The Abel-Jacobi map

Robin Visser

Abstract

Let C be a non-singular curve over $\mathbb{C}$. We define the concept of the Jacobian $J(C)$ being an abelian variety associated to the curve C, and give an explicit description of the Abel-Jacobi map from C to $J(C)$ over $\mathbb{C}$. We also study its relation to $\mathrm{Pic}^0(C)$, and finally give a brief overview of some results for $J(C)$ for small genus curves C.

Introduction

Given a curve C over a field k, one of the most studied problems in geometry and number theory is calculating the k-rational points on C. There is no algorithm guaranteed to solve this question in general, however one of the techniques which can often help us in practice is to study the Jacobian $J(C)$ of the curve C.

In this project, we shall briefly discuss some basic properties of the Jacobian, as well as define the Abel-Jacobi map $C \to J(C)$ which gives an embedding of the curve C into its Jacobian if the genus is non-zero. This therefore yields many applications to studying the curve C, just one of which includes obtaining practical algorithms in certain cases to calculating all k-rational points on C.

Preliminaries

There are various ways to define the Jacobian. For completeness, we shall first give a more general functorial definition for the Jacobian, after which we shall specialise to a specific construction which works for the complex numbers $\mathbb{C}$.

Definition 1: [4, p. 85] Let C be a smooth projective curve. Let $\mathbf{Var}_{\mathbb{C}}$ denote the category of varieties[1] over $\mathbb{C}$ and let **Set** denote the category of sets. For any variety T in $\mathbf{Var}_{\mathbb{C}}$, we denote $\mathrm{Pic}^0(T)$ as the *degree 0 Picard group* of T.

We define P_C^0 as the contravariant functor between $\mathbf{Var}_{\mathbb{C}}$ and **Set** given by

$$\begin{aligned} P_C^0 : \mathbf{Var}_{\mathbb{C}} &\longrightarrow \mathbf{Set} \\ T &\longmapsto \frac{\mathrm{Pic}^0(C \times T)}{\mathrm{Pic}^0(T)}. \end{aligned}$$

Furthermore, for any variety J', we define the contravariant functor $h_{J'}$ given by

$$\begin{aligned} h_{J'} : \mathbf{Var}_{\mathbb{C}} &\longrightarrow \mathbf{Set} \\ T &\longmapsto \mathrm{Hom}(T, J'). \end{aligned}$$

We thus define the **Jacobian** $J(C)$ of C as the variety J such that the functor P_C^0 is isomorphic to h_J.[2] We note that J is *unique* (up to isomorphism) by Yoneda's lemma.

[1] Here, we consider varieties in the most general sense, as a topological space covered by finitely many open sets, each of which has the structure of an affine variety. See Milne's notes [4] for a full formal definition.

[2] We remark that this definition is also simply the statement that P_C^0 is *represented* by $J(C)$.

We also remark that this functorial definition can be generalised for any arbitrary base field k, although we note that $J(C)$ may not exist if $C(k) = \emptyset$ [4, p. 86]. For the purposes of this mini-project, we shall only consider the case $k = \mathbb{C}$.

One corollary of the above definition is that the functorial definition of the Jacobian $J(C)$ is isomorphic to $\text{Pic}^0(C)$ and thus $J(C)$ is naturally an abelian variety. However, we note that this definition does not give any explicit construction for $J(C)$. We shall therefore define a construction in the case $k = \mathbb{C}$.

Definition 2: [2, p. 153] Let C be a smooth projective curve of genus g. We note that any such curve can also be considered as a Riemann surface with genus g (a g-holed torus).

Let $\Omega_{\mathbb{C}}(\mathbb{C}(C))$ denote the set of regular differentials on C. We note that this is $\mathbb{C}$-vector space of dimension g [2, p. 102]. Let $\omega_1, \omega_2, \ldots, \omega_g$ be a basis for $\Omega_{\mathbb{C}}(\mathbb{C}(C))$ over $\mathbb{C}$. We now define a lattice $\Lambda \subset \mathbb{C}^g$ generated by integrating over all closed loops on the Riemann surface C, given by

$$\Lambda := \left\{ \Big(\int_\gamma \omega_1, \int_\gamma \omega_2, \ldots, \int_\gamma \omega_g \Big) \;\middle|\; \gamma \text{ is a closed loop on the } g\text{-holed torus } C \right\} \subset \mathbb{C}^g.$$

More specifically, we can also define Λ by explicitly giving a basis. Indeed, note that any closed loop on the corresponding Riemann surface is generated by $2g$ incontractible loops $\gamma_1, \gamma_2, \ldots, \gamma_{2g}$, as shown in Figure 1.

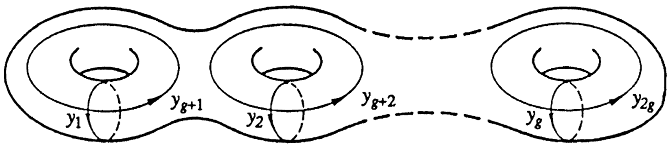

Figure 1: A g-holed torus with incontractible loops $\gamma_1, \gamma_2, \ldots, \gamma_{2g}$ [2, p. 106].

Now for each incontractible loop γ_j, we define π_j as a vector of g values over $\mathbb{C}$, given by

$$\pi_j := \Big(\int_{\gamma_j} \omega_1, \int_{\gamma_j} \omega_2, \ldots, \int_{\gamma_j} \omega_g \Big) \in \mathbb{C}^g$$

One can show that the vectors $\pi_1, \pi_2, \ldots, \pi_{2g}$ are linearly independent over $\mathbb{R}$ [2, p. 111]. Thus, the $2g$ vectors span a lattice in $\mathbb{C}^g$ We therefore note that $\Lambda \subset \mathbb{C}^g$ can be given as

$$\Lambda := \Big\{ \sum_{j=1}^{2g} m_j \pi_j : m_j \in \mathbb{Z} \Big\} \subset \mathbb{C}^g$$

We thus define the **Jacobian** $J(C)$ of C over $\mathbb{C}$ as the g-dimensional complex torus $\mathbb{C}^g/\Lambda$.

We are now ready to define the Abel-Jacobi map.

Definition 3: [2, p. 154] Let C be a smooth projective curve of genus g. As before, let $\omega_1, \omega_2, \ldots, \omega_g$ be a basis for $\Omega_{\mathbb{C}}(\mathbb{C}(C))$ over $\mathbb{C}$. Let P_0 be any arbitrary point on C. We define the **Abel-Jacobi map** as a map from the curve C to its Jacobian $J(C)$ given by

$$\begin{aligned} u : C &\longrightarrow J(C) = \mathbb{C}^g/\Lambda \\ P &\longmapsto \Big(\int_{P_0}^{P} \omega_1, \int_{P_0}^{P} \omega_2, \ldots, \int_{P_0}^{P} \omega_g \Big) \bmod \Lambda \end{aligned} \tag{1}$$

We note that the choice of the base point P_0 is clearly not unique, although choosing a different value for P_0 only changes the Abel-Jacobi map $u : C \to J(C)$ up to translation.

At first sight, the above definition for the Jacobian $J(C)$ for curves C over $\mathbb{C}$ does not bear any resemblance to the functorial definition or to $\mathrm{Pic}^0(C)$. To see that $J(C)$ is indeed an abelian variety isomorphic to $\mathrm{Pic}^0(C)$ as abelian groups, we now state the main theorem for this project.

Theorem 4: [2, p. 155] (*Abel-Jacobi Theorem*) Let C be a smooth projective curve of genus g, and let $u : C \to J(C)$ denote the Abel-Jacobi map as given above. We can extend this map to a map $v : \mathrm{Div}(C) \to J(C)$ on the divisors of C in the natural way, given by

$$\begin{aligned} v : \mathrm{Div}(C) &\longrightarrow J(C) \\ \sum_{P \in C} n_P\,(P) &\longmapsto \sum_{P \in C} n_P\, u(P) \end{aligned}$$

The theorem states that the induced map from $\mathrm{Pic}(C) \to J(C)$ is well-defined, and this furthermore induces an isomorphism $\mathrm{Pic}^0(C) \to J(C)$.

The result that both $\mathrm{Pic}^0(C) \to J(C)$ is well-defined (i.e. that $v(D) = 0$ for $D \in \mathrm{Princ}(C)$) and injective (i.e. if for some $D \in \mathrm{Div}^0(C)$ we have $v(D) = 0$, then D is principal) is usually called *Abel's theorem*. The result that $v : \mathrm{Div}^0(C) \to J(C)$ is surjective is referred to as *Jacobi's inversion theorem*.

Unfortunately, a full proof of the above result is beyond the scope of this miniproject, but can be found in Griffiths [2, p. 156]. Instead, we shall prove some simpler propositions and work through some small genus examples using the above theorem.

Firstly, we note that once we have the above isomorphism between $J(C)$ and $\mathrm{Pic}^0(C)$, we can restate the Abel-Jacobi map as a map from the curve C to $\mathrm{Pic}^0(C)$ given by

$$\begin{aligned} u : C &\longrightarrow \mathrm{Pic}^0(C) \\ P &\longmapsto (P) - (P_0) \end{aligned} \tag{2}$$

We now prove that this map is injective if the genus of C is non-zero.

Lemma 5: Let C be a smooth projective curve of genus $g \geq 1$. Then the Abel-Jacobi map $u : C \hookrightarrow \mathrm{Pic}^0(C)$ is an injective map.

Proof: Assume for contradiction there exist two distinct points P, Q on C such that $(P) - (P_0) \equiv (Q) - (P_0)$ in $\mathrm{Pic}^0(C)$. Therefore, there exists some function $f \in \mathbb{C}(C)$ such that $\mathrm{div}(f) = (P) - (Q)$.

Now considering the degree of the map $f : C \to \mathbb{P}^1$, we note that f has only a single pole at Q. Therefore we obtain that the map $f : C \to \mathbb{P}^1$ has degree 1, and thus $C \cong \mathbb{P}^1$, which implies C has genus 0. This therefore yields a contradiction. □

Note that the above lemma proves that if C is a smooth projective curve of genus $g \geq 1$, then we can embed the curve C in its Jacobian $C \hookrightarrow J(C)$. This therefore motivates studying the Jacobian $J(C)$ which would hopefully yield results about the curve C.

We shall now go through some examples of using the Abel-Jacobi theorem to compute the Jacobian $J(C)$ for various curves C of small genus.

Genus 0

For completeness, we consider the trivial genus 0 case. In the case where the curve C has genus 0, we simply have that $C \cong \mathbb{P}^1$. Since any degree 0 divisor on $\mathbb{P}^1$ is principal, this implies $\mathrm{Pic}^0(C)$ is trivial, and thus the Jacobian $J(C)$ consists of only a single point.

Genus 1

Now let C be a genus 1 curve. Since $\mathbb{C}$ is algebraically closed, we are free to pick any base point P_0 on $C(\mathbb{C})$ and can therefore consider C as an elliptic curve. We shall now prove that the Abel-Jacobi map is an isomorphism for elliptic curves.

Theorem 6: [5, p. 61] Let C be a smooth projective curve of genus 1. Then C is isomorphic to $\mathrm{Pic}^0(C)$.

Proof: Note that we have already proved injectivity in Lemma 5. To prove surjectivity, let $D \in \mathrm{Pic}^0(C)$. Thus $D + (P_0)$ has degree 1. Therefore, by Riemann's theorem, we have that $\ell(D + (P_0)) \geq 1 + 1 - g = 1$.

This implies that there exists some function $f \in \mathbb{C}(C)$ such that $\mathrm{div}(f)+D+(P_0)$ is effective. Furthermore, since the divisor $\mathrm{div}(f) + D + (P_0)$ has degree 1, we therefore must have the existence of some point $P \in C$ such that

$$\mathrm{div}(f) + D + (P_0) = (P).$$

Thus $D \equiv (P) - (P_0)$ which implies $u(P) \equiv D$ and thus for elliptic curves the Abel-Jacobi map is surjective. □

This proves that $C \cong \mathrm{Pic}^0(C)$ which, by the Abel-Jacobi theorem, proves that C is isomorphic to its Jacobian $J(C)$! We note that $\mathrm{Pic}^0(C)$ naturally has the structure of an abelian group, and this therefore induces a natural group law on any elliptic curve C (with respect to some base point P_0). This group law on C can be given by an explicit chord-tangent construction on the curve C, where the full details can be found in Silverman [5, p. 51].

We can also explicitly state the isomorphism between C and $J(C)$ in terms of the first description of the Abel-Jacobi map given in terms of path integrals on the torus $\mathbb{C}/\Lambda$.

Let C be an elliptic curve given in Weierstrass form as $C : y^2 = x^3 + ax + b$. Noting that $\Omega_{\mathbb{C}}(\mathbb{C}(C))$ is a 1-dimensional vector space over $\mathbb{C}$ spanned by $\frac{dx}{y}$ [5, p. 48], we can give the isomorphism between C and $J(C)$ as

$$\begin{aligned} u : C &\longrightarrow J(C) = \mathbb{C}/\Lambda \\ P &\longmapsto \int_{P_0}^{P} \frac{dx}{y} = \int_{P_0}^{P} \frac{dx}{\sqrt{x^3+ax+b}} \mod \Lambda. \end{aligned}$$ [3]

Unfortunately, there isn't much we can do to directly further simplify the integral given above. These are know as *elliptic integrals* and their solutions cannot be expressed directly in terms of elementary functions. We shall simply remark that an inverse to the map described above can be given in terms of the Weierstrass $\wp$-function (relative to Λ) [5, p. 165].

Far more can be said about elliptic integrals and the study of elliptic curves over $\mathbb{C}$. For a more detailed discussion, we refer the interested reader to Silverman, Chapter VI [5, p. 157].

Genus 2

In the genus 1 case, we had the remarkably simple result that the Jacobian $J(C)$ is isomorphic to the curve C itself. In the genus 2 case, we are however not so lucky and no longer have that $C \to J(C)$ is an isomorphism.

---

[3] We remark that there is the small issue of the indeterminacy of the sign in the square root. This is therefore not well-defined as a value in $\mathbb{C}$ but is still well-defined on the torus $\mathbb{C}/\Lambda$.

We can however apply a similar argument done in Theorem 6 using Riemann-Roch for genus 2 curves to obtain some explicit description for the elements in $\mathrm{Pic}^0(C)$. Indeed, let C be a genus 2 curve with hyperelliptic model $y^2 = f(x)$ where $\deg(f) = 5$ and let $i : C \to C$ be the involution map given by $(x, y) \mapsto (x, -y)$. One can prove that every element in $\mathrm{Pic}^0(C)$ can uniquely be represented as

$$(P) + (Q) - 2(\infty)$$

for some unique unordered pair $\{P, Q\}$, with the small exception that all elements of the form $\{P, i(P)\}$ are identified with each other [1, p. 2].

Unfortunately, giving an explicit description of the Jacobian as an abelian variety for an arbitrary genus 2 curve is a highly non-trivial task. It's worth mentioning that Cassels, Flynn [1] gave an explicit construction for the Jacobian of an arbitrary genus 2 curve over k as a smooth projective curve in $\mathbb{P}^{15}$ defined by 72 quadratic forms over k. Explicitly computing $J(C)$ for an arbitrary genus 2 curve is therefore clearly far beyond the scope of this project.

However, we can compute the Jacobian for certain types of genus 2 curves. Indeed, let C be a genus 2 curve given by the equation

$$C : y^2 = Ax^6 + Bx^4 + Cx^2 + D$$

and assume that the discriminant of the polynomial $Ax^6 + Bx^4 + Cx^2 + D$ is non-zero (so that C has genus 2). We can define the elliptic curves E_1 and E_2 given by

$$E_1 : y^2 = Ax^3 + Bx^2 + Cx + D \quad \text{and} \quad E_2 : y^2 = Dx^3 + Cx^2 + Bx + A.$$

Note that we can define non-constant morphisms from C to E_1 and E_2 given by $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto (1/x^2, y/x^3)$ respectively. It's therefore possible to prove that the Jacobian $J(C)$ in this case is simply the product of the above given elliptic curves $J(C) \cong E_1 \times E_2$ [3, p. 45]. In this case, we say that the curve has **split jacobian** [3].[4]

Conclusion

We have only just started to touch the very tip of what Jacobian varieties have to offer. Not only are they of much theoretical interest, but also have many computational applications in cryptography and computer science.

References

[1] Cassels, J., Flynn, E. (1996). *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2* (London Mathematical Society Lecture Note Series). Cambridge: Cambridge University Press.

[2] Griffiths, P. (1989). *Introduction to Algebraic Curves.* Providence, R.I: American Mathematical Society.

[3] Kuhn, R. (1988). *Curves of Genus 2 with Split Jacobian.* Trans. Amer. Math. Soc., Vol. 307, No. 1, pp.41-49.

[4] Milne, J. (2008). *Abelian varieties.* [online] Available at: `https://www.jmilne.org/math/CourseNotes/AV.pdf` [Accessed 19 Dec. 2020].

[5] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* 2nd edition, Springer-Verlag New York.

[4] Furthermore, if one wishes to explicitly define $J(C)$ as a projective variety, we can use the Segre embedding to define $J(C)$ as a projective variety in $\mathbb{P}^8$.