A FEW ELEMENTARY FACTS ABOUT ELLIPTIC CURVES

1. Introduction

In our paper we shall present a number of facts regarding the doubly periodic meromorphic functions, also known as *elliptic functions*. We shall focus on the elliptic functions of order two and, in particular, on the Weierstass $\mathcal{P}$-function. The doubly periodic meromorphic functions can be looked at as meromorphic functions defined on complex tori. This is because, as a topological space, a complex torus is the quotient of the complex plane over an integer lattice.

2. Periodic functions

Definition 1. *A meromorphic function f is said to be periodic if and only if there exists a nonzero $\omega \in \mathbb{C}$ such that $f(z+\omega) = f(z)$, for all $z \in \mathbb{C}$. The complex number ω is called period.*

As a first observation, we may say that if ω is a period, then any integer multiple $n\omega$ is also a period. Also, if there exist two periods ω_1 and ω_2, then $n_1\omega_1 + n_2\omega_2$ is also a period, for all $n_1, n_2 \in \mathbb{Z}$. Given a meromorphic function f, define M to be the set of all its periods (including 0). From the above observations, we deduce that M is a Z-module.

If f is a non-constant meromorphic function, the module M containing all its periods cannot have a accumulation point, since otherwise f would be a constant. Therefore each point in M is *isolated*. In order words, M is a *discrete* module.

We have the following theorem regarding the module M:

Theorem 1. *If M is the module of periods of a meromorphic function f, it must have one of the following forms:*

- $M = \{0\}$.
- $M = \{n\omega | n \in \mathbb{Z}\}$, *for some nonzero complex value ω.*
- $M = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$, *for some nonnzero complex values $\omega_1, \omega_2 \in \mathbb{C}$, whose ratio is not real.*

Proof. Let us suppose that M has nonzero elements. Then take a nonzero element ω_1 of smallest absolute value. This is always possible, since in any disk or radius $\leq r$, there are only finitely many elements of M. Define $A = \{n\omega_1 | n \in \mathbb{Z}\}$. We have $A \subset M$. If $M \neq A$, choose ω_2 the smallest element (in terms of absolute value) in $M - A$. First, note that ω_1/ω_2 cannot be real, otherwise, choose an integer m such that $m \leq \omega_1/\omega_2 < m+1$. It follows that $|\omega_1 - m\omega_2| < |\omega_1|$ which contradicts the minimality of ω_1.

Finally, let us prove that $M = \{n_1\omega_1+n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$. We remark that since ω_1/ω_2 is not real, any complex number can be written uniquely in the form $t\omega_1+s\omega_2$, where s and t are real numbers. In order to see this clearly, it is enough to look at ω_1 and ω_2 as vectors in the two-dimensional real vector space. Since ω_1 and ω_2 are independent as vectors, it becomes obvious why any complex number can be written uniquely as a linear combination of ω_1 and ω_2 with real coefficients. Now, take an arbitrary element x of M and write it in the form $s\omega_1 + t\omega_2$, where s and t are real numbers. Choose integers n_1 and n_2 such that $|s - n_1| < 1/2$ and $|t - n_2| < 1/2$. It follows easily that $|x-n_1\omega_1-n_2\omega_2| < 1/2|\omega_1|+1/2|\omega_2| \leq |\omega_2|$ (the first inequality is strict, since ω_1/ω_2 is nonreal). Because of the way ω_2 was chosen, it follows that $x = n\omega_1$ or $x = n_1\omega_1+n_2\omega_2$. Hence, $M = \{n_1\omega_1+n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$. $\square$

3. Elliptic Functions and Unimodular Forms

Definition 2. *We shall call a meromorphic function f elliptic iff its module of periods M is a linear linear combination of two periods ω_1 and ω_2, such that ω_1/ω_2 is nonreal (i.e. the third case of the previous theorem).*

The pair (ω_1, ω_2) mentioned above is a basis for the module M. In this section we shall discuss about the possible bases of a module of periods M. Suppose (ω_1', ω_2') is another basis of M. Then

$$\omega_1' = m_1\omega_1 + n_1\omega_2,$$
$$\omega_2' = m_2\omega_1 + n_2\omega_2$$

and

$$\omega_1 = m_1'\omega_1 + n_1'\omega_2,$$
$$\omega_2 = m_2'\omega_1 + n_2'\omega_2$$

Using matrices, we can write

$$\begin{pmatrix} \omega_1' & \overline{\omega'}_1 \\ \omega_2' & \overline{\omega'}_2 \end{pmatrix} = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}$$

$$\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix} = \begin{pmatrix} m_1' & n_1' \\ m_2' & n_2' \end{pmatrix} \begin{pmatrix} \omega_1' & \overline{\omega'}_1 \\ \omega_2' & \overline{\omega'}_2 \end{pmatrix}$$

Consequently, we have

$$\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix} = \begin{pmatrix} m_1' & n_1' \\ m_2' & n_2' \end{pmatrix} \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}$$

We have $\omega_1\overline{\omega_2}-\omega_2\overline{\omega_1} \neq 0$, because otherwise ω_1/ω_2 is real, which contradicts our assumption. It follows that

$$\begin{pmatrix} m_1' & n_1' \\ m_2' & n_2' \end{pmatrix} \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and, since all the entries are integral,

$$\begin{vmatrix} m_1' & n_1' \\ m_2' & n_2' \end{vmatrix} = \begin{vmatrix} m_1 & n_1 \\ m_2 & n_2 \end{vmatrix} = \pm 1$$

Therefore, from (ω_1, ω_2) one can obtain (ω_1', ω_2') via a linear transformation of determinant 1, which is usually called $unimodular\ transformation$. We have thus seen that any two bases of the same module M are related to one another by a unimodular transformation.

From all the possible bases of a module, one can choose a particular one, with certain characteristics which will be called *cannonical basis*. This fact is the object of the following

Theorem 2. *Given a module M, there exists a basis (ω_1, ω_2) such that the ratio $\sigma = \omega_1/\omega_2$ has the following properties:*

- *Im $\sigma > 0$*
- *-1/2 $\leq$ Re σ $\leq$ 1/2*
- $|\sigma| \geq 1$
- *If $|\sigma| = 1$, then Re $\sigma \geq 0$*

Also, σ defined above is uniquely determined by these conditions, up to a choice of two, four or six corresponding bases.

4. General Properties of Elliptic Functions

We shall use a convenient notation: $z_1 \equiv z_2$ iff $z_1 - z_2$ belongs to M (in other words, iff $z_1 - z_2 = n_1\omega_1 + n_2\omega_2$, for two integers n_1 and n_2). Let f be a elliptic function with (ω_1, ω_2) as basis of the module of periods. Since f is doubly-periodic, it is entirely determined by its values on a parallelogram P_a whose vertices are a, $a + \omega_1$, $a + \omega_2$ and $a + \omega_1 + \omega_2$. The complex value a can be chosen arbitrarily.

Theorem 3. *If the elliptic funtion f has no poles, it is a constant.*

Proof. If f has no poles, it is bounded in a parallelogram P_a. Since f is doubly periodic, it is bounded on the whole complex plane. By Liouville's theorem, f must be a constant function. □

As we have seen before, the set of poles of f has no accumulation point. It follows that in any parallelogram P_a there are finitely many poles. When we shall refer to $the\ poles\ of\ f$, we shall mean the set of mutually incongruent poles.

Theorem 4. *The sum of residues of an elliptic function f is zero.*

Proof. Choose $a \in \mathbb{C}$ such that the parallelogram P_a does not contain any pole of f. Consider the boundary ∂P_a of P_a traced in the positive sense. Then the integral

$$\frac{1}{2\pi i} \int_{\partial P_a} f(z)$$

equals the sum of residues of f. But the sum equals 0, since the integrals over the opposite sides of the parallelogram cancel each other. $\square$

A simple corollary [1] of this theorem is that an elliptic function cannot have a single simple pole, otherwise, the sum of residues would not equal 0.

Theorem 5. *A nonconstant elliptic function f has the same number of poles as it has zeroes. (Every pole or zero is counted according to its multiplicity)*

Proof. We may consider the function f'/f which has simple poles wherever f has a pole or a zero. The residue of a pole α of f'/f equals its multiplicity in f if α is a zero of f, and minus its multiplicity in f, if α is a pole of f. Applying now theorem 4 to the function f'/f, we get the desired result. $\square$

Since $f(z)-c$ and $f(z)$ have the same number of poles, we conclude that they must have the same number of zeroes.

Definition 3. *Given an elliptic function f, the number of mutually incongruent roots of $f(z)=c$ is called the order of the elliptic function.*

Obviously, the order does not depend on the choice of c.

Theorem 6. *Suppose the nonconstant elliptic function f has the zeroes $a_1,\cdots,a_n$ and poles $b_1,\cdots,b_n$ (multiple roots and poles appear multiple times). Then $a_1+\cdots+a_n \equiv b_1+\cdots+b_n$ (mod M).*

Proof. Consider all a_i and b_i in the parallelogram P_a for some a. We consider the following integral on ∂P_a:

$$\frac{1}{2\pi i}\int_{\partial P_a}\frac{zf'(z)}{f(z)}dz$$

Given the properties of the poles and zeroes of f'/f mentioned above, we deduce that f has a zero (or a pole) at t, of order $k\in\mathbb{Z}_{>0}$, iff zf'/f has a simple pole at t with residue nt (or $-nt$). It follows that the integral equals $a_1+\cdots+a_n-b_1-\cdots-b_n$. Now, we must prove that the integral is in M. For this purpose, we write the integral on the pairs of two opposite sides:

$$\frac{1}{2\pi i}\left(\int_a^{a+\omega_1}\frac{zf'(z)}{f(z)}dz-\int_{a+\omega_2}^{a+\omega_1+\omega_2}\frac{zf'(z)}{f(z)}dz\right)=\frac{-\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}dz$$

Also,

$$\frac{-\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}dz=\frac{-\omega_2}{2\pi i}\int_{\partial D}\frac{1}{w}dw$$

where D is the curve given by $f(z)$ when z varies from a to $a+\omega_1$. $\frac{1}{2\pi i}\int_{\partial D}\frac{1}{w}dw$ is an integer (=the winding number with respect to 0). Taking into account both pairs of opposite sides of P_a, we get the desired result. $\square$

[1]Latin *corona* "garland" > diminutive *corolla* > *corollarium* "gratuity" > English

5. The Weierstass $\mathcal{P}$-function

The simplest example of an elliptic function is of order 2. As we have seen before, there is no elliptic function of order 1. An elliptic function of degree 2 can have either one pole of degree 2 or two distinct simple poles. We shall analyse, following Weierstass, the case of an elliptic function with a double pole.

We may place the pole at the origin and consider the coefficient of z^{-2} as being 1 (translations and multiplications by constants do not change essential properties of elliptic functions). If we consider f(z)-f(-z) we get a elliptic function that has no singular part. (The function $f(z) - f(-z)$ could only have a single simple pole at 0, but this is impossible). Hence, $f(z) - f(-z)$ is constant and setting $z = \omega_1/2$, we get that this constant is zero. Therefore, $f(z) = f(-z)$ and we can write

$$\mathcal{P}(z) = z^{-2} + a_0 + a_1 z^2 + ...$$

We may suppose that $a_0 = 0$, because adding/substracting a constant from f is irrelevant. What we get is the so called $Weierstass$ $\mathcal{P}$-function. This elliptic function can be written as

$$\mathcal{P}(z) = z^{-2} + a_1 z^2 + a_2 z^4 + ... \tag{1}$$

The existence of a elliptic function of order 2 has not yet been proven. We shall prove that the Weierstrass $\mathcal{P}$-function is uniquely determined for a basis (ω_1, ω_2), being given by the formula:

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{2}$$

where the summation is over all $\omega = n_1\omega_1 + n_2\omega_2$, $\omega \neq 0$. We shall prove first that this sum is convergent. For every $|\omega| > 2|z|$, we have

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{10|z|}{|\omega|^3}$$

This is because $|2\omega - z| < 5/2|\omega|$ and $|z - \omega| \geq |\omega| - |z| \geq |\omega|/2$.

We conclude that in order for the sum (2) to converge, it is enough to prove that the sum

$$\sum_{\omega \neq 0} \frac{1}{|\omega|^3} < \infty$$

Also, since ω_1/ω_2 is not real $|n_1\omega_1 + n_2\omega_2| = |\omega_2||n_1\omega_1/\omega_2 + n_2| \geq c|n_1|$ for some positive real constant c (for any integers n_1, n_2). Similarly, we find a constant d such that $|n_1\omega_1 + n_2\omega_2| \geq d|n_2|$, for any integers n_1, n_2. In conclusion, $|n_1\omega_1 + n_2\omega_2| \geq k(|n_1| + |n_2|)$, where $k = cd/(c+d) \geq 0$. Since there are exactly $4n$ ordered pairs (n_1, n_2) of integers such that $|n_1| + |n_2| =$

n, we have

$$\sum_{\omega \neq 0} \frac{1}{|\omega|^3} < \frac{1}{4k^3} \sum_{1}^{\infty} \frac{1}{n^2}.$$

We also need to prove that $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ has periods ω_1 and ω_2. We denote, for this purpose

$$f(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{3}$$

Since the series is absolutely convergent, we may differentiate term by term:

$$f'(z) = -\frac{2}{z^3} - \sum_{\omega \neq 0} \frac{2}{(z-\omega)^3} = -2 \sum_{\omega} \frac{1}{(z-\omega)^3}$$

This series is also absolutely convergent, since if $|\omega| > 2|z|$, we have

$$\sum_{\omega} \left| \frac{1}{(z-\omega)^3} \right| \leq 16 \sum_{\omega} \frac{1}{|\omega|^3}$$

and we deduce that (3) converges absolutely. Consequently, $f(z+\omega_1) - f(z)$ and $f(z+\omega_2) - f(z)$ are constant functions. By definition, f is even and, therefore, setting $z = -\omega_1/2$ and $z = -\omega_2/2$ we get that the constants are 0. Therefore, $f(z+\omega_1) = f(z)$ and $f(z+\omega_2) = f(z)$, for all $z \in \mathbb{C}$. Hence, we proved that f is elliptic. If $\mathcal{P}$ has the form in (1) and is doubly periodic, with periods ω_1 and ω_2, it follows that $\mathcal{P} - f$ has no singular part, and is therefore constant. Since both $\mathcal{P}$ and f have no constant term (i.e. the coefficient of z^0 is 0), it follows that $\mathcal{P} = f$. Hence, we deduce that

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

and also that

$$\mathcal{P}'(z) = -2 \sum_{\omega} \frac{1}{(z-\omega)^3}$$

6. The function $\zeta(z)$

Because $\mathcal{P}$ has no residues, it is the derivative of a function -$\zeta(z)$, where

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \neq 0} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right)$$

In order to prove that this series converges, we note that

$$\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} = \frac{z^2}{\omega^2 (z-\omega)}$$

Hence, if $|\omega| > 2|z|$,

$$\sum_{\omega\neq 0}\left|\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\right| = \sum\left|\frac{z}{\omega^2(z-\omega)}\right| \leq |z|^2\sum\frac{2}{|\omega|^3}$$

and, consequently, the series converges absolutely.

Since $f(z+\omega_i) = f(z)$, for $i = 1, 2$ it follows that $\zeta(z+\omega_i) = \zeta(z)+\eta_i$, for $i = 1, 2$, where η_i are complex constants. These complex constants have a beautiful property which comes from the fact that

$$\frac{1}{2\pi i}\int_{\partial P_a}\zeta(z)dz = 1 \tag{4}$$

We prove first (4). If we look at (2), we deduce that

$$\zeta(z) = z^{-1} - \frac{a_1}{3}z^3 - \frac{a_2}{5}z^5 + \cdots$$

Now, if we evaluate the integral on two opposite sides of the parallelogram P_a, we get

$$\frac{1}{2\pi i}\left(\int_a^{a+\omega_1}\zeta(z)dz - \int_{a+\omega_2}^{a+\omega_1+\omega_2}\zeta(z)dz\right) = \frac{-\eta_1\omega_2}{2\pi i}$$

Integrating similarly on the other pair of opposide sides, we get that

$$\frac{-\eta_2\omega_1}{2\pi i} - \frac{-\eta_1\omega_2}{2\pi i} = 1$$

and, finally,

$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i$$

which is called $Legendre's\ relation$.

7. The Differential equation corresponding to $\mathcal{P}$

Using the definition of $\zeta(z)$, we have the following identity

$$\frac{1}{z-\omega}+\frac{1}{w}+\frac{z}{\omega^2} = -\frac{z^2}{\omega^3} - \frac{z^3}{\omega^4} - \cdots$$

Consequently, we can write

$$\zeta(z) = \frac{1}{z} + \sum_{k=2}^{\infty} G_k z^{2k-1}$$

where by G_k we mean

$$G_k = \sum_{\omega\neq 0}\frac{1}{\omega^{2k}} \tag{5}$$

We note that $\zeta(z)$ has no terms of the form z^{2n} since $\mathcal{P}$ is an even function (and ζ is odd). Differentiating (5), we get

$$\mathcal{P} = \frac{1}{z^2} + \sum_{k=2}^{\infty}(2k-1)G_k z^{2k-2}$$

Writing only the significant parts of the following functions, we have:

$$\mathcal{P}(z) = \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + \cdots$$

$$\mathcal{P}'(z) = -\frac{2}{z^3} + 6G_2 z + 20G_3 z^3 + \cdots$$

$$\mathcal{P}'(z)^2 = \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + \cdots$$

$$4\mathcal{P}(z)^3 = \frac{4}{z^6} + \frac{36G_2}{z^2} + 60G_3 + \cdots$$

$$60G_2\mathcal{P}(z) = \frac{60G_2}{z^2} + 0 + \cdots$$

It follows that

$$\mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + 60G_2\mathcal{P}(z) = -140G_3 + \cdots$$

The left side of the last identity is an elliptic function and it does not have any singular part. Therefore, it must equal a constant. Setting $z = 0$, we get that the constant is $-140G_3$. Hence

$$\mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + 60G_2\mathcal{P}(z) + 140G_3 = 0$$

If we set $g_2 = 60G_2$ and $g_3 = 140G_3$, we get

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3$$

Provided that e_1, e_2 and e_3 are the complex roots of the polynomial $4y^3 - g_2 y - g_3$, we can write

$$\mathcal{P}'(z)^2 = 4(\mathcal{P}(z) - e_1)(\mathcal{P}(z) - e_2)(\mathcal{P}(z) - e_3)$$

Because $\mathcal{P}$ is even and periodic, we have $\mathcal{P}(\omega_1 - z) = \mathcal{P}(z)$. It follows that $\mathcal{P}'(\omega_1 - z) = \mathcal{P}'(z)$. Hence $\mathcal{P}'(\omega_1/2) = 0$. Similarly, $\mathcal{P}'(\omega_2/2) = 0$. We have also, $\mathcal{P}'(\omega_1 + \omega_2 - z) = \mathcal{P}'(z)$, and therefore, $\mathcal{P}'((\omega_1 + \omega_2)/2) = 0$. Since $\mathcal{P}'$ has only one pole (of order 3), it must have exactly three roots (counting multiplicity). On the other hand, the complex numbers $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ are mutually incongruent. Therefore, they are the three distinct roots of $\mathcal{P}'$.

For every e_i there exists d_i such that $\mathcal{P}(d_i) = e_i$ (this equation in fact has a double solutions, as we shall see below). Also, d_i are roots of $\mathcal{P}'$. Therefore, if we apply $\mathcal{P}$ on the set of roots of $\mathcal{P}'$ (a set which has three elements, $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$), we get the whole set $\{e_1, e_2, e_3\}$. Consequently, we may set $\mathcal{P}(\omega_1/2) = e_1$ and $\mathcal{P}(\omega_2/2) = e_2$ and $\mathcal{P}((\omega_1 + \omega_2)/2) = e_3$.

Every root of $\mathcal{P} - e_i$ is also a root of $\mathcal{P}'$. If, for instance, $e_1 = e_2$, then the root d_1 of $\mathcal{P} - e_1$ has multiplicity at least 2 in $\mathcal{P}'$ and, therefore, multiplicity at least 3 in $\mathcal{P} - e_1$, which is impossible for an elliptic curve of order 2. In conclusion, we derive an important observation, namely that *all roots* e_i *are distinct*.

References

[1] L.Ahlfors, *Complex Analysis*, (1979), 263-278