ELLIPTIC FUNCTIONS (WEEK 12)

Elliptic functions are doubly periodic meromorphic functions. By *doubly periodic*, we mean that there are $\omega_1, \omega_2 \in \mathbb{C}^\times$ such that $f(z+\omega_1) = f(z) = f(z+\omega_2)$ for all $z \in \mathbb{C}$. If we assume that $\omega_2/\omega_1 \notin \mathbb{R}$, then the set $L = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$ is a *lattice* in $\mathbb{C}$: a rank 2 free Abelian subgroup of $(\mathbb{C}, +)$. Let $\mathbb{C}/L$ denote the corresponding quotient group. Topologically, $\mathbb{C}/L$ is a torus, and with its complex structure it is an *elliptic curve*.[1] If f is an elliptic function with period lattice L, then it extends across the quotient map $\mathbb{C} \to \mathbb{C}/L$ to become a function on the elliptic curve $\mathbb{C}/L$. One way to understand a geometric object is by its functions, whence the importance of elliptic functions.

These notes will closely follow the development of elliptic functions in Chapter 7 of Lars Ahlfors' classic text, *Complex Analysis*; some of the later portions draw from notes by Jerry Shurman.

1. Singly periodic functions

We should walk before we run, so let's first consider *singly periodic functions*, *i.e.*, meromorphic functions f for which there exists $\omega \in \mathbb{C}$ such that $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$. We have seen examples before: the exponential function has period $2\pi i$, and $\sin$ and $\cos$ have period 2π.

Fix $\omega \in \mathbb{C}^\times$ and suppose $\Omega \subseteq \mathbb{C}$ is an open set which is closed under addition and subtraction of ω: if $z \in \Omega$, then $z \pm \omega \in \Omega$. It follows by induction that $\Omega = \Omega + \mathbb{Z}\omega$. Examples of such regions include $\mathbb{C}$ and an "open strip" parallel to ω. To better describe this open strip, transform it by dividing by ω. This has the effect of scaling by $1/|\omega|$ and rotating so that the strip is now parallel to the real axis. Thus the strip is determined by real numbers $a < b$ such that $a < \operatorname{Im}(2\pi z/\omega) < b$ for all z in the strip. (The 2π is a convenient normalization factor, as we shall shortly see.)

The function $z \mapsto \zeta = e^{2\pi i z/\omega}$ is ω-periodic. If we plug Ω into it, we get an open set in the ζ-plane. If $\Omega = \mathbb{C}$, the result is $\mathbb{C}^\times$. If Ω is the strip given by $a < \operatorname{Im}(2\pi z/\omega) < b$, the result is the annulus $e^{-b} < |\zeta| < e^{-a}$. (This follows because $e^{2\pi i z/\omega} = e^{-\operatorname{Im}(2\pi z/\omega}e^{i\operatorname{Re}(2\pi z/\omega)}$.)

Proposition 1.1. *Suppose that f is meromorphic and ω-periodic on Ω. Then there exists a unique function F on $\Omega' = e^{2\pi i\Omega/\omega}$ such that*

$$f(z) = F(e^{2\pi i z/\omega}). \tag{1}$$

Proof. To determine $F(\zeta)$, first note that $\zeta = e^{2\pi i z/\omega}$ for some $z \in \Omega$, and that z is unique up to addition of an integer-multiple of ω. Since f is ω-periodic, the formula $F(\zeta) = f(z)$ is well-defined, and it is clearly meromorphic in Ω'. Uniqueness follows from noting that when F is meromorphic on Ω', equation (1) defines a function f meromorphic on Ω with period ω. □

Now suppose that Ω' contains an annulus $r < |\zeta| < R$ on which F has is analytic. On this annulus, F has a Laurent series

$$F(\zeta) = \sum_{n=-\infty}^{\infty} c_n \zeta^n,$$

whence

$$f(z) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi i n z/\omega}.$$

[1]Curves are one-dimensional and tori are two-dimensional. What gives? The 'curve' in 'elliptic curve' indicates a single *complex* dimension.

This is the *complex Fourier series* for f in the strip $-\log(R) < \operatorname{Im}(2\pi z/\omega) < -\log r$.

By old formulae, we know that for $r < s < R$,

$$c_n = \frac{1}{2\pi i} \int_{|\zeta|=s} \frac{F(\zeta)}{\zeta^{n+1}}\, d\zeta,$$

which, by change of variables, is equivalent to

$$c_n = \frac{1}{\omega} \int_d^{d+\omega} f(z) e^{-2\pi i n z/\omega}\, dz.$$

Here d is an arbitrary point in the strip corresponding to the annulus, and the integration is along any path from d to $d+\omega$ which remains in the strip. (You will verify the final details of this in your homework.) We have thus proven the following result.

Theorem 1.2. *Suppose f is meromorphic and ω-periodic on an open set $\Omega \subseteq \mathbb{C}$ and is analytic on the strip given by $a < \operatorname{Im}(2\pi z/\omega) < b$. Then*

$$f(z) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi i n z/\omega}$$

for z in the strip, and

$$c_n = \frac{1}{\omega} \int_d^{d+\omega} f(z) e^{-2\pi i n z/\omega}\, dz$$

for d in the strip and the integration along any path from d to $d+\omega$ in the strip. If f is analytic on $\mathbb{C}$, then the Fourier series is valid on $\mathbb{C}$ as well. □

2. Doubly periodic functions

An *elliptic function* is a meromorphic function on the plane with two periods, $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_2/\omega_1 \notin \mathbb{R}$. The significance of the final condition is that one of the periods is not a real scaling of the other. This has the effect of making $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a rank 2 free Abelian group inside $(\mathbb{C}, +)$, as we shall currently show.

2.1. **The period lattice.** For the moment, forget the condition on ω_2/ω_1 and just suppose that $f(z+\omega_1) = f(z) = f(z+\omega_2)$ for all $z \in \mathbb{C}$. Let $M := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ denote the *period module* of f.

Proposition 2.1. *If f is not constant with periods $\omega_1, \omega_2 \in \mathbb{C}^\times$, then $M = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is discrete.*

Proof. Since $f(\omega) = f(0)$ for all $\omega \in M$, the existence of an accumulation point in M would imply that f is constant (by the Identity Theorem). □

Theorem 2.2. *A discrete subgroup A of $(\mathbb{C}, +)$ is either*
(0) rank 0: $A = \{0\}$,
(1) rank 1: $A = \mathbb{Z}\omega$ for some $\omega \in \mathbb{C}^\times$, or
(2) rank 2: $A = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for some $\omega_1, \omega_2 \in \mathbb{C}^\times$ with $\omega_2/\omega_1 \notin \mathbb{R}$.

Proof. We may assume that $A \neq \{0\}$. Take $r > 0$ such that $\overline{D}_r(0) \cap A$ contains more than just 0. Since $\overline{D}_r(0)$ is compact and A is discrete, the intersection contains only finitely many points. Choose one with minimum nonzero modulus and call it ω_1. (You can check that there are always exactly two, four, or six points in A closest to 0.) Then $\mathbb{Z}\omega_1 \subseteq A$.

If $A = \mathbb{Z}\omega_1$, we are in case (1) and done. Suppose there exists $\omega \in A \setminus \mathbb{Z}\omega_1$. Among all such ω, there exists one, ω_2, of smallest modulus. Suppose for contradiction that $\omega_2/\omega_1 \in \mathbb{R}$. Then we could find an integer n such that $n < \omega_2/\omega_1 < n+1$. It would follow that $|n\omega_1 - \omega_2| < |\omega_1|$, a contradiction.

We now aim to show that $A = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. We claim that every $z \in \mathbb{C}$ may be written as $z = \lambda_1\omega_1 + \lambda_2\omega_2$ with $\lambda_1, \lambda_2 \in \mathbb{R}$. To see this, we attempt to solve the equations

$$z = \lambda_1\omega_1 + \lambda_2\omega_2$$
$$\overline{z} = \lambda_1\overline{\omega}_1 + \lambda_2\overline{\omega}_2.$$

The determinant $\omega_1\overline{\omega}_2 - \omega_2\overline{\omega}_1 \neq 0$ (otherwise ω_2/ω_1 is real) and thus the system has a unique solution $(\lambda_1, \lambda_2) \in \mathbb{C}^2$. But clearly $(\overline{\lambda}_1, \overline{\lambda}_2)$ is a solution as well, so $(\lambda_1, \lambda_2) \in \mathbb{R}^2$, as desired.

Now choose integers m_1, m_2 such that $|\lambda_1 - m_1| \leq 1/2$ and $|\lambda_2 - m_2| \leq 1/2$. If $z \in A$, then $z' = z - m_1\omega_1 - m_2\omega_2 \in A$ as well. Thus $|z'| < \frac{1}{2}|\omega_1| + \frac{1}{2}|\omega_2| \leq |\omega_2|$. (The first inequality is strict since ω_2 is not a real multiple of ω_1.) Since ω_2 has minimal modulus in $A \setminus \mathbb{Z}\omega_1$, we learn that $z' \in \mathbb{Z}\omega_1$, say $z' = n\omega_1$. Thus $z = (m_1 + n)\omega_1 + m_2\omega_2 \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and we conclude that $A = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. □

2.2. **The modular group.** From now on, we assume that the period lattice has rank 2. Any pair (ω_1, ω_2) such that $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is called a *basis* of L (and necessarily satisfies $\omega_2/\omega_1 \notin \mathbb{R}$).

Suppose that (ω_1', ω_2') is another basis of L. Then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\omega_1' = a\omega_1 + b\omega_2$$
$$\omega_2' = c\omega_1 + d\omega_2.$$

In matrix form, this is

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

The same relation is valid for the complex conjugates, so

$$\begin{pmatrix} \omega_1' & \overline{\omega}_1' \\ \omega_2' & \overline{\omega}_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}.$$

Since (ω_1', ω_2') is also a basis, there are also integers a', b', c', d' such that

$$\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega_1' & \overline{\omega}_1' \\ \omega_2' & \overline{\omega}_2' \end{pmatrix}.$$

Substituting, we get

$$\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}.$$

We know that $\det \begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix} \neq 0$ (since $\omega_2/\omega_1 \notin \mathbb{R}$), and thus we may multiply on the right by $\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}^{-1}$ to get

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus the integer matrices are inverses of each other, and their determinants multiply to give 1. Since both determinants are integers, we see that $ad - bc$ and $a'd' - b'c'$ are ± 1. Let $\mathrm{GL}_2(\mathbb{Z}) := \{m \in M_{2\times 2}(\mathbb{Z}) \mid \det m = \pm 1\}$ denote the General Linear group of 2×2 invertible integer matrices. We have proven the following result.

Theorem 2.3. *Suppose $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$ with ordered basis (ω_1, ω_2). Then the set of all ordered bases of L is the $\mathrm{GL}_2(\mathbb{Z})$-orbit of (ω_1, ω_2),* i.e., *the set of (ω_1', ω_2') such that*

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

for some integers a, b, c, d with $ad - bc = \pm 1$. □

The group $\mathrm{GL}_2(\mathbb{Z})$ is called the *modular group*. That term, though, is also sometimes used for $\mathrm{SL}_2(\mathbb{Z})$, the 2×2 integer matrices with determinant 1. This latter group can be thought of as the transformations that change basis in an orientation-preserving fashion.

2.3. **The canonical basis.** We now single out a nearly unique basis called the *canonical basis* of a lattice L.

Theorem 2.4. *Given a lattice L, there exists a basis (ω_1, ω_2) such that $\tau = \omega_2/\omega_1$ satisfies the following conditions:*

(i) $\mathrm{Im}(\tau) > 0$,
(ii) $-1/2 < \mathrm{Re}(\tau) \leq 1/2$,
(iii) $|\tau| \geq 1$, *and*
(iv) if $|\tau| = 1$, *then* $\mathrm{Re}(\tau) \geq 0$.

The ratio τ is uniquely determined by these conditions, and there is a choice of two, four, or six corresponding ordered bases.

Proof. Choose ω_1 and ω_2 as in the proof of Theorem 2.2. Then $|\omega_1| \leq |\omega_2| \leq |\omega_1 \pm \omega_2|$. In terms of $\tau = \omega_2/\omega_1$, the first inequality becomes $|\tau| \geq 1$. Dividing the second inequality by $|\omega_1|$ we get $|\tau| \leq |1 \pm \tau|$. Squaring and expanding by real and imaginary parts gives

$$\mathrm{Re}(\tau)^2 + \mathrm{Im}(\tau)^2 \leq (1 \pm \mathrm{Re}(\tau))^2 + \mathrm{Im}(\tau^2).$$

Canceling, expanding, and rearranging gives

$$0 \leq 1 \pm 2\,\mathrm{Re}(\tau),$$

i.e., $|\mathrm{Re}(\tau)| \leq 1/2$.

If $\mathrm{Im}(\tau) < 0$, replace (ω_1, ω_2) by $(-\omega_1, \omega_2)$, making $\mathrm{Im}(\tau) > 0$ without changing $\mathrm{Re}(\tau)$. If $\mathrm{Re}(\tau) = -1/2$, replace the basis by $(\omega_1, \omega_1 + \omega_2)$, and if $|\tau| = 1$ with $\mathrm{Re}(\tau) < 0$, replace it by $(-\omega_2, \omega_1)$. After these changes, all the conditions are satisfied. Uniqueness will be handled in Theorem 2.6.

There are always at least two bases corresponding to $\tau = \omega_2/\omega_1$, namely (ω_1, ω_2) and $(-\omega_1, -\omega_2)$. We handle the exceptional cases of 4 and 6 bases after the proof of 2.6. ☐

Definition 2.5. The collection of τ described by Theorem 2.4 is called the *fundamental region* of the unimodular group.

The unimodular group $\mathrm{GL}_2(\mathbb{Z})$ acts on bases (ω_1, ω_2) via matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} = \begin{pmatrix} a\omega_2 + b\omega_1 \\ c\omega_2 + d\omega_1. \end{pmatrix}$$

(We have swapped the usual order of ω_1 and ω_2 so as to more closely mirror $\tau = \frac{\omega_2}{\omega_1}$.) As such, it acts on the quotient $\tau = \omega_2/\omega_1$ via a linear fractional transformation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1} = \frac{a\tau + b}{c\tau + d}$$

Theorem 2.6. *If τ and τ' are in the fundamental region and $\tau' = (a\tau + b)/(c\tau + d)$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, then $\tau = \tau'$.*

Proof. Suppose that $\tau' = (a\tau + b)/(c\tau + d)$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Then

$$\mathrm{Im}(\tau') = \frac{\pm \mathrm{Im}(\tau)}{|c\tau + d|^2}$$

with sign matching that of $ad - bc = \pm 1$. If τ and τ' are in the fundamental region, then the sign must be positive, so $ad - bc = 1$. Without loss of generality, $\mathrm{Im}(\tau') \geq \mathrm{Im}(\tau)$, so $|c\tau + d| \leq 1$.

If $c = 0$, then $d = \pm 1$ or 0. Since $ad - bc = 1$, we have $ad = 1$, so either $a = d = 1$ or $a = d = -1$. Then $\tau' = \tau \pm b$, whence $|b| = |\operatorname{Re}(\tau') - \operatorname{Re}(\tau)| < 1$. Therefore $b = 0$ and $\tau = \tau'$.

We leave the $c \neq 0$ case as a moral exercise for the reader. The arguments are somewhat intricate, but unsurprising. □

Finally, we note that τ corresponds to bases other than (ω_1, ω_2) and $(-\omega_1, -\omega_2)$ if and only if τ is a fixed point of some unimodular transformation. This only happens for $\tau = i$ (which is a fixed point of $-1/\tau$) and $\tau = e^{\pi i/3}$ (which is a fixed point of $-(\tau+1)/\tau$ and $-1/(\tau+1)$.) We leave it to the reader to check that these are the only possibilities.

2.4. **General properties of elliptic functions.** Let f be a meromorphic function on $\mathbb{C}$ with period lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ of rank 2. (We do not assume that (ω_1, ω_2) is a canonical basis, nor do we assume that L comprises all periods of f.)

Some notation to ease our upcoming work: write $z_1 \equiv z_2 \pmod{L}$ if $z_1 - z_2 \in L$. For $a \in \mathbb{C}$, write P_a for the "half open" parallelogram with vertices $a, a + \omega_1, a + \omega_2, a + \omega_1 + \omega_2$ that includes the line segments $[a, a+\omega_1]$ and $[a+\omega_1, a+\omega_1+\omega_2)$ but does not include the other two sides. Then every point in $\mathbb{C}/L$ (the set of equivalence classes modulo L) contains a unique representative in P_a.

Theorem 2.7. *If f is an elliptic function without poles, then f is constant.*

Proof. If f is analytic on P_a, then it is bounded on the closure of P_a, and hence bounded and analytic on $\mathbb{C}$. By Liouville's theorem, f is constant. □

Proposition 2.8. *An elliptic function has finitely many poles in P_a.*

Proof. Poles always form a discrete set, and P_a is bounded. □

Theorem 2.9. *The sum of the residues of an elliptic function at poles in a parallelogram P_a is zero.*

Proof. We may perturb a so that none of the poles lie on ∂P_a. Then, by the residue theorem, the sum of the residues at poles in P_a equals

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

Since f has periods ω_1 and ω_2, the line integrals along opposite sides cancel, and we get that the sum of the residues is 0. □

Corollary 2.10. *No elliptic function has a single simple pole (and no other poles) in some P_a.*

Proof. A simple pole has a nonzero residue, and the sum of the residues is zero. □

Theorem 2.11. *A nonzero elliptic function has equally many poles and zeros in any P_a (where poles and zeroes are counted with multiplicity).*

Proof. Fix a nonzero elliptic function f. In the proof of Theorem 4.4.7 we saw that the *logarithmic derivative* f'/f has the zeros and poles of f as simple poles, with residues equal to their (signed) multiplicities. Since f'/f is also elliptic, the result follows from Theorem 2.9. □

Note that for any constant $c \in \mathbb{C}$, $f(z) - c$ has the same poles as $f(z)$. It follows that all values are assumed the same number of times by f.

Definition 2.12. The number of incongruent (mod L) roots of the equations $f(z) = c$ is called the *order* of the elliptic function.

Theorem 2.13. *The zeros* $a_1, \ldots, a_n$ *and poles* $b_1, \ldots, b_n$ *of an elliptic function satisfy* $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{L}$.

Proof. Choose $a \in \mathbb{C}$ such that none of the zeros or poles are on ∂P_a. Also choose zeros and poles inside of P_a. By calculus of residues,

$$\frac{1}{2\pi i} \int_{\partial P_a} \frac{z f'(z)}{f(z)} \, dz = a_1 + \cdots + a_n - b_1 - \cdots - b_n.$$

(Check this!) It remains to prove that the left-hand side is an element of $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. The portion of the integral contributed by the sides $[a, a+\omega_1]$ and $[a+\omega_2, a+\omega_1+\omega_2]$ is

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

(Check this!) As z varies in $[a, a+\omega_1]$, the values $f(z)$ describe a closed curve in the plane; call this curve γ. Then the right-hand side of the above expression is manifestly $-\omega_2 \operatorname{Ind}_\gamma(0)$, which is an integer multiple of ω_2. A similar argument applies to the other pair of opposite sides. We conclude that

$$a_1 + \cdots + a_n - b_1 - \cdots - b_n = m\omega_1 + n\omega_2$$

for some integers m, n, as desired. $\square$