

Abel's Theorem

Tobias Schnieders, 19.02.2026

Today, we will get to know *Abel's Theorem*, a very far reaching generalisation of the trigonometric angle sum identities. As a corollary, we will obtain the group law for elliptic curves, a group law that lays the foundations for elliptic curve cryptography.

This introduction is based on [1], [2], [3] and [4].

General prerequisite: Let X be a compact Riemann surface of genus g .

1. The Genus-Degree Formula

Theorem 1.1. *Let $f \in \mathbb{C}[x, y]$ be irreducible. Suppose that $\deg(f) \geq 3$ and that $C_f := \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\} \subseteq \mathbb{P}^2$ is smooth. Denote by g_{C_f} the genus of the Riemann surface C_f defined by f . It holds that*

$$g_{C_f} = \frac{(\deg(f) - 1)(\deg(f) - 2)}{2}.$$

Example 1.2. Consider the polynomial $f := x^3 - y^2 - x$. The real part of its zero locus $C_f \cap \mathbb{R}^2$ is depicted in Figure 1. By Theorem 1.1, it is a Riemann surface of genus $\frac{(3-1)(3-2)}{2} = 1$. In the picture, we can see two connected components. Both are closed rounded curves, the second one is closed at ∞ . We can imagine the Riemann surface C_f to be a donut-like shape passing through the real plane in these two connected components.

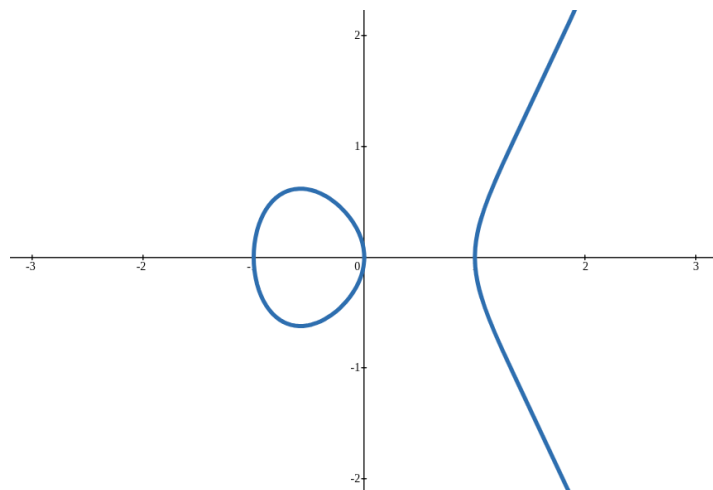


Figure 1: The zero locus of $f = x^3 - y^2 - x$.

2. Divisors

Definition 2.1 (Divisor). A divisor on X is a formal integral linear combination of finitely many points in X , that is a sum of the form

$$\sum_{p \in X} n_p p$$

where $n_p \in \mathbb{Z}$ and at most finitely many n_p are not equal to 0. With formal addition, all divisors on X form an abelian group, which is denoted by $\text{Div}(X)$.

Definition 2.2 (Degree). Let $D = \sum_{p \in X} n_p p$ be a divisor on X . Its degree is given by

$$\deg(D) := \sum_{p \in X} n_p.$$

Remark 2.3. The degree map is a group homomorphism $\text{Div}(X) \rightarrow \mathbb{Z}$.

Definition 2.4. We denote the subgroup of $\text{Div}(X)$ of divisors of degree 0 by

$$\text{Div}_0(X) := \ker(\deg).$$

Definition 2.5 (Principal Divisor). Let $f : X \rightarrow \mathbb{C}$ be a meromorphic function that is not constantly 0. Its divisor, denoted by (f) , is the sum of all zeros of f (with their multiplicities) minus the sum of all poles of f (with their multiplicities).

A divisor D on X is called principal if there exists a meromorphic function $f \neq 0$ such that $(f) = D$. The subgroup of $\text{Div}(X)$ of principal divisors is denoted by $\text{PDiv}(X)$.

Example 2.6. Consider the compact Riemann surface $\mathbb{P}^1 := \mathbb{C} \cup \{\infty\}$ and the meromorphic function $f(x) := \frac{1}{x(x-1)}$. It holds that

$$(f) = -[0] - [1] + 2[\infty].$$

The square brackets around the points in \mathbb{P}^1 are used to distinguish these points from the coefficients. We observe that $\deg((f)) = 0$.

Moreover, we note that every holomorphic function $g : \mathbb{P}^1 \rightarrow \mathbb{C}$ is constant. This is because $g|_{\mathbb{C}} : \mathbb{C} \rightarrow \mathbb{C}$ is a holomorphic and bounded function which is constant by Liouville's theorem.

These two observations are examples of the following theorem.

Theorem 2.7. Every principal divisor on X has degree 0.

Remark 2.8. Using Abel’s theorem, we will find an description of the group $\text{Div}_0(X)/\text{PDiv}(X)$ up to isomorphism.

3. The Abel-Jacobi map

To define the Abel-Jacobi map, we need a few new concepts. These are presented in the following.

Definition 3.1 (Space of Global Holomorphic 1-Forms). *We call*

$$\Omega^1(X) := \{\omega \mid \omega \text{ is a global holomorphic 1-form on } X\}$$

the \mathbb{C} -vector space of global holomorphic 1-forms¹.

Theorem 3.2. *The vector space $\Omega^1(X)$ is finite-dimensional and it holds that*

$$\dim_{\mathbb{C}}(\Omega^1(X)) = g.$$

Example 3.3. Recall the Riemann surface C_f of genus 1 defined by $f := x^3 - y^2 - x$ from Example 1.2. Consider the 1-form $\omega := \frac{dx}{y}$ on $U := C_f \cap \{(x, y) \in \mathbb{C}^2 \mid y \neq 0\}$. Note that ω is holomorphic and non-zero on U . Covering C_f with finitely many open sets like U and transforming ω to these open sets, we find that ω is globally well-defined and everywhere holomorphic and non-zero. Since $\dim_{\mathbb{C}}(\Omega^1(C_f)) = 1$ we obtain

$$\Omega^1(C_f) = \{\lambda\omega \mid \lambda \in \mathbb{C}\}.$$

Remark 3.4. The Abel-Jacobi map will map a point $p \in X$ to the linear form $\omega \mapsto \int_{p_0}^p \omega$ for a fixed base point $p_0 \in X$, however, the codomain of the Abel-Jacobi map cannot be $\Omega^1(X)^*$, because this would be ill-defined, since different paths² in X from p_0 to p may yield different functionals in $\Omega^1(X)^*$. To “fix” this problem, we need to mod out all *closed paths*³.

We observe that $\int_{\gamma} \omega = 0$ for all $\omega \in \Omega^1(X)$ and all *boundary paths*⁴ γ . By the generalised version of Stokes’ theorem, it therefore suffices to mod out $2g$

¹A *global holomorphic 1-form* is a global holomorphic section of the cotangent bundle of X .

²A *path* in X from p_0 to p is a continuous map $\gamma : [0, 1] \rightarrow X$ such that $\gamma(0) = p_0$ and $\gamma(1) = p$.

³A path $\gamma : [0, 1] \rightarrow X$ in X is called *closed* if $\gamma(0) = \gamma(1)$.

⁴Let $\gamma_1, \gamma_2 : [0, 1] \rightarrow X$ be closed paths in X starting at the same point, that is $\gamma_1(0) = \gamma_2(0)$. We can concatenate them as follows $\gamma_1 * \gamma_2 : [0, 1] \rightarrow X : t \mapsto \begin{cases} \gamma_1(2t) & \text{if } t \leq \frac{1}{2} \\ \gamma_2(2t-1) & \text{if } t > \frac{1}{2} \end{cases}$ to obtain another closed path $\gamma_1 * \gamma_2$ in X starting at the same point as γ_1 and γ_2 . This operation turns the set of closed paths starting at a given base point $p_0 \in X$ into a group. A closed path $\gamma : [0, 1] \rightarrow X$ in X is called a *boundary path* if there exists closed paths γ_1 and γ_2 in X starting at $\gamma(0)$ such that γ is homotopic to $\gamma_1 * \gamma_2 * \gamma_1^{-1} * \gamma_2^{-1}$.

independent⁵ closed paths (paths through every handle and around every handle of X) to make the definition well-defined.

Definition 3.5 (Period Lattice). *We call*

$$\Lambda(X) := \left\{ \omega \mapsto \int_{\gamma} \omega \mid \gamma \text{ closed path in } X \right\} \subseteq \Omega^1(X)^*$$

the period lattice of X .

Definition 3.6 (Jacobian). *We call*

$$\text{Jac}(X) := \Omega^1(X)^* / \Lambda(X)$$

the Jacobian of X .

Remark 3.7. Note that $\text{Jac}(X)$ is an abelian group.

Definition 3.8 (Abel-Jacobi map). *Let $p_0 \in X$. The Abel-Jacobi map with respect to p_0 is given by*

$$A_{p_0} : X \rightarrow \text{Jac}(X) : p \mapsto \left(\omega \mapsto \int_{p_0}^p \omega \right)$$

where the integration is taken along any path from p_0 to p .

We can extend this definition to $\text{Div}(X)$ as follows

$$A_{p_0} : \text{Div}(X) \rightarrow \text{Jac}(X) : \sum_{p \in X} n_p p \mapsto \sum_{p \in X} n_p A_{p_0}(p).$$

Theorem 3.9. *Let $p_0, q_0 \in X$ and $D \in \text{Div}_0(X)$. It holds that*

$$A_{p_0}(D) = A_{q_0}(D).$$

Proof. We calculate

⁵To be precise, we mod out a chosen basis of the abelian group, i.e. \mathbb{Z} -module, $H_1(X, \mathbb{Z}) := \{\text{closed paths in } X \text{ starting at } p_0\} / \{\text{boundary paths in } X \text{ starting at } p_0\}$, where $p_0 \in X$ denotes a chosen base point $p_0 \in X$. Also, note that $\dim_{\mathbb{C}}(H_1(X, \mathbb{Z})) = 2g$.

$$\begin{aligned}
A_{p_0}(D) - A_{q_0}(D) &= \sum_{p \in X} n_p A_{p_0}(p) - \sum_{p \in X} n_p A_{q_0}(p) \\
&= \sum_{p \in X} n_p (A_{p_0}(p) - A_{q_0}(p)) \\
&= \sum_{p \in X} n_p \left(\left(\omega \mapsto \int_{p_0}^p \omega \right) - \left(\omega \mapsto \int_{q_0}^p \omega \right) \right) \\
&= \sum_{p \in X} n_p \left(\omega \mapsto \left(\int_{p_0}^p \omega - \int_{q_0}^p \omega \right) \right) \\
&= \underbrace{\left(\sum_{p \in X} n_p \right)}_{=0} \left(\omega \mapsto \int_{p_0}^{q_0} \omega \right) \\
&= 0.
\end{aligned}$$

□

Definition 3.10 (Abel-Jacobi map). *The Abel-Jacobi map is given by*

$$A : \text{Div}_0(X) \rightarrow \text{Jac}(X) : \sum_{p \in X} n_p p \mapsto \sum_{p \in X} n_p A_{p_0}(p)$$

where $p_0 \in X$ is chosen arbitrarily.

Remark 3.11. The Abel-Jacobi map A is a group homomorphism.

4. Abel's Theorem

Theorem 4.1 (Jacobi Inversion). *The Abel-Jacobi map A is surjective.*

Theorem 4.2 (Abel's Theorem). *Let $D \in \text{Div}(X)$. The following are equivalent:*

- (a) D is principal, i.e. there exists a meromorphic $f : X \rightarrow \mathbb{C}$ such that $D = (f)$,
- (b) $\deg(D) = 0$ and $A(D) = 0$.

Corollary 4.3. *It holds that*

$$\text{Div}_0(X) / \text{PDiv}(X) \cong \text{Jac}(X),$$

where the isomorphism is induced by the Abel-Jacobi map A .

5. Explicit Computations

In order to perform explicit computations, we need to choose a basis $\omega_1, \dots, \omega_g$ of $\Omega^1(X)$ and $2g$ closed paths $\alpha_1, \dots, \alpha_g$ (one around each handle of X), and β_1, \dots, β_g (one through each handle of X)⁶ in X .

Definition 5.1 (Big Period Matrix). *The big period matrix of X with respect to $\omega_1, \dots, \omega_g$ and $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ is given by*

$$\Pi := \begin{pmatrix} \int_{\alpha_1} \omega_1 & \dots & \int_{\alpha_g} \omega_1 & \int_{\beta_1} \omega_1 & \dots & \int_{\beta_g} \omega_1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \int_{\alpha_1} \omega_g & \dots & \int_{\alpha_g} \omega_g & \int_{\beta_1} \omega_g & \dots & \int_{\beta_g} \omega_g \end{pmatrix} \in \mathbb{C}^{g \times 2g}.$$

Theorem 5.2. *The submatrices $\Pi_{*,1\dots g}$ and $\Pi_{*,g+1\dots 2g}$ are invertible.*

Definition 5.3 (Small Period Matrix). *The small period matrix of X with respect to $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ is given by*

$$\Pi_{*,1\dots g}^{-1} \Pi_{*,g+1\dots 2g} \in \mathbb{C}^{g \times g}.$$

Remark 5.4. The small period matrix of X with respect to $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ is independent of the choice of the basis of $\Omega^1(X)$.

Theorem 5.5 (Riemann's Bilinear Relations). *The small period matrix of X with respect to $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ is a symmetric matrix with positive definite imaginary part.*

We can use Oscar [5] respectively Hecke [6] to compute big and small period matrices as follows.

Example 5.6. The following code computes a small period matrix of the Riemann surface defined by the polynomial $x^5 + x^4 + x^3 - x + 4 - y^2$.

```
using Oscar, Oscar.Hecke, Oscar.Hecke.RiemannSurfaces
QQxy, (x,y) = polynomial_ring(QQ, ["x", "y"])
f = x^5 + x^4 + x^3 - x + 4 - y^2
RS = RiemannSurface(f)
small_period_matrix(RS)
```

6. The Group Law for Elliptic Curves

Using Abel's theorem, one can prove Corollary 6.3, a characterisation of elliptic curves, from which their group law can be deduced.

⁶More precisely, we choose a smooth basis $(\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g)$ of $H_1(X, \mathbb{Z})$ such that α_i and β_i intersect transversally in precisely 1 point, $\text{im}(\alpha_i) \cap \text{im}(\alpha_j) = \emptyset$ and $\text{im}(\beta_i) \cap \text{im}(\beta_j) = \emptyset$ for all $i, j \in \{1, \dots, g\}$ with $i \neq j$.

Definition 6.1 (Elliptic Curve). An elliptic curve is a compact Riemann surface of genus 1.

Example 6.2. Recall the Riemann surface C_f of genus 1 defined by $f = x^3 - y^2 - x$ from Example 1.2. It is an elliptic curve.

Corollary 6.3. Let $p_0 \in X$. The following are equivalent.

- (a) X is an elliptic curve,
- (b) the Abel-Jacobi map $A_{p_0} : X \rightarrow \text{Jac}(X)$ with respect to p_0 is biholomorphic.

Remark 6.4. Recall that the Jacobian is defined to be a \mathbb{C} -vector space modulo a full-rank lattice. In particular, the Jacobian is an abelian group. Now, let X be an elliptic curve and $p_0 \in X$ be an arbitrary point. By Corollary 6.3, X is an abelian group and p_0 is its neutral element, since

$$A_{p_0}(p_0) = \left(\omega \mapsto \int_{p_0}^{p_0} \omega \right) = (\omega \mapsto 0) = 0.$$

We can also interpret this group structure geometrically as follows. Let $P, Q, E \in X$. To add P and Q on X with respect to the fixed base point, i.e. neutral element, E , we draw the unique line passing through P and Q . This line meets X in a unique third point, which we call $R \in X$. Then we consider the unique line passing through R and E . This line does also meet X in a unique third point, the sum of P and Q with respect to the chosen neutral element E .

Of course, one could also define the group structure on an elliptic curve in this geometric way. However, in that way, it would not be obvious, why the defined operation turns the elliptic curve into an abelian group. Namely, proving associativity is not trivial.

Example 6.5. We consider the polynomial $f := x^3 - y^2 + 1 \in \mathbb{C}[x, y]$. As presented in Theorem 1.1, this defines a Riemann surface $C_f \subseteq \mathbb{P}^2$ of genus 1, that is an elliptic curve. Its real part is depicted in Figure 2.

We consider the base point $E := (0, -1) \in C_f$ and the two points $P := (2, 3) \in C_f$ and $Q := (0, 1) \in C_f$. To add these two points with respect to E , we draw the line through P and Q . This line intersects C_f in P, Q and $R := (-1, 0)$. Then, we draw the line through R and E , which intersects C_f in R, E and $(2, -3)$. Hence, we find

$$P + Q = (2, -3).$$

In this example, it can, furthermore, be proven that E, P, Q, R , and $P + Q$ are the only points $(x, y) \in \mathbb{Q}^2$ such that $f(x, y) = 0$. But this is another story ...

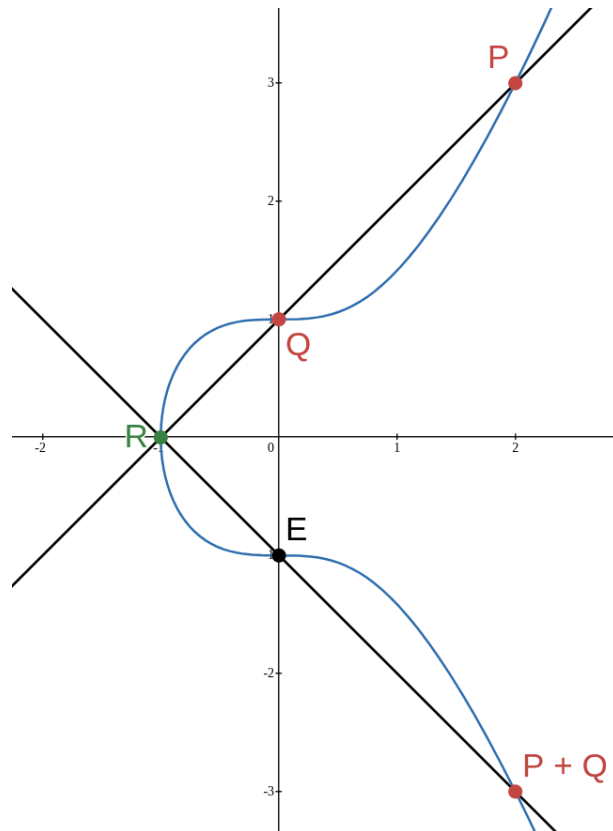


Figure 2: A real picture of the elliptic curve defined by $f = x^3 - y^2 + 1$ together with an addition on this elliptic curve.

7. Bibliography

- [1] A. Gathmann, ‘Algebraic Geometry’. 2003.
- [2] A. Gathmann, ‘Algebraic Geometry’. 2022.
- [3] R. Miranda, *Algebraic curves and Riemann surfaces*, vol. 5. in Grad. Stud. Math., vol. 5. Providence, RI: AMS, American Mathematical Society, 1995.
- [4] I. Radloff, ‘Algebraic curves and Riemann surfaces’. 2025.
- [5] ‘OSCAR – Open Source Computer Algebra Research system, Version 1.6.0’. [Online]. Available: <https://www.oscar-system.org/>
- [6] C. Fieker, W. Hart, T. Hofmann, and F. Johansson, ‘Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language’, in *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, in ISSAC '17. New York, NY, USA: ACM, 2017, pp. 157–164. doi: 10.1145/3087604.3087611.