Modular Functions and Picard's Little Theorem

Daniel Milanovich

Picard's Theorems are two very important results in complex analysis, representing enormous strengthenings of Liouville's theorem and the Casorati-Weierstrass Theorem, respectively. The respective statements of the theorems are as follows:

Theorem 0.1. *An an entire function takes on every value, with possibly one exception.*

Theorem 0.2. *A function takes on every value infinitely often in any neighborhood of an essential singularity, with possibly one value that is never taken on.*

Both of these theorems are proven in Gamelin's textbook, but here we will give a different proof of them, using a special kind of function known as a *modular function.* Along the way we will investigate modular functions themselves, and present some interesting properties of them. All material is based on Apostol [1], unless otherwise noted.

Contents

1 Lattices

Construction of a modular function will rely closely on the concept of a lattice of points in $\mathbb{C}$:

Definition 1.1. A *lattice* is a set of points in $\mathbb{C}$ of the form

$$\Omega(\omega_1, \omega_2) = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z},\, \omega_1/\omega_2 \notin \mathbb{R}\}.$$

Note that ω_1 and ω_2 are fixed. The Greek letter Ω is often used to represent a lattice.

the condition $\omega_1/\omega_2 \notin \mathbb{R}$ is required to prevent degenerate cases. Indeed, set $\omega_1 = r_e^{i\theta_1}$ and $\omega_2 = r_2 e^{i\theta_2}$. Then $\omega_1/\omega_2 = (r_1/r_2)e^{i(\theta_1-\theta_2)}$. But this ratio is real, so $\theta_1 = \theta_2$, and the whole lattice just lies on a single line (in fact, if ω_1/ω_2 is irrational, then the lattice generated would be the whole line. A proof of this is left as an exercise to the reader).

Given a lattice, we want a sense of the *smallest* ω_1 and ω_2 that generate the lattice. This can be formalized in the following definition:

Definition 1.2. A pair of complex numbers (ω_1, ω_2) is a *Fundamental Pair* of the lattice Ω if every point in omega can be represented as $m\omega_1 + n\omega_2$, for some integers m and n.

The name "fundamental" is justified by the following theorem:

Theorem 1.1. *If Ω is a lattice, then the (closed) triangle T with vertices 0, ω_1, and ω_2 contains no points of Ω other than the vertices if and only if (ω_1, ω_2) is a fundamental pair of Ω.*

Proof. One direction is trivial. Let (ω_1, ω_2) be a fundamental pair of Ω, and consider the (closed) parallelogram P with vertices 0, ω_1, ω_2, and $\omega_1 + \omega_2$. Every point z in this parallelogram is of the form $z = a\omega_1 + b\omega_2$ for $0 \leq a, b, \leq 1$. But $z \in \Omega$ if and only if $a, b \in \mathbb{Z}$, so $P \cap \Omega = \{0, \omega_1, \omega_2, \omega_1 + \omega_2\}$, and in particular, there are no points of Ω in the interior of P.

The other way is a bit trickier. Let $\omega \in \Omega$. Because we only consider a lattice when ω_1/ω_2 is not real, ω_1 and ω_2 are linearly independent when considered as vectors. Thus $\omega = a\omega_1 + b\omega_2$ for some $a, b \in \mathbb{R}$. It is obvious that

$$a = \lfloor a \rfloor + r_1, \quad b = \lfloor b \rfloor + r_2$$

for $0 \leq r_1, r_2 < 1$. This means

$$\omega - \lfloor a \rfloor \omega_1 - \lfloor b \rfloor \omega_2 = r_1\omega_1 + r_2\omega_2 = p$$

for some $p \in \Omega$ (the left hand side of this is clearly in Ω, so p is in Ω). If r_1 and r_2 are not both 0, then p lies inside of P as defined above. But this means that either p or $q = \omega_1 + \omega_2 - p$ (also in Ω) will lie on T, giving a contradiction. Thus $r_1, r_2 = 0$, and $a, b \in \mathbb{Z}$, so that (ω_1, ω_2) is a fundamental pair of Ω. □

It is easy to see that a pair (ω_1, ω_2) does not uniquely generate a lattice ($(-\omega_1, -\omega_2)$ clearly generates the same lattice as well). However, one generating pair can be produced from another, by the following theorem:

Theorem 1.2. *The two pairs lattices $\Omega(\omega_1, \omega_2)$ and $\Omega(\omega_1', \omega_2')$ are equivalent if an only if there exist integers a, b, c, d such that $ad - bc = 1$, and*

$$\omega_2' = a\omega_2 + b\omega_1$$

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

The proof of this fact is left as an exercise to the reader.

2 Groups

In order to understand what modular functions are actually doing, and why we might care about them, we have to discuss *the Modular Group.* To do this, we begin with a relatively informal discussion of groups in general. The study of groups is rich and varied, and we cannot hope to cover everything of interest here. We will discuss only the basics, and give an overview of the *orbit of a group action.* The material in the first two sections is based on my own knowledge.

2.1 Basics

Definition 2.1. A group is a set G (finite or infinite), equipped with a binary operation $G \times G \to G$, denoted by a dot $\cdot$ or by juxtaposition, which satisfies the following axioms:

1. (Closure) If $g, h \in G$, then $g \cdot h \in G$.
2. (Identity) There is some $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. (Inverses) For all $g \in G$, there is some h in g such that $g \cdot h = h \cdot g = e$. This h is generally denoted by g^{-1}.

4. (Associativity) For all $g, h, k \in G$, $g(hk) = (gh)k$.

An important note is that a group is not, in general, commutative – that is, $gh \neq hg$ for any two elements in an arbitrary group. If any two elements in a given group *do* commute, then the group is called *commutative* or *abelian*.

This is a nice list of axioms, but we would like to have a few basic properties under our belt before we go further. We summarize those properties here, and provide proofs for some of them.

Theorem 2.1. *The identity of a group is unique.*

Proof. Assume that there are two identities e_1 and e_2. Then for some g, $e_1 g = g = e_2 g$. Right-multiplying by g^{-1}, we get $e_1 = e_2$. □

Theorem 2.2. *The inverse of an element is unique.*

Proof. Say we have two inverses h_1 and h_2, such that $h_1 g = h_2 g = e$. Then right-multiplying by an inverse of g (it does not matter which) and applying associativity, we get $h_1 = h_2$. □

Theorem 2.3. *For all g, $(g^{-1})^{-1} = g$.*

Proof. It is clear that $(g^{-1})^{-1} \cdot g^{-1} = e = gg^{-1}$. But by the previous theorem, the inverse of g^{-1} is unique, so $(g^{-1})^{-1} = g$. □

Theorem 2.4. *For any g and h, $(gh)^{-1} = h^{-1}g^{-1}$.*

Proof. We have $(gh)(gh)^{-1} = e = ghh^{-1}g^{-1}$. The inverse of gh is unique, so we must have $(gh)^{-1} = h^{-1}g^{-1}$. □

Theorem 2.5. *Every bracketing of $g_1 \cdots g_n$ is equivalent (this generalizes the axiom of associativity).*

Proof. We precede by induction. The axiom of associativity itself gives us the base case, so for the inductive step we assume that the property holds for product of n elements. Then we have

$$g_1(g_2 \cdots g_{n+1}) = (g_1 g_2)(g_3 \cdots g_{n+1}) = \cdots = (g_1 \cdots g_n)g_{n+1}.$$

All subdivisions of the bracketed elements are equivalent by our inductive hypothesis, so every bracketing of $n + 1$ elements is equivalent. □

There is a slight issue with this last proof, which is that we do not actually know if we have hit all the possible bracketings. To do this we would need to give some (necessarily inductive) definition of a bracketing, which we would then use straightforwardly in the proof. Giving such a definition trivial, and left as an exercise to the reader.

Another nice fact to have are cancellation laws, which we enshrine as a theorem:

Theorem 2.6. *If $gh = gk$, then $h = k$. Likewise, if $hg = kg$, then $h = k$.*

Proof. We simply left- or right- multiply by g^{-1}, as appropriate. □

With some basic properties in place, we move on to what is probably the most important aspect of groups for our purposes: the idea of a *group action*.

2.2 Group Actions and Orbits

One of the main motivation for groups is to capture information about other objects: we can, for instance, describe the rotational and reflectional symmetries of an equilateral triangle using a group. This idea of storing information about other objects is captured by the concept of a group action:

Definition 2.2. A *group action* of G on and set A is a function $\sigma : G \times A \to A$, denoted by a dot $\cdot$ or by juxtaposition, satisfying the following axioms:

1. For all $a \in A$, $e \cdot a = a$.
2. For all $g, h \in G$ and $a \in A$, $(gh) \cdot a = g \cdot (h \cdot a)$, where gh is the group operation.

The following is also important for our discussion of the Modular Group below:

Definition 2.3. If G is a group acting on a set A, and $a \in A$, then the *orbit of a under the group action* is defined to be $Ga = \{ga : g \in G\}$. That is, it is the set of every element of A that can be obtained by some element of G acting on a.

It turns out that the set of orbits of a group action are disjoint, and form a partition of A:

Theorem 2.7. *For all $a, b_1, b_2 \in A$, if $a \in Gb_1$ and $a \in Gb_2$, then $Gb_1 = Gb_2$.*

Proof. Let

$$a = gb_1 \tag{1}$$

$$a = hb_2 \tag{2}$$

$$c = kb_1 \tag{3}$$

for some $c \in A$ and $g, h, k \in G$, so that $c \in Gb_1$. Then $b_1 = k^{-1}c$, and we can plug this into (1) to get $a = gk^{-1}c$. Plugging this into (2) gives $hb_2 = gk^{-1}c \Rightarrow c = kg^{-1}hb_2$, so c is in the orbit of b_2. But c was arbitrary, so every element of the orbit of b_1 is also in the orbit of b_2, completing the proof. □

2.3 The Modular Group

We are now in a position to understand a particular group that will be of use to us: the Modular Group:

Definition 2.4. The *Modular Group*, denoted by Γ, is the set of a linear fraction transformations of the form $(az + b)/(cz + d)$, with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. The group operation is normal functional composition, so that for $\alpha, \beta \in \Gamma$, $\alpha\beta = \alpha \circ \beta$.

Technically, we need to verify that this definition satisfies the group axioms given above. This task is fairly tedious and unenlightening, however, and is left as an exercise to the reader.

With this definition in hand, what we really want to do with Γ is have it act on points in the upper half plane $H = \{z : \mathrm{Im}(z) > 0\}$. The action will be defined in the obvious way:

Definition 2.5. The action of $\mu(z) \in \Gamma$ on a point $\tau \in H$ is given by $\mu(\tau)$.

The following is important step when defining any group action:

Theorem 2.8. *The group action given above is well defined. In particular, given $\mu \in \Gamma$ and $\tau \in H$, $\mu(\tau)$ is also in H.*

Proof. Let $\mu(z) = (az + b)/(cz + d)$, and $\tau = x + iy$. Then

$$\begin{aligned}\mathrm{Im}(\mu(\tau)) &= \mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \mathrm{Re}(a\tau + b)\,\mathrm{Im}\left(\frac{1}{c\tau + d}\right) + \mathrm{Re}\left(\frac{1}{c\tau + d}\right)\mathrm{Im}(a\tau + b) \\ &= (ax + b)\left(\frac{-cy}{|c\tau + d|^2}\right) + (ay)\left(\frac{cx + d}{|c\tau + d|^2}\right) = \frac{(ad - bc)y}{|c\tau + d|^2} = \frac{y}{|c\tau + d|^2} > 0,\end{aligned}$$

giving the desired result. □

We would also like to consider the orbits of Γ. In particular, we would like to define a region of H that contains one point from every orbit. However, there is no reason for this region to be topologically well-behaved, so we set forth the definition of a *fundamental region* of Γ:

Definition 2.6. A region R in H is called a *fundamental region* of Γ given the following properties:

1. If $a, b \in R$ such that $a \neq b$, and S is a orbit of the action of Γ on H, then we do not have both $a \in S$ and $b \in S$, and
2. If $\tau \in H$, then there is a point τ' in the orbit of τ such that $\tau' \in \overline{R}$.

The important thing to note is that applying the group action to all of the points in the closure of one fundamental region will give us a new one. The following theorem, which is outside the scope of this paper, gives a particularly useful fundamental region to work with, which we will call R_Γ:

Theorem 2.9. *The region* $R_\Gamma = \{z : -\frac{1}{2} < \mathrm{Re}(z) < \frac{1}{2}, \quad |z| < 1\}$ *is a fundamental region of* Γ.

3 Modular Functions

We are now in a position to define a modular function. A modular function f is a function that satisfies the following conditions:

Definition 3.1. A *modular function* is a meromorphic function on the upper half plane H which satisfies the following properties:

1. $f(\mu(z)) = f(z)$ for all μ in the modular group Γ.
2. f has a Fourier expansion of the form

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

We would now like to construct an actual example of a modular function. This will be Klein's Modular Function $J(\tau)$.

3.1 Klein's Modular Function

We begin by defining the *Eisenstein Series of order n*, denoted G_n, as

$$G_n(\omega_1, \omega_2) = \sum_{\substack{j,k \in \mathbb{Z} \\ (j,k) \neq (0,0)}} \frac{1}{(j\omega_1 + k\omega_2)^n}$$

for ω_2/ω_1 not real. Of course we must prove convergence:

Theorem 3.1. *The Eisenstein Series G_n converges absolutely if and only if $n > 2$.*

Proof. Let $Q_k = \{z : z = m\omega_1 + n\omega_2,\ m, n \in \mathbb{Z},\ -k \leq m, n \leq k\}$, and $B_k = Q_k \setminus Q_{k-1}$. We have

$$|Q_k| = (2k+1)^2,$$

so

$$|B_k| = (2k+1)^2 - (2k-1)^2 = 8k.$$

Each Q_k lies in a closed filled parallelogram P_k, and each B_k in ∂P_k. We define R to be the maximum distance from 0 to ∂P_1 and r to be the minimum. The P_k are (integer) dilates of each other, which means that the maximum distance from 0 to ∂P_k is just kR, and likewise the minimum is kr. Now for all points $\omega \in B_k$, we will have

$$kr \leq |\omega| \leq kR,$$

$$\frac{1}{(kR)^n} \leq \frac{1}{|\omega|^n} \leq \frac{1}{(kr)^n}$$

so that the partial sums $S_k = \sum_{Q_k} |\omega|^{-n}$ are bounded by

$$\sum_{j=1}^{k} \frac{8j}{(jR)^n} \leq S_k \leq \sum_{j=1}^{k} \frac{8j}{(jr)^n}$$

$$\frac{8}{R^n} \sum_{1}^{k} \frac{1}{j^{n-1}} \leq S_k \leq \frac{8}{r^n} \sum_{1}^{k} \frac{1}{j^{n-1}}.$$

If $n > 2$, so S_k is bounded above by a convergent series, and thus converges. If $n \leq 2$, then S_k is bounded below by a divergent series, and diverges. Thus G_n converges if and only if $n > 2$, as desired. □

We will now use Eisenstein Series to define the following special functions:

$$g_2 = 60G_4, \qquad g_3 = 140G_6, \qquad \Delta = g_2^3 - 27g_3^2.$$

The last of these is called the *discriminant*. We now remind ourselves of the following definition:

Definition 3.2. A function $f(z)$ is *homogeneous of degree k* if for all a and z, $f(az) = a^k f(z)$.

We can use the definitions of g_2, g_3 and Δ to determine that

$$g_2(c\omega_1, c\omega_2) = 60 \sum \frac{1}{(cj\omega_1 + ck\omega_2)^4} = 60c^{-4} g_2(\omega_1, \omega_2)$$

$$g_3(c\omega_1, c\omega_2) = 140 \sum \frac{1}{(cj\omega_1 + ck\omega_2)^6} = 60c^{-6} g_3(\omega_1, \omega_2)$$

$$\Delta(c\omega_1, c\omega_2) = g_2^3(c\omega_1, c\omega_2) - 27g_3^2(c\omega_1, c\omega_2) = c^{-12} g_2^3(\omega_1, \omega_2) - 27c^{-12} g_3^2(\omega_1, \omega_2) = c^{-12} \Delta(\omega_1 \omega_2).$$

Thus g_2, g_3, and Δ are homogeneous of degrees -4, -6, and -12, respectively. What this means in particular is that

$$\Delta(\omega_1, \omega_2) = \omega_1^{-12} \Delta(1, \omega_2/\omega_1),$$

so by re-scaling we can regard Δ as a function of a single variable $\tau = \omega_2/\omega_1$. We do likewise for g_2 and g_3, so that we now have three functions of the single complex variable τ. We can also choose ω_1 and ω_2 such that ω_2/ω_1 has positive imaginary part, so it is sufficient to study what these functions do on H.

We are now in a position to define the *Klein J function*. For ω_1 and ω_2, this is given by

$$J(\omega_1, \omega_2) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)}.$$

But since g_2^3 and Δ are homogeneous of the same order, J is also homogeneous of that order, and we can regard it too as a function of τ. We now need to show that J is a modular function, beginning with

Theorem 3.2. *$g_2(\tau)$, $g_3(\tau)$, $\Delta(\tau)$, and (in particular) $J(\tau)$ are analytic on H.*

Proof. This theorem consists of two parts: showing that $\Delta(\tau) \neq 0$ on H, and showing that $g_2(\tau)$ and $g_3(\tau)$ are analytic. The first part is beyond the scope of this paper. For the second part, we will prove a more general result: that $G_n(\tau)$ is analytic for all $n > 2$. G_n is homogeneous of order n, so it is fine for us to write it as a function of $\tau \in H$; the equation for G_n is then

$$G_n(\tau) = \sum_{\substack{j,k \in \mathbb{Z} \\ (j,k) \neq (0,0)}} \frac{1}{(j + k\tau)^n}.$$

We will prove that this converges absolutely and uniformly on any strip of the form $S = \{\tau = x + iy : |x| \leq A,\ y \geq \delta > 0\}$. To do this, consider

$$\frac{(q+x)^2 + y^2}{1+q^2} > N \tag{4}$$

where $N > 0$ and $q \in \mathbb{Q}$. We want an N such that this holds for all q. If $|q| \leq A + \delta$ then we have

$$\frac{(q+x)^2 + y^2}{1+q^2} \geq \frac{\delta^2}{1+q^2} \geq \frac{\delta^2}{1+(A+\delta)^2}.$$

This last expression doesn't depend on q, so we can take $N = \delta^2/(1 + (A+\delta)^2)$. Conversely, if $|q| > A$, then

$$\left|\frac{x}{q}\right| < \frac{|x|}{A+\delta} \leq \frac{A}{A+\delta} < 1$$

$$\left|1 + \frac{x}{q}\right| \geq 1 \geq 1 - \left|\frac{x}{q}\right| > 1 - \frac{A}{A+\delta} = \frac{\delta}{A+\delta}.$$

Multiplying both sides by q gives

$$|q + x| \geq \frac{q\delta}{A+\delta}$$

$$\frac{(q+x)^2 + y^2}{1+q^2} > (q+x)^2 \cdot \frac{1}{1+q^2} > \frac{\delta^2}{(A+\delta^2)} \cdot \frac{q^2}{1+q^2}.$$

It is the case that $q^2/(1+q^2)$ is increasing as a function of q^2:

$$\frac{q^2}{1+q^2} = \frac{1}{1+\frac{1}{q^2}},$$

as q^2 gets big, $1 + (1/q^2)$ gets small(er), so $q^2/(1+q^2)$ gets larg(er). This tells us that

$$\frac{q^2}{1+q^2} \geq \frac{(A+\delta)^2}{1+(A+\delta)^2},$$

so

$$\frac{(q+x)^2 + y^2}{1+q^2} > \frac{\delta^2}{(A+\delta)^2} \frac{(A+\delta)^2}{1+(A+\delta)^2} = \frac{\delta^2}{1+(A+\delta)^2},$$

which is exactly the value of N that we got in the previous case. Thus we have found and N such that (4) holds for all q.

From here, we need to turn this into something about Eisenstein series. Thankfully, this is not too difficult: substituting $q = j/k$ for some j and k in the sum for $G_n(\tau)$ and multiplying by k^2, we can rearrange (4) as

$$(q+x)^2 + y^2 > K(1+q^2)$$

$$(j+kx)^2 + (ky)^2 > N(j^2 + k^2). \tag{5}$$

Note that our proof above tacitly assumed that $k \neq 0$, but the expression here trivially holds if $k = 0$, for any $0 < N < 1$, so we can modify N to be something like

$$N = \min\left\{\frac{1}{2}, \frac{\delta^2}{1+(A+\delta)^2}\right\}$$

(the specific value 1/2 is not important, just as long as it is strictly between 0 and 1). Now (5) is equivalent to

$$|j + k\tau|^2 > N|j + ki|^2$$

$$\frac{1}{|j+k\tau|^2} \leq \frac{1/N}{|j+ki|^2},$$

which implies

$$\frac{1}{|j+k\tau|^n} \leq \frac{M}{|j+ki|^n}$$

for any $n > 2$ and some $M > 0$. But

$$\sum_{\substack{j,k\in\mathbb{Z}\\(j,k)\neq(0,0)}} \frac{M}{|j+k\tau|^n}$$

converges absolutely by Theorem 3.1, so by the M-test, the series for $G_n(\tau)$ converges absolutely, completing the proof. $\square$

Now we verify property 2:

Theorem 3.3. *If $(az+b)/(cz+d) \in \Gamma$, then*

$$J\left(\frac{az+b}{cz+d}\right) = J(z).$$

Proof. If ω_1 and ω_2 are elements of a lattice Ω, then by Theorem 1.2 we can generate the same sublattice of Ω by $\omega_1' = c\omega_2 + d\omega_1$, and $\omega_2' = a\omega_2 + b\omega_1$. This means that $g_2(\omega_1', \omega_2') = g_2(\omega_1, \omega_2)$, and likewise for g_3, Δ, and, of course, J. Note that we are treating these as functions of the two variables ω_1 and ω_2 here; we would like them in terms of $\tau = \omega_2/\omega_1$. It is only natural to define

$$\tau' = \frac{\omega_2'}{\omega_1'} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1} = \frac{a\tau+b}{c\tau+d}.$$

But this means that $g_2(\tau') = g_3(\tau)$, and thus for g_3, Δ, and J, completing the proof. $\square$

And finally, the Fourier expansion of $J(\tau)$:

Theorem 3.4. *The Fourier expansion of $J(\tau)$ is of the form*

$$J(\tau) = \sum_{-\infty}^{\infty} a_n e^{2\pi i n\tau}.$$

Proof. Let $z = e^{2\pi i\tau}$. If $\tau = a + ib$ is in H, then

$$0 < |z| = |e^{2\pi i\tau}| = |e^{2\pi i a}||e^{-2\pi b}| = e^{-2\pi b} < 1$$

because $b > 0$, so x is in the punctured unit disk $D = \{0 < |x| < 1\}$. Now let $f(z) = J(\tau)$, so that f is defined on the punctured unit disk. Now for each z, there are infinitely many τ such that $z = e^{2\pi i\tau}$. But if we have $z = e^{2\pi i\tau} = e^{2\pi i\tau'}$ for some τ and τ', then $\tau - \tau'$ is an integer. Further, $\tau + 1 \in \Gamma$, so $J(\tau+1) = J(\tau)$. f is therefore well defined. And it is analytic – by the chain rule, we have

$$f'(z) = \frac{d}{dz} J(\tau) = J'(\tau)\frac{d\tau}{dz} = \frac{J'(\tau)}{2\pi i e^{2\pi i \tau}}.$$

Thus f has a Laurent expansion around 0

$$f(z) = \sum_{-\infty}^{\infty} a_n z^n.$$

Substituting back $z = e^{2\pi i \tau}$ gives us the desired result. $\square$

After the previous three theorems, we finally have an example of a modular function. There is also a fact about the certain values of $J(\tau)$ which will be important for Picard's Little Theorem:

Theorem 3.5. *Let ρ be the point $-\frac{1}{2} + i\sqrt{3}$, so that ρ is a "corner" of the fundamental region R_Γ. Then $J(\rho) = 0$ with multiplicity 3 and $J(i) = 0$ with multiplicity 2. In addition, $J(\tau)$ takes every value exactly once in the closure of R_Γ.*

Proof. Noting that $\rho^3 = 1$ and $\rho^2 + \rho + 1 = 0$, we have

$$\frac{1}{60} g_2(\rho) = \sum_{m,n} \frac{1}{(m+n\rho)^4} = \sum_{m,n} \frac{1}{(m\rho^2 + n\rho)^4} = \frac{1}{\rho^4} \sum_{m,n} \frac{1}{(m\rho^2 + n)^4} = \frac{1}{\rho} \sum_{m,n} \frac{1}{n - m - m\rho} = \cdots$$

and setting $N = n - m$ and $M = -m$,

$$\cdots = \frac{1}{\rho} \sum_{m,n} \frac{1}{(N + M\rho)^4} = \frac{1}{60\rho} g_2(\rho),$$

so $g_2(\rho) = 0$. Running through largely the same calculations would give us $g_3(i) = 0$ as well. Plugging these values into the definition of J gives us the desired result. The multiplicities are a result of the following theorem (Theorem 3.6). The other statement follows by Theorems 3.6 and 3.7. $\square$

3.2 Properties

One remarkable property of modular functions, which we will not prove, is the following:

Theorem 3.6. *If f is a non-constant modular function, then f has an equal number of zeros and poles in the in closure of R_Γ.*

In fact, we can extend this theorem by applying it to $f - c$ for any complex number c: this tells us that f takes on every complex value (including infinity) the same number of times in the closure of R_Γ. And if f misses a value, then it must be constant.

Another elegant fact is the following:

Theorem 3.7. *Every rational function of $J(\tau)$ is a modular function, and vice versa. That is, every modular function can be written as a rational function of $J(\tau)$. (For those familiar with them, this shows that the set of modular functions forms a field, isomorphic to the field of rational functions.)*

Proof. The first direction is clear – all the properties of modular functions are satisfied for a rational function of J, as a result of the modularity of J itself. For the other direction, let f be a modular function with zeros at $z_1, \cdots, z_n$ and poles at $p_1, \cdots, p_n$ in the closure of R_Γ, possibly with repetition (so that there may be multiplicities). We then define

$$Q_k(\tau) = \begin{cases} \frac{J(\tau) - J(z_k)}{J(\tau) - J(p_k)} & z_k, p_k \neq \infty \\ 1 & \text{otherwise} \end{cases}$$

$$g(\tau) = \prod_{k=0}^{n} Q_k(\tau).$$

It is clear that g has the same zeros and poles as f in the closure of R_Γ, with the same multiplicities. But this means f/g has no zeros and no poles anywhere. It thus equals some constant c, such that $f = cg$, which is rational, as desired. $\square$

4 Picard's Little Theorem

We are almost in a position to use $J(\tau)$ to prove Picard's Little Theorem - that a entire non-constant analytic function takes on every possible value except possibly one (as in for example the exponential function). Before we do this, though, we will define *simple connected domains* and give a statement of the Monodromy Theorem [2]:

Definition 4.1. A domain D in $\mathbb{C}$ is *simply connected* if it has no "holes" in it. That is, for any closed path P in D, there is a continuous function mapping P to a single point.

Theorem 4.1. ***The Monodromy Theorem****. If f is analytic in a disk contained in a simply connected domain D, and f can be analytically continued along every polygonal arc in D, then f can be analytically continued to a single-valued analytic function on all of D.*

And now, the finale:

Theorem 4.2. ***Picard's Little Theorem****. If f is an entire function, and for any two a and b in $\mathbb{C}$ with $a \neq b$, f never takes on the values a and b, then f is constant on all of $\mathbb{C}$.*

Proof. We begin by defining

$$g(z) = \frac{f(z) - a}{b - a},$$

such that g is entire and g never takes the values on the values 0 or 1. Now by Theorem 3.5, $J(\tau)$ takes every possible value once in the closure of R_Γ, so $J^{-1}(w)$ is a well defined function on $\mathbb{C}$ under a restriction to the codomain R_Γ. By the same theorem, $J'(\tau)$ equals 0 only at $\tau = \rho$ or $\tau = i$, so $J^{-1}(w)$ is analytic everywhere except at $w = 0$ or $w = 1$. Now we define

$$h(z) = J^{-1}(g(z)),$$

such that $h(z)$ is analytic on every open subset of $\mathbb{C}$, as $g(z)$ does not equal 1 or 0. Thus, by the Monodromy Theorem, we have a unique analytic continuation of h to the entire complex plane, so that h is entire. Now we define

$$\phi(z) = \exp(h(z));$$

so that this too is analytic. However, $\mathrm{Im}(h(z)) > 1$, since the codomain of J^{-1} is a subset of H, so

$$|\phi(z)| = e^{-\operatorname{Im} h(z)} < 1.$$

But this means that ϕ is a bounded entire function, and is therefore constant by Liouville's Theorem. But this means that h is constant, such that g is constant, such that f is constant, completing the proof. □

5 References

1. Apostol, Tom M. Modular Functions and Dirichlet Series in Number Theory. 2nd ed. New York: Springer-Verlag, 1990. Print. Graduate Texts in Mathematics ; 41.

2. http://mathworld.wolfram.com/MonodromyTheorem.html;
http://mathworld.wolfram.com/SimplyConnected.html