CHAPTER 21

Abel's theorem for elliptic curves

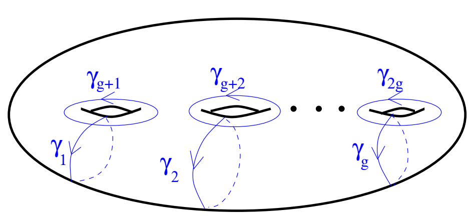
Given a divisor $D = \sum n_i[p_i]$ on an elliptic curve E, we can formally compute the sum in the group law, ending up with a single point on E. It seems of interest to ask if anything special is true if this point is the origin $\mathcal{O}$. In fact, assuming $\sum n_i = 0$, it will turn out that this is true precisely if D is the divisor of a meromorphic function on the curve. We begin by describing the statement of Abel's theorem for a curve of arbitrary genus (which does not have a group law), to place the statement for genus one in a broader context. Then we prove the genus-1 case, introducing theta functions along the way.

21.1. The Jacobian of an algebraic curve

Let M be a Riemann surface of genus g. We will need to accept some facts in order to state Abel's theorem for M. (These will be returned to in later chapters, along with the proof of Abel.) It turns out that the space of holomorphic 1-forms has dimension g, whilst the (abelian) *homology group* of 1-cycles modulo boundaries (cf. §19.1 for definitions) has rank $2g$. In terms of bases,

$$H_1(M, \mathbb{Z}) \cong \mathbb{Z}\left\langle \gamma_1, \ldots, \gamma_{2g} \right\rangle,$$
$$\Omega^1(M) \cong \mathbb{C}\left\langle \omega_1, \ldots, \omega_g \right\rangle.$$

21.1.1. REMARK. A visual "explanation" of the statement about homology groups may be the best one:



Exercises (3)-(4) of Chapter 25 provide a way to write down the holomorphic forms on M, provided one believes that any Riemann surface is the normalization of an algebraic curve C in $\mathbb{P}^2$ whose only singularities (if any) are nodes. (This statement relies on the existence of nonconstant meromorphic functions on M, which is nontrivial.) Since the genus g of M is $\frac{(d-1)(d-2)}{2} - \delta$ (with $d = \deg(C)$, $\delta = \#$ of ODPs), it is enough to show that all meromorphic 1-forms are rational (cf. §25.1) and furthermore that *holomorphic* pullbacks of rational 1-forms from $\mathbb{P}^2$ span a space of dimension $\binom{d-1}{2} - \delta$ (cf. §25.2).

Just to get an idea of how this works, suppose $C = \{F(Z,X,Y) = 0\}$ is *smooth* of degree d, and recall that S_3^m denotes degree-m homogeneous polynomials in 3 variables, with dimension $\binom{m+2}{2}$. If G is a homogeneous polynomial of degree n, write $g(x,y) = G(1,x,y)$ (and similarly $f(x,y) = F(1,x,y)$). Then the meromorphic 1-form on $\mathbb{P}^2$ which in affine coordinates takes the form $\frac{g \cdot dx}{f_y}$, restricts to a holomorphic 1-form on C precisely if[1] $n = d-3$. (This is equivalent to saying $\deg(g) \leq d-3$.) Hence,[2] $\Omega^1(C)$ has dimension $\binom{(d-3)+2}{2} = \binom{d-1}{2} = \frac{(d-1)(d-2)}{2} = g$.

Anyhow, let $\gamma_j \in H_1(M,\mathbb{Z})$ be a basis element; associated to it is a *period vector*

$$\pi_j := \begin{pmatrix} \int_{\gamma_j} \omega_1 \\ \vdots \\ \int_{\gamma_j} \omega_g \end{pmatrix} \in \mathbb{C}^g.$$

Together these form a $g \times 2g$ *period matrix* Π with $\mathbb{R}$-linearly independent columns. (This isn't obvious, and will be addressed in §25.2.) Hence their columns generate (over $\mathbb{Z}$) a $2g$-lattice $\Lambda_M \subset \mathbb{C}^g$ ($\cong \mathbb{R}^{2g}$).

Recall that if V is a vector space (say, over $\mathbb{C}$) then the dual space is the space of linear functions $V^\vee := \mathrm{Hom}(V,\mathbb{C})$.

[1]The computation in the Ch. 25 exercises proving this is "ugly" but straightforward; *Poincaré residues* facilitate a conceptual and essentially 1-line proof (but at the cost of more sophisticated machinery).

[2]putting off to §25.2 that this formula encompasses *all* rational holomorphic forms.

21.1.2. DEFINITION. The *Jacobian* of M is the abelian group

$$J(M) := \frac{\left(\Omega^1(M)\right)^\vee}{\text{image}\,\{H_1(M,\mathbb{Z})\}},$$

where the denominator means the linear functions on $\Omega^1(M)$ obtained by integrating $\omega \in \Omega^1(M)$ over 1-cycles. Evaluation of linear functions against the basis $\{\omega_1, \ldots, \omega_g\}$ induces an isomorphism

$$J(M) \xrightarrow{\cong} \frac{\mathbb{C}^g}{\Lambda_M}\ ;$$

that is, the Jacobian is a complex g-torus.

21.1.3. LEMMA. *Any morphism* $\varphi\colon \mathbb{P}^1 \to \mathbb{C}^g/\Lambda_M$ *of complex manifolds is constant.*

PROOF. Writing $u_1, \ldots, u_g$ for the coordinates on $\mathbb{C}^g$, the g-torus $\mathbb{C}^g/\Lambda_M$ has g independent holomorphic 1-forms: $du_1, \ldots, du_g$. Since $\varphi^*(du_i) \in \Omega^1(\mathbb{P}^1)$ and $\Omega^1(\mathbb{P}^1) = \{0\}$, we have

$$0 \;=\; \varphi^*(du_i) \underset{\text{locally}}{=} d(\varphi^* u_i)$$

which implies $\varphi^* u_i = u_i \circ \varphi$ (*a priori* only locally well-defined) is *constant* for each $i = 1, \ldots, g$. □

21.2. The Abel-Jacobi map

When is a given divisor $D \in \mathrm{Div}(M)$ of the form (f), for some nontrivial meromorphic function f on M? Since $\deg((f)) = 0$ for any $f \in \mathcal{K}(M)^*$, it is clear that D *must* be of degree 0 — i.e. in the kernel of

$$\begin{aligned} \deg:\ \mathrm{Div}(M) &\longrightarrow \mathbb{Z} \\ \textstyle\sum n_i[p_i] &\longmapsto \textstyle\sum n_i. \end{aligned}$$

So consider a divisor D in

$$\mathrm{Div}^0(M) := \ker(\deg).$$

We may write

$$D = \sum_j ([q_j] - [r_j]) = \partial \underbrace{\left(\textstyle\sum_j \overrightarrow{r_j q_j} \right)}_{=:\Gamma}$$

where "∂" means topological boundary and $\overrightarrow{r_j q_j}$ is a C^∞ path from r_j to q_j.

21.2.1. DEFINITION. The *Abel-Jacobi map*

$$AJ : \ \mathrm{Div}^0(M) \to J(M)$$

sends $D \, (= \partial\Gamma)$ to

$$\int_\Gamma = \sum_j \int_{r_j}^{q_j}$$

viewed as a functional on $\Omega^1(M)$.

The first question that arises is whether this is even well-defined, which in this case means *independent of the choice of "1-chain" (sum of paths)* Γ. To check this, let $\partial\Gamma = D = \partial\Gamma'$. Then $\partial(\Gamma - \Gamma') = 0$, meaning that $\Gamma - \Gamma'$ is a 1-cycle hence represents a class in $H_1(M, \mathbb{Z})$. Consequently,

$$\textstyle\int_{\Gamma - \Gamma'} = \int_\Gamma - \int_{\Gamma'}$$

"belongs to the denominator of $J(M)$". It's even easier to check that AJ is a homomorphism (of abelian groups), which is left to you.

Now suppose $D = (f)$, and consider the family of divisors

$$D_t := f^{-1}(t) \in \mathrm{Div}(M),$$

parametrized by $t \in \mathbb{P}^1$. Then $D = D_0 - D_\infty$, and the composition

$$\mathbb{P}^1 \longrightarrow \mathrm{Div}^0(M) \xrightarrow{AJ} J(M)$$

sending

$$t \longmapsto D_0 - D_t \longmapsto AJ(D_0 - D_t)$$

is constant by Lemma 21.1.3, and *zero* at $t = 0$. Thus $AJ(D) = 0$, and we observe that

$$AJ \text{ factors through } \mathrm{Pic}^0(M) := \frac{\mathrm{Div}^0(M)}{(\mathcal{K}(M)^*)}$$

in a well-defined fashion. (The denominator means "divisors of meromorphic functions", and the statement is simply that AJ kills these.) $\mathrm{Pic}^0(M)$ is called the *Picard group* of M.[3]

The next result will be proved in Chapter 31. Its surjectivity portion is traditionally referred to as the *Jacobi inversion theorem*, while *Abel's theorem* is the injectivity portion.

21.2.2. THEOREM. [ABEL, 1826; JACOBI, 1835]

$$AJ : \mathrm{Pic}^0(M) \to J(M)$$

is an isomorphism.

Leaving aside the surjectivity part, the meaning of the "well-definedness + injectivity" of this map is that for $D \in \mathrm{Div}^0(M)$,

$$\underset{(\text{for some } f \in \mathcal{K}(M)^*)}{D = (f)} \qquad \Longleftrightarrow \qquad AJ(D) \equiv 0 \mod \Lambda_M,$$

completely answering the question we asked at the outset. Note that the forward implication ($\Longrightarrow$) is just well-definedness, which is completely proved. What is nontrivial is the injectivity/backward implication, since you actually have to find some f having D as its divisor!

21.2.3. EXAMPLE. We consider what this means in the genus-one case, i.e. for $M = E$ (the normalization of) an elliptic curve with flex $\mathcal{O}$. Let $\omega \in \Omega^1(E)$ be nonzero, and consider $D \in \mathrm{Div}^0(E)$. We can write $D = \sum n_i[p_i]$ with $\sum n_i = 0$, and

$$AJ\left(\sum n_i[p_i]\right) = AJ\left(\sum n_i([p_i] - [\mathcal{O}])\right) = \sum n_i \int_{\mathcal{O}}^{p_i} \omega = \sum n_i u(p_i)$$

where $u\colon (E, +) \to (\mathbb{C}/\Lambda_E, +)$ is the Abel map. Here the right-hand sum is taking place in $\mathbb{C}/\Lambda_E$, and we see right away that

$$AJ\left(\sum n_i[p_i]\right) = 0 \iff \sum n_i u(p_i) \underset{\Lambda_E}{\equiv} 0.$$

[3]Technically, this is the "degree-zero part" of the Picard group; see §26.1.

By Abel's theorem (on the left) and the fact that u is an isomorphism of groups (on the right), we have that

$$\begin{array}{ccc} \sum n_i[p_i] = (f) & \Longleftrightarrow & \sum n_i \cdot p_i = \mathcal{O} \\ \text{for some } f \in \mathcal{K}(E)^* & & \text{in the group law on } E(\mathbb{C}). \end{array} \tag{21.2.4}$$

As above, the forward implication is immediate from the constancy of morphisms from $\mathbb{P}^1$ to E (Lemma 21.1.3).

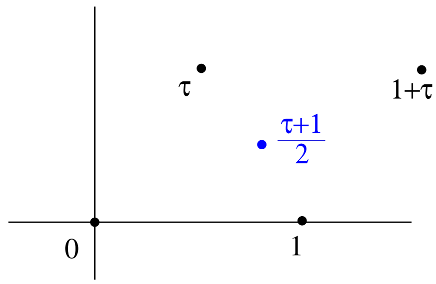
21.2.5. REMARK. Suppose M is smoothly embedded as an algebraic curve in $\mathbb{P}^n$, meeting the hyperplane at infinity $Z_0 = 0$ in a single point $\mathcal{O}$. Write $C = M \cap \mathbb{C}^n$ and $R = \mathbb{C}[C] = \mathbb{C}[z_1, \ldots, z_n]/I(C)$ for the coordinate ring, with fraction field $F = \mathbb{C}(C)^*$. Then we have $\mathrm{Pic}(C) := \frac{\mathrm{Div}(C)}{(\mathbb{C}(C)^*)} = \mathrm{Pic}^0(M)$ (cf. Exercise (6)).

Now associated to each point $p \in C$ is an ideal $I_p \subset M$, comprising functions vanishing at p. An *effective* divisor $D = \sum_i n_i[p_i]$ is one with all $n_i \geq 0$, and this corresponds to an ideal $I_D := \prod_i I_{p_i}^{n_i} \subset R$. There exist *fractional ideals* – i.e. R-modules in F – which furnish inverses I_p^{-1} (cf. Exercise (6)), and using these we can represent arbitrary divisors too. The *principal* fractional ideals fR ($f \in F$) correspond to divisors of rational functions. The Picard group of C is thus presented as the *quotient of the group of fractional ideals of R by the group of principal fractional ideals.*

If we take instead $F = K$ to be an algebraic number field, with $R = \mathcal{O}_K$ its ring of integers, the "Picard" group of fractional modulo principal fractional ideals is known as the *ideal class group* of K. What both cases have in common is that $\mathbb{C}[C]$ and $\mathcal{O}_K$ are *Dedekind domains*, for which being a PID is equivalent to being a UFD. Since nontriviality of the "Picard" group in each case detects the existence of nonprincipal ideals, it also detects the failure of unique factorization in R. One consequence of Abel's theorem is thus that $\mathbb{C}[C]$ is a UFD if and only if C has genus zero.

21.3. Direct proof of Abel's Theorem for genus one

In this section we will deduce a result equivalent to the backward implication in (21.2.4), recasting it as an existence theorem for elliptic functions. It will be convenient to work with a period lattice of the form $\Lambda = \mathbb{Z}\langle 1, \tau \rangle$, $\tau \in \mathfrak{H}$ (upper half-plane):



Any elliptic curve E is isomorphic to a $\mathbb{C}/\Lambda$ of this type, by rescaling the 1-form (or equivalently, the coordinate on $\mathbb{C}$).

21.3.1. THEOREM. *Suppose $m_j \in \mathbb{Z}$ and $u_j \in \mathbb{C}$ satisfy $\sum m_j = 0$ and $\sum m_j u_j \equiv 0$ mod Λ. Then, writing $D := \sum m_j [u_j] \in \mathrm{Div}(\mathbb{C}/\Lambda)$, there exists $g \in \mathcal{K}(\mathbb{C}/\Lambda)$ such that $(g) = D$. (You may think of g as a Λ-periodic meromorphic function on $\mathbb{C}$.)*

PROOF. Introduce the *theta function* (on $\mathbb{C}$)

$$\theta(u) := \sum_{n \in \mathbb{Z}} e^{\pi i \{n^2 \tau + 2nu\}}.$$

The sum converges uniformly on compact sets, hence defines an entire function. (For u in a closed disk of radius $M/2$, and $|n| > \frac{M+1}{\mathrm{Im}(\tau)}$, the n^{th} term has modulus bounded by $e^{-2\pi |n|}$.) While θ is *not* Λ-periodic, it has several nice properties:

(a) $\theta(-u) = \theta(u)$ [this is clear]
(b) $\theta(u+1) = \theta(u)$ [see Exercise (1)]
(c) $\theta(u+\tau) = e^{-2\pi i \left(\frac{\tau}{2} + u\right)} \theta(u)$. To check this, write $\theta(u+\tau)$

$$= \sum_{n \in \mathbb{Z}} e^{\pi i \{n^2 \tau + 2nu + 2n\tau\}} = \sum_{n \in \mathbb{Z}} e^{\pi i \{(n+1)^2 \tau + 2(n+1)u - \tau - 2u\}}$$

which becomes, reindexing by $m = n+1$,

$$= e^{-\pi i \tau - 2\pi i u} \sum_{m \in \mathbb{Z}} e^{\pi i (m^2 \tau + 2mu)}$$

as required.

(d) θ has a simple (order 1) zero at $\frac{\tau+1}{2}$ and nowhere else in the fundamental domain $\mathfrak{F}$ bounded by vertices $0, 1, \tau, 1+\tau$. (To see that there is just a single simple zero in $\mathfrak{F}$, apply (b) and (c) to reduce the integral of $\mathrm{dlog}(\theta) = \frac{d\theta}{\theta}$ around the boundary $\partial\mathfrak{F}$ to $\int_\tau^{\tau+1} d\{2\pi i(\frac{\tau}{2}+u)\} = 2\pi i$. For the rest, see Exercise (2).)

Now consider

$$f(u) := \prod_j \theta\left(u - u_j + \frac{\tau+1}{2}\right)^{m_j};$$

clearly $f(u+1) = f(u)$ by property (b); but also (using property (c))

$$\begin{aligned}\frac{f(u+\tau)}{f(u)} &= \prod_j \left(\frac{\theta\left(\left\{u - u_j + \left(\frac{\tau+1}{2}\right)\right\} + \tau\right)}{\theta\left(u - u_j + \frac{\tau+1}{2}\right)}\right)^{m_j} \\ &= \prod_j \left(e^{-2\pi i\left(\tau + \frac{1}{2} + u - u_j\right)}\right)^{m_j} \\ &= e^{-2\pi i\left(\tau+\frac{1}{2}+u\right)\sum m_j} \cdot e^{2\pi i \sum m_j u_j}.\end{aligned}$$

By asssumption, $\sum m_j = 0$ and $\sum m_j u_j = M + N\tau$, so the last expression equals $e^{2\pi i N\tau}$. The function

$$g(u) := e^{-2\pi i N u} f(u)$$

will therefore satisfy $g(u+\tau) = g(u) = g(u+1)$. So it is Λ-periodic, and the definition of f together with property (d) makes it clear that $(g) = \sum m_j [u_j]$. □

Exercises

(1) Verify property (b) for the theta function above (§21.3).

(2) Finish the proof of property (d) for the theta function by computing $\frac{1}{2\pi i}\int_{\partial\mathfrak{F}} u\,\mathrm{dlog}(\theta)$.

(3) Prove directly that $\mathcal{K}(\mathbb{C}/\Lambda) \cong \mathbb{C}(\wp, \wp')$ (i.e., Theorem 3.1.7(b)) as follows: (a) Check that any Λ-periodic meromorphic function on $\mathbb{C}$ can be written as $f + g\wp'$, where f and g are *even* Λ-periodic meromorphic functions. (b) Show that $\wp(u) - \wp(u_0)$ has simple zeroes at $\pm u_0$ [resp. a double zero at u_0] if $2u_0 \not\equiv 0$ [resp. $\equiv 0$]

mod Λ (and no other zeroes in $\mathbb{C}/\Lambda$). (c) Finish the proof by showing that an even Λ-periodic meromorphic function $f(u)$ can be written as a product $\prod_i (\wp(u) - \wp(u_i))^{m_i}$.

(4) (a) Verify the claim that $\text{Pic}(C) = \text{Pic}^0(M)$ in Remark 21.2.5. [Hint: what is the kernel of the restriction map from $\text{Pic}(M) \twoheadrightarrow \text{Pic}(C)$? (You may assume that $\mathbb{C}(C) \cong \mathcal{K}(M)$, which is dealt with in §25.1.)] (b) Assuming there exists a function $f \in \mathcal{K}(M)^*$ with $(f) = -[p] - \sum_{i=1}^{m-1}[q_i] + m[\mathcal{O}]$, construct a fractional ideal inverse to I_p (notation as in the Remark). (c) Using Abel's theorem, show that such a function exists in the genus one case.

(5) What does Abel's theorem say if $g = 0$? Prove it!