 alone. This also tells us that $y \in M_P$ but $y \notin M_P^2$, so $\mathrm{ord}_P(y) = 1$. Now, consider that

$$2\,\mathrm{ord}_P(y) = \mathrm{ord}_P(y^2) = \mathrm{ord}_P(x^3 + x) = \mathrm{ord}_P(x) + \mathrm{ord}_P(x^2 + 1)$$

but $x^2 + 1$ is nonzero at P, so its order is 0. This means $\mathrm{ord}_P(x) = 2$.

The Riemann–Roch Theorem

Divisors

Let C be a curve. One can define the set $\mathrm{Div}(C)$ to be the set of formal sums

$$\sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$ and there are only finitely many $P \in C$ such that $n_P \neq 0$, and we define its degree to be $\sum_{P \in C} n_P$. Observe that $\mathrm{Div}(C)$ forms an abelian group.

Principal divisors

Let $f \in \overline{K}(C)^*$ then we can define $\mathrm{div}(f)$ to be

$$\sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Observe that the image $H = f(\overline{K}(C)^*)$ makes a (normal) subgroup of $\mathrm{Div}(C)$. We then define $\mathrm{Pic}(C) := \mathrm{Div}(C)/H$. We also define the equivalence relation $\sim$, and say $D_1 \sim D_2$ whenever $D_1 - D_2 \in H$.

Div^0 and Pic^0

Proposition 1 (admitted here)

Let C be a curve and let $f \in \overline{K}(C)^*$.

- $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}$.
- $\deg(\mathrm{div}(f)) = 0$.

We denote by $\mathrm{Div}^0(C)$ the subgroup of $\mathrm{Div}(C)$ with elements of degree 0. Similarly, $\mathrm{Pic}^0(C)$ is the subgroup of $\mathrm{Pic}(C)$ where each divisor in each equivalence class of $\mathrm{Pic}(C)$ has degree zero. The degree is the same in each divisor class due to this proposition.

Differentials

For any $f \in \bar{K}(C)$, we write $\mathrm{d}f$ as a symbol. Now one can impose the following equivalence

- $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$ for all $x, y \in \bar{K}(C)$,
- $\mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x$ for all $x, y \in \bar{K}(C)$,
- $\mathrm{d}a = 0$ for all $a \in \bar{K}$.

The set of those symbols modulo this equivalence is denoted by Ω_C, and is called the space of (meromorphic) differential forms on C.

Proposition 2

Ω_C is a 1-dimensional $\bar{K}(C)$-vector space. (admitted here)

Divisor of a differential

Proposition 3 (admitted here)

Let $P \in C$ and let t be a uniformizer at P. For every $\omega \in \Omega_C$, there exists a unique $g \in \bar{K}(C)$ depending on ω and t such that

$$\omega = g\mathrm{d}t.$$

However, the quantity $\mathrm{ord}_P(g)$ is the same for different g defined from different uniformizers t. We call this quantity the order of ω at P and denote it by $\mathrm{ord}_P(\omega)$.

Furthermore, for a fixed $\omega \in \Omega_C$, the quantity $\mathrm{ord}_P(\omega)$ is nonzero for finitely many $P \in C$.

Definition 4

For any $\omega \in \Omega_C$, we define $\mathrm{div}(\omega)$ to be the formal sum

$$\sum_{P \in C} \mathrm{ord}_P(\omega)(P).$$

The canonical divisor class

Since Ω_C is one-dimensional, for any $\omega_1, \omega_2 \in \Omega_C \setminus \{0\}$, there exists $g \in \bar{K}(C)$ such that $\omega_1 = g\omega_2$. This means

$$\mathrm{div}(\omega_1) = \mathrm{div}(g\omega_2) = \mathrm{div}(g) + \mathrm{div}(\omega_2).$$

That is, $\mathrm{div}(\omega_1)$ and $\mathrm{div}(\omega_2)$ belong to the same class in $\mathrm{Pic}(C)$.

Any divisor in this class is called a canonical divisor. Later on, we will denote by K_C any canonical divisor.

A partial order on divisors

Let $D = \sum_{P \in C} n_P(P)$ be a divisor on a curve C. We say that D is positive and write $D \geq 0$ if $n_P \geq 0$ for all $P \in C$.

We extend this partial order and say $D_1 \leq D_2$ whenever $D_2 - D_1 \geq 0$.

Consider the following vector space defined for any divisor $D \in \mathrm{Div}(C)$:

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \ \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Then $\mathcal{L}(D)$ is a finite dimensional $\overline{K}$-vector space (admitted here). Its dimension is denoted by $\ell(D)$.

The main theorem of Riemann–Roch

The original question before the Riemann–Roch theorem was about determining $\ell(D)$ from a given D. Riemann came up with the inequality

$$\ell(D) \geq \deg D - g + 1$$

where there is a constant g that makes this true for all $D \in \mathrm{Div}(C)$.

After that, Roch finished the inequality, giving us the celebrated main theorem as follows.

Theorem 5 (Riemann–Roch theorem)

Let C be a smooth curve and let K_C be a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every $D \in \mathrm{Div}(C)$,

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Riemann–Roch toolbox

Corollary 6

- $\ell(K_C) = g$.
- $\deg K_C = 2g - 2$.
- *If* $\deg D > 2g - 2$ *then* $\ell(D) = \deg D - g + 1$.

This can be easily proved using different substitutions for D in the Riemann–Roch theorem.

Elliptic Curves

Before going to elliptic curves, let us admit the following useful result.

Theorem 7 (admitted here)

The following are equivalent.

- *C is isomorphic to $\mathbb{P}^1$.*
- *C has genus 0.*
- *There exists distinct points $P, Q \in C$ such that $(P) \sim (Q)$.*

Smooth curves of genus one with a specified base point

For now, we define elliptic curves as smooth curves of genus one with a specified base point.

Let us prove that in such curve E, we can define a group law on its points which is isomorphic to $\mathrm{Pic}^0(E)$.

Proposition 8

Let C be a smooth curve of genus one with a specified base point P_0*. For all* $P, Q \in C$ *there exists a unique* $R \in C$ *such that* $(P) + (Q) \sim (R) + (P_0)$*. We denote this point R by* $\sigma_{P_0}(P, Q)$*.*

Proof

Proof.

- Define $D = (P) + (Q) - (P_0)$. Since it has degree 1, one can apply the Riemann–Roch toolbox to see that $\ell(D) = \deg D - g + 1 = 1$.

Proof.

- Define $D = (P) + (Q) - (P_0)$. Since it has degree 1, one can apply the Riemann–Roch toolbox to see that $\ell(D) = \deg D - g + 1 = 1$.
- Pick an element $f \in \mathcal{L}(D) \setminus \{0\}$. By definition, $\mathrm{div}(f) \geq -D$, so $\mathrm{div}(f)$ can be written as $(P_0) - (P) - (Q) + D'$ for some positive divisor D'.

Proof

Proof.

- Define $D = (P) + (Q) - (P_0)$. Since it has degree 1, one can apply the Riemann–Roch toolbox to see that $\ell(D) = \deg D - g + 1 = 1$.
- Pick an element $f \in \mathcal{L}(D) \setminus \{0\}$. By definition, $\mathrm{div}(f) \geq -D$, so $\mathrm{div}(f)$ can be written as $(P_0) - (P) - (Q) + D'$ for some positive divisor D'.
- Since $\deg \mathrm{div}(f) = 0$, the quantity $\deg D'$ must be 1, so $D' = (R)$ for some $R \in C$. This proves the existence.

Proof.

- Define $D = (P) + (Q) - (P_0)$. Since it has degree 1, one can apply the Riemann–Roch toolbox to see that $\ell(D) = \deg D - g + 1 = 1$.
- Pick an element $f \in \mathcal{L}(D) \setminus \{0\}$. By definition, $\mathrm{div}(f) \geq -D$, so $\mathrm{div}(f)$ can be written as $(P_0) - (P) - (Q) + D'$ for some positive divisor D'.
- Since $\deg \mathrm{div}(f) = 0$, the quantity $\deg D'$ must be 1, so $D' = (R)$ for some $R \in C$. This proves the existence.
- Now suppose there are $R_1, R_2 \in C$ such that $(P) + (Q) \sim (R_1) + (P_0) \sim (R_2) + (P_0)$ then $(R_1) \sim (R_2)$. If $R_1 \neq R_2$ then the curve has genus 0, a contradiction.

Proof

Proof.

- Define $D = (P) + (Q) - (P_0)$. Since it has degree 1, one can apply the Riemann–Roch toolbox to see that $\ell(D) = \deg D - g + 1 = 1$.
- Pick an element $f \in \mathcal{L}(D) \setminus \{0\}$. By definition, $\mathrm{div}(f) \geq -D$, so $\mathrm{div}(f)$ can be written as $(P_0) - (P) - (Q) + D'$ for some positive divisor D'.
- Since $\deg \mathrm{div}(f) = 0$, the quantity $\deg D'$ must be 1, so $D' = (R)$ for some $R \in C$. This proves the existence.
- Now suppose there are $R_1, R_2 \in C$ such that $(P) + (Q) \sim (R_1) + (P_0) \sim (R_2) + (P_0)$ then $(R_1) \sim (R_2)$. If $R_1 \neq R_2$ then the curve has genus 0, a contradiction.
- Therefore, $R_1 = R_2$. This proves the uniqueness.

□

Proposition 9

For a smooth curve C of genus one, for any $P_0 \in C$ one can turn C into an abelian group with the group operation being σ_{P_0}.

Proof.

Let us only prove the associativity here (the rest will be in the appendix). Let $P, Q, R \in C$ and let us show that $\sigma_{P_0}(\sigma_{P_0}(P, Q), R) = \sigma_{P_0}(P, \sigma_{P_0}(Q, R))$. Let $S = \sigma_{P_0}(Q, R)$, $T = \sigma_{P_0}(P, S)$, $U = \sigma_{P_0}(P, Q)$, and $V = \sigma_{P_0}(U, R)$. We have

$$(Q) + (R) \sim (S) + (P_0)$$
$$(P) + (S) \sim (T) + (P_0)$$
$$(P) + (Q) \sim (U) + (P_0)$$
$$(U) + (R) \sim (V) + (P_0).$$

Therefore, $(P) + (Q) + (R) \sim (V) + 2(P_0) \sim (T) + 2(P_0)$, i.e. $(V) \sim (T)$. Hence, $V = T$. □

It is actually $\mathrm{Pic}^0(C)$!

Proposition 10

For a smooth curve C of genus one and any $P_0 \in C$, the group (C, σ_{P_0}) is isomorphic to $(\mathrm{Pic}^0(C), +)$.

Proof.

Define

$$\kappa\colon \begin{cases} C & \to \mathrm{Pic}^0(C) \\ P & \mapsto [(P) - (P_0)]_{\sim}. \end{cases}$$

It is not hard to show that κ is a group isomorphism. $\square$

Conclusion

This proves that for an elliptic curve C, $\mathrm{Pic}^0(C)$ gives a group structure to C.

Furthermore, this algebraic group law also coincides with the geometric group law.

Geometric group law

Consider the following figure, visualized on $\mathbb{R}^2$.

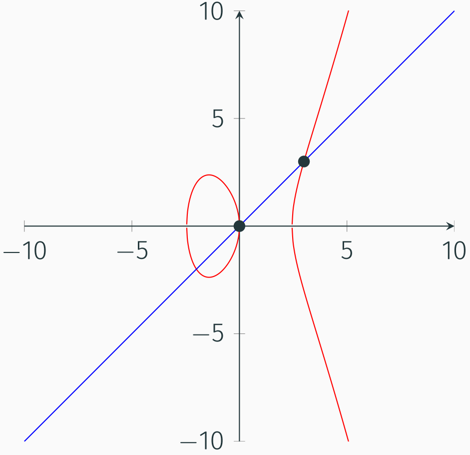


Figure 4: An elliptic curve with two specified points an a line passing through them

A visualization

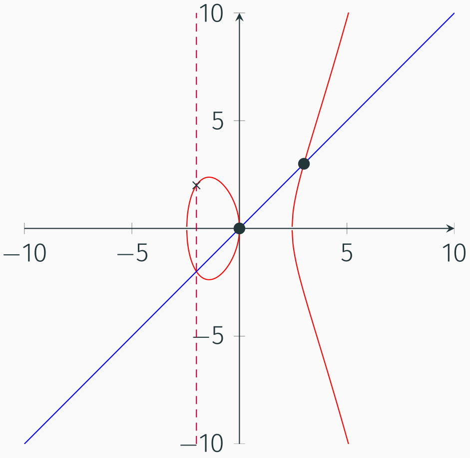


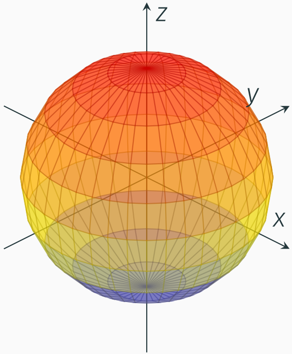
Figure 5: An elliptic curve with two specified points an a line passing through them, where O is the point at infinity. The sum of the two black dots is denoted by $\times$ at $(-2, 2)$.

References

- Gregoric, Rok (2020). ***Baby's first Riemann–Roch.*** URL: https://web.ma.utexas.edu/users/gregoric/Baby's%20Riemann-Roch.pdf.
- Hartshorne, Robin (1977). ***Algebraic Geometry.*** Springer New York. ISBN: 9781475738490. DOI: 10.1007/978-1-4757-3849-0. URL: http://dx.doi.org/10.1007/978-1-4757-3849-0.
- Silverman, Joseph H. (2009). ***The Arithmetic of Elliptic Curves.*** Springer New York. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

Appendix

Projective Space



Projective Geometry

Formally, we define $\mathbb{P}^n(K)$ as the quotient of $\mathbb{A}^{n+1}(K) \setminus \{0\}$ by the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \text{ if and only if there exists } \lambda \in K \text{ such that } x_i = \lambda y_i \text{ for all } i \in \{0, \ldots, n\}.$$

Note that we denote this equivalence class by $[x_0, \ldots, x_n]$, and also note that $[0, \ldots, 0] \notin \mathbb{P}^n$!

Example

Consider the polynomial f defined by $f(x, y) = x^2 + y^2 - 1$.

Examples of homogenization

Example

Consider the polynomial f defined by $f(x, y) = x^2 + y^2 - 1$.

Its homogenized form is $f^*(X, Y, Z) = X^2 + Y^2 - Z^2$.

Example

Consider the polynomial f defined by $f(x, y) = y^2 - x^3 - 17$.

Examples of homogenization

Example

Consider the polynomial f defined by $f(x, y) = x^2 + y^2 - 1$.

Its homogenized form is $f^*(X, Y, Z) = X^2 + Y^2 - Z^2$.

Example

Consider the polynomial f defined by $f(x, y) = y^2 - x^3 - 17$.

Its homogenized form is $f^*(X, Y, Z) = Y^2Z - X^3 - 17Z^3$.

Ideal of an algebraic set

For a given algebraic set $V \subseteq \mathbb{A}^n$, the set

$$I(V) := \{f \in \overline{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V\}$$

forms an ideal. We call this ideal the ideal of V.

If this ideal is prime, then we say that V is a variety.

Varieties generated by a single polynomial

We admit the following result.

Theorem 11

Let $f \in \overline{K}[x_1, \ldots, x_n]$ be irreducible and let I be the ideal generated by f. Then V_I is an algebraic variety of dimension $n - 1$.

The converse is also true, i.e., any algebraic variety of dimension $n - 1$ can be expressed as a variety generated by an ideal generated by a single polynomial.

Projective closure

Given an irreducible polynomial $f \in \bar{K}[x_1, \ldots, x_n]$, we can homogenize it to $f^* \in \bar{K}[x_0, \ldots, x_n]$ so that we can define a projective variety $\bar{V}_{(f)} := \{P \in \mathbb{P}^n : f^*(P) = 0\}$.

Later on, we often just say "let C be a curve generated by f" instead of going through the details of constructing the projective closure, proving that the ideal is prime, etc.

Identifying some subsets of $\mathbb{P}^n$ with $\mathbb{A}^n$

Consider the projective space $\mathbb{P}^n$. Pick an integer $i \in \{0, \dots n\}$ and consider the subset

$$U_i := \{[x_0, \dots, x_n] \in \mathbb{P}^n : x_i \neq 0\}.$$

One can explicitly identify U_i with $\mathbb{A}^n$ by the bijection ϕ defined as

$$\phi\colon \begin{cases} U_i & \to \mathbb{A}^n \\ [x_0, \dots, x_n] & \mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right) \end{cases}$$

Homogenizing an equation

If we have an equation, say, $y^2 = x^3 + 17$, defined in $\mathbb{A}^2(K)$. We can *homogenize* it into $Y^2Z = X^3 + 17Z^3$, which is defined in $\mathbb{P}^2(K)$.

Procedurally, if we have a function $f \in K[X_1, \ldots, X_n]$. The homogenization is

$$(x_0, \ldots, x_n) \mapsto x_i^{\deg f} f\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

For the function $f(x, y) := y^2 - x^3 - 17$, the homogenization with respect to z, written as f^*, is

$$(x, y, z) \mapsto z^3 f\left(\frac{x}{z}, \frac{y}{z}\right) = z^3\left(\frac{y^2}{z^2} - \frac{x^3}{z^3} - 17\right) = y^2z - x^3 - 17z^3.$$

This gives the equation $f^*(X, Y, Z) = 0$, i.e. $Y^2Z = X^3 + 17Z^3$.

Remark

Note that for any $\lambda \in K^*$, $f^*(X, Y, Z) = 0$ holds if and only if $f^*(\lambda X, \lambda Y, \lambda Z) = 0$. This makes f^* well-defined in $\mathbb{P}^n(K)$.

From an affine polynomial $f \in K[x_1, \ldots, x_n]$, one can use this process to define f^* so that the solution to $f(P) = 0$ injects into the set of solutions to $f^*(P) = 0$. This gives a projective closure of an algebraic set.

We define

$$U_i := \{[x_0, \ldots, x_n] \in \mathbb{P}^n \colon x_i \neq 0\}$$

and we may identify U_i with $\mathbb{A}^n$ by the bijection ϕ defined as

$$\phi\colon \begin{cases} U_i & \to \mathbb{A}^n \\ [x_0, \ldots, x_n] & \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right). \end{cases}$$

If $V \subseteq \mathbb{P}^n$ is a projective variety, then one can choose one of U_i's such that $U_i \cap V \neq \emptyset$ and consider the affine subset $\widetilde{V} := \phi(V \cap U_i)$[2].

Then we define $\overline{K}[V]$ and $\overline{K}(V)$ to be $\overline{K}[\widetilde{V}]$ and $\overline{K}(\widetilde{V})$, respectively.

[2] Note that $\widetilde{V}$ is not a standard notation.

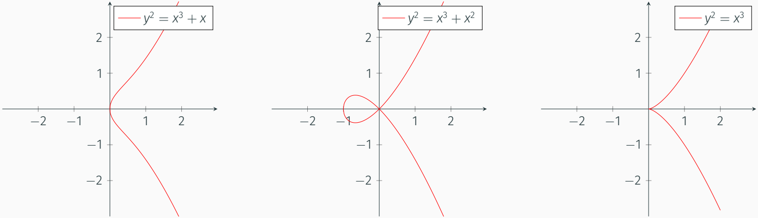
Useful properties

The valuation enjoys the following useful properties. (admitted here)

- For all $f, g \in \bar{K}(V)$, $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$.
- For all $f, g \in \bar{K}(V)$, $\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f) + \mathrm{ord}_P(g))$.
- For all $f, g \in \bar{K}(V)$, if $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$ then $\mathrm{ord}_P(f+g) = \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$.
- For all $f \in \bar{K}(V)$, $\mathrm{ord}_P(f) = \infty$ if and only if $f = 0$.
- There exists an element $t \in \bar{K}(V)$ such that $\mathrm{ord}_P(t) = 1$. We call this element the uniformizer at P.

Smooth curves

Recall figure 1:



At the origin, in the last two curves, the tangent is not well-defined. This motivates the notion of smoothness.

For the special case of curves defined by a single polynomial $f \in \overline{K}[x_1, \ldots, x_n]$, we say that a point P is singular or non-smooth if

$$\partial_{x_1} f(P) = \partial_{x_2} f(P) = \cdots = \partial_{x_n} f(P) = 0.$$

And we say it is smooth or nonsingular otherwise. A curve is smooth if every point is smooth.

Proof that σ_{P_0} is an abelian group law

We proved that it is associative. We're left with proving commutativity, identity, and inverse.

Proof.

(Commutativity) It is obvious that $\sigma_{P_0}(P, Q) = \sigma_{P_0}(Q, P)$ by definition of σ_{P_0} and the commutativity of divisors.

(Identity) Let $P \in C$ and let $Q = \sigma_{P_0}(P, P_0)$. By definition, $(P) + (P_0) \sim (Q) + (P_0)$ so $P = Q$. This proves that P_0 is neutral.

(Inverse) Let $P \in C$. Consider another structure σ_P and let $Q = \sigma_P(P_0, P_0)$. Then, by definition, $(P_0) + (P_0) \sim (Q) + (P)$. Therefore, $\sigma_{P_0}(P, Q) = P_0$ due to uniqueness of the solution. Therefore, Q is an inverse of P for σ_{P_0}.

This completes the proof. □

Proof that κ is a group isomorphism

Proof.

First, we can obviously see that κ is injective because if $(P) - (P_0) \sim (Q) - (P_0)$ then $P = Q$ (using the fact that the genus is one).

Now, suppose $[D]_\sim \in \mathrm{Pic}^0(C)$, then define $D' = D + (P_0)$ and apply the Riemann–Roch toolbox to see that $\ell(D') = 1$. Pick any $f \in \mathcal{L}(D') \setminus \{0\}$ and observe that $\mathrm{div}(f) \geq -D - (P_0)$. But $\deg \mathrm{div}(f) = 0$ so $\mathrm{div}(f)$ must be $-D - (P_0) + (P)$ for some $P \in C$. This means $D \sim (P) - (P_0)$, i.e. $\kappa(P) = [D]_\sim$. This proves the surjectivity.

Now, observe that for all $P, Q \in C$,

$$\kappa(\sigma_{P_0}(P,Q)) = [\sigma_{P_0}(P,Q) - (P_0)]_\sim = [(P) + (Q) - 2(P_0)]_\sim = \kappa(P) + \kappa(Q).$$

This proves that κ is a homomorphism.

This completes the proof. $\square$

A line hits three points

We consider the special case of the smooth curve $C \subseteq \mathbb{P}^2$ defined from an equation giving algebraic set in $\mathbb{A}^2$ and taking the projective closure.

Given any two points P, Q (not necessarily distinct) on C, there exists a unique line that pass through them (if $P = Q$, this is not unique, and we impose this line to be tangent to C), and this line hits C at exactly three points (counting multiplicity and points at infinity).

The point other than P and Q that is hit by this line is called $P \star Q$. We now join the point $P \star Q$ with the base point P_0, and the other point that is hit by this line is now called $P + Q$, i.e. this is the result of the group law on P and Q.

Note that this is made intuitive by visualizing in $\mathbb{R}^2$, but the geometric manipulation gives an algebraic procedure, which can therefore be extended to other field K in general.