Jorge Aylón Berzosa

Solving quintic equations via elliptic functions

Universidad de Zaragoza

Directora del trabajo: Concepción María Martínez Pérez

1 de Agosto de 2021

Abstract

Todo matemático conoce el resultado de Galois sobre la irresolubilidad por radicales de los polinomios de grado quinto, redactado en 1831 y famósamente publicado en 1846 de forma póstuma. Si tenemos en cuenta la cantidad de intentos infructuosos que hicieron falta por parte de grandes matemáticos hasta alcanzar este resultado, sorprende la celeridad con que Hermite publicó en 1859, en un libro titutalado "Sur la résolution de l'equation du cinquième degré", un método para resolver cualquier ecuación quíntica recurriendo a ciertas propiedades algebráicas de las funciones elípticas. En este trabajo se explorará ese método, pero el texto al que nos ceñirémos principalmente no será el de Hermite, sino al de los matemáticos Viktor Prasolov y Yuri Solovyev "Elliptic functions and elliptic integrals", publicado en 1997.
Las funciones elípticas son funciones complejas $f : \mathbb{C} \to \mathbb{C}$ doblemente periódicas, i.e., funciones tales que existen $\Omega_1, \Omega_2 \in \mathbb{C}$ para los cuales $f(z+\Omega_i) = f(z)$, $i = 1,2$, de forma que Ω_1 y Ω_2 son linealmente independientes si se consideran como vectores en $\mathbb{R}^2$.

Puesto que el desarrollo necesario para estudiar la conexión entre funciones elípticas y ecuaciones quínticas requiere muchos cálculos bastante onerosos, se corre el riesgo de perder de vista el objetivo final inmersos en cuentas aparentemente innecesarias. Por ello, dejaré aquí un breve esquema del camino a seguir.
Primero, comenzaremos definiendo las funciones theta $\Theta_i(v|\tau)$ para $i = 0,1,2,3$; donde $v, \tau \in \mathbb{C}$ y $\mathrm{Im}(\tau) > 0$. Estas funciones se expresan mediante series de potencias de la siguiente forma:

$$\Theta_0(v|\tau) = \sum_{m=-\infty}^{\infty} (-1)^m q^{m^2} e^{2\pi i m v},$$
$$\Theta_1(v|\tau) = i \sum_{m=-\infty}^{\infty} (-1)^m q^{\left(m-\frac{1}{2}\right)^2} e^{\pi i (2m-1) v},$$
$$\Theta_2(v|\tau) = \sum_{m=-\infty}^{\infty} q^{(m-\frac{1}{2})^2} e^{\pi i (2m-1) v},$$
$$\Theta_3(v|\tau) = \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi i m v};$$

donde $q := q(\tau) = e^{i\pi\tau}$.
Las funciones theta no son doblemente periódicas en v, pero casi. Todas ellas se comportan de manera bastante simple bajo los cambios de variable $v \mapsto v+1$ y $v \mapsto v+\tau$. Por ejemplo, para $\Theta_3(v|\tau)$ se tiene

$$\Theta_3(v+1 \mid \tau) = \Theta_3(v \mid \tau), \Theta_3(v+\tau|\tau) = q^{-1} e^{-2\pi i v} \Theta_3(v|\tau).$$

Esta "casi" periodicidad nos permite considerar cocientes de funciones theta que sí serán doblemente periódicos, y usando propiedas generales de las funciones doblemente periódicas hallaremos información muy útil de las funciones theta.
Eventualmente llegaremos a obtener una expresión de las funciones theta como productos infinitos, lo

que motivará la definición de las siguientes funciones:

$$\eta(\tau) = q^{\frac{1}{2}} \prod_{k=1}^{\infty}(1-q^{2k}),$$
$$f(\tau) = q^{-\frac{1}{24}} \prod_{k=1}^{\infty}(1+q^{2k-1}),$$
$$f_1(\tau) = q^{-\frac{1}{24}} \prod_{k=1}^{\infty}(1-q^{2k-1}),$$
$$f_2(\tau) = \sqrt{2}q^{\frac{1}{12}} \prod_{k=1}^{\infty}(1+q^{2k}).$$

Nuestro principal interés será la función $f(\tau)$, puesto que nos permite definir las funciones

$$u(\tau) = f(\tau), \quad v_c(\tau) = f\left(\frac{\tau + c'}{5}\right) \quad \text{and} \quad v_\infty(\tau) = f(5\tau), \ c = 0,1,2,3,4.$$

(Aquí, c' depende de c; luego veremos exactamente cómo.)
Deduciremos seguidamente que estas funciones satisfacen una ecuación llamada la "ecuación modular":

$$v_c^6 - u^5 v_c^5 + 4uv_c + u^6 = 0, \quad c = 0,1,2,3,4,\infty;$$

Específicamente, si $u = f(\tau)$ se considera como un parámetro, entonces las seis raices del polinomio $v^6 - u^5 v^5 + 4uv + u^6$ vienen dadas por $v = v_c(\tau)$.
Así habremos logrado al fin hallar una conexión clara entre raíces de polinomios y funciones elípticas (aunque las funciones u y v_c no son elípticas, la teoría de funciones elípticas es necesaria para estudiar sus propiedades). La transformación

$$w_z = \frac{(v_\infty - v_z)(v_{z+1} - v_{z-1})(v_{z+2} - v_{z-1})}{\sqrt[5]{u^3}}, \quad z = 0,1,2,3,4;$$

donde los subíndices se entienden módulo 5, nos dan las cinco raíces del polinomio de grado cinco

$$w(w^2+5)^2 - u^{12} + 64u^{-12}.$$

Después, usando la sustitución

$$y(\tau) = \frac{f_1^8(\tau) - f_2^8(\tau)}{f^2(\tau)(w^2(\tau)+5)}$$

se puede obtener la ecuación

$$y^5 + 5y = \frac{f_1^8 - f_2^8}{f^2}.$$

Para concluir, veremos que cualquier ecuación quíntica se puede reducir a la forma $y^5 + 5y - a = 0$ y que

$$af^2(\tau) = f_1^8(\tau) - f_2^8(\tau)$$

siempre se puede resolver para τ. Para eso, veremos que la solución a esta ecuación es un τ tal que

$$f^{24} - a^2 f^{12} - 64 = 0.$$

Esta es una ecuación cuadrática para $t = f^{12}$, con lo cual podemos hallar facilmente sus 24 raíces. Si además podemos invertir $f(\tau)$, entonces sólo quedaría comprobar los valores de τ correspondientes a las 24 raíces, y aquel que satisfaga $af^2(\tau) = f_1^8(\tau) - f_2^8(\tau)$ nos permitirá hallar las raices de la ecuación quíntica original. Así, vemos que si además de invertir potencias (radicales) podemos invertir la función $f(\tau)$, entonces podemos resolver cualquier ecuación quíntica.

Es en este punto donde surgen las dificultades computacionales. El problema de invertir $f(\tau)$ no es en absoluto trivial, y es por esta razón que un resultado aparentemente tan bueno como un algoritmo general para la resolución de ecuaciones quínticas es tan poco conocido: a nivel computacional no ofrece ninguna ventaja, y cualquier método numérico ofrece mejores soluciones. De hecho, implementar este algoritmo en un ordenador demostró ser un problema extremadamente complicado. Los primeros en lograrlo fueron R.B.King y E.R.Canfield, y publicaron su método en un artículo titulado "An algebraic algorithm for calculating the roots of a general quintic equation" en 1991 en el Journal of Mathematical Physics. Su trabajo se basa principalmente en el artículo de Kiepert "Auflösung der Gleichungen Fünften Grades" (1878) y el libro de Klein "Vorlesunger über das Ikosaeder"(1888). Un buen resumen general de sus ideas se puede encontrar en "Beyond the quartic equation" del propio R.B.King.

Contents

Chapter 1

Theory of elliptic functions

In what follows, by function we will mean complex meromorphic function, that is, functions which are analytic in the whole complex plane except perhaps at a set of singularities without an accumulation point.

Definition 1.1. Given a function f, we will say that Ω is a period of f if at each regular point z

$$f(z) = f(z+\Omega) \tag{1.1}$$

For example, $\Omega = 2\pi i$ is a period of the complex exponential e^z.
A simple consequence follows from the definition:

Corollary 1.1. Given a meromorphic function f with periods $\Omega_1, \ldots, \Omega_n$ and integers $m_1, \ldots, m_n$, then

$$m_1\Omega_1 + \ldots + m_n\Omega_n$$

is also a period of f, i.e., the set of periods of f is an abelian group with the usual sum operation.

Now we will see that periodicity behaves well under the usual operations with analytic functions.

Proposition 1.1. Let f and g have period Ω. Then the following functions also have the same period:

$$f(z+c), \quad f(z) \pm g(z), \quad f(z)g(z), \quad \frac{f(z)}{g(z)}, \quad f'(z), \ \ c \in \mathbb{C} \text{ a constant.}$$

Proof. We only have to be a bit more careful with $f'(z)$. Given a regular point z of f, we can find $\delta > 0$ such that f is analytic in the discs $D(z,\delta)$ and $D(z+\Omega,\delta)$. Then, for h with $|h| < \delta$ we have

$$\frac{f(z+\Omega+h) - f(z+\Omega)}{h} = \frac{f(z+h) - f(z)}{h}$$

and we need only take the limit as $h \to 0$. □

Proposition 1.2. Let f be a non-constant periodic function. Then there exists $\mu > 0$ such that every nontrivial period Ω of f satisfies $|\Omega| \geq \mu$

Proof. Assume the contrary and let $z \in \mathbb{C}$ be a nonsingular point of f. We may find a sequence of periods $\{\Omega_k\}_{k=0}^{\infty}$ such that

$$\lim_{k\to+\infty} |\Omega_k| = 0,$$

but then the fact that f is meromorphic implies that there exists some $k_0 \in \mathbb{N}$ such that $z+\Omega_k$ is nonsingular for every $k > k_0$.
We may assume without loss of generality that $k_0 = 0$, but then

$$\frac{f(z) - f(z+\Omega_k)}{\Omega_k} = 0 \text{ for any } k,$$

so it follows that

$$f'(z) = \lim_{k\to+\infty} \frac{f(z) - f(z+\Omega_k)}{\Omega_k} = 0$$

and f is constant, as this holds for every non-singular z. □

1.1 Jacobi's theorem

Definition 1.2. Given a function f with n periods $\Omega_1,\ldots,\Omega_n$, we will say that they form a primitive set of periods if any other period Ω of f can be written as

$$\Omega = m_1\Omega_1 + \ldots + m_n\Omega_n,$$

where $m_1,\ldots,m_n$ are integers, and this cannot be done if we eliminate any Ω_k from the list.

Theorem 1.1. *There does not exist a nonconstant function with a primitive set of periods containing $n \geq 3$ periods. If f is a nonconstant function and Ω,Ω' form a set of two primitive periods of f, then*

$$Im\frac{\Omega}{\Omega'} \neq 0$$

Proof. First we notice that in any bounded subset $A \subset \mathbb{C}$ we can only have a finite number of periods, since otherwise we could find a compact subset C containing A and the periods would have an accumulation point inside of C, wich in turn would yield a sequence of periods $\{\Omega_k\}_{k=0}^{\infty}$ with the property that $\Omega_n - \Omega_m \to 0$ as m and n tend to infinity, so that we could obtain arbitrarily small periods of f contrary to proposition 1.2. Now, given a period Ω, we may consider its integer multiples $m\Omega$, all of which will lie in a straight line L. We consider two separate cases, namely when all the periods of f lie in the line L and when they don't.

1. All the periods of f lie in L:
   Consider the segment of L from $-\Omega$ to Ω. Since it contains finitely many periods, we may assume that Ω is of smallest modulus possible.
   Now notice that any point of L can be expresed as $t\Omega$ for $t \in \mathbb{R}$, and that all the points $m\Omega$ with $m \in \mathbb{Z}$ are periods. Moreover, these exhaust all the periods of f. Indeed, if we had $\Omega' = t\Omega$ some period of f, we could write $t = m + r$ with m an integer and $0 \leq r < 1$, and since $m\Omega$ is a period then $\bar{\Omega} = \Omega' - m\Omega = r\Omega$ is also a period with modulus $r|\Omega|$. But then the only possibility that doesn't contradict our assumption of Ω having the smallest possible modulus is that $r = 0$.

2. Not all the periods of f lie in L:
   Let Ω' be a period not lying in L and consider the triangle with vertices $0,\Omega,\Omega'$. It can only contain a finite number of periods, so by choosing some point in the interior or on the sides of the triangle we arrive at a triangle containing fewer periods. Continuing this process we arrive at a triangle wich only contains three periods lying at its vertices. Clearly we may assume that said triangle is our original one with vertices $0,\Omega,\Omega'$.
   We now consider the parallelogram with vertices $0,\Omega,\Omega',\Omega+\Omega'$; and notice that its "left half" corresponds to our triangle, while the "right half" contains no period except at the vertices: if it did contain some period $\bar{\Omega}_1$, then $\bar{\Omega}_2 = \Omega + \Omega' - \bar{\Omega}_1$ would be a period lying in the "left half" but not on its vertices, contradicting our assumption.
   It is now easy to prove that all the periods of f are of the form $m\Omega + m'\Omega'$ for $m,m' \in \mathbb{Z}$. Indeed, given any period $\bar{\Omega}$ we may write it as $\bar{\Omega} = t\Omega + t'\Omega'$. Letting $t = m + r$ and $t' = m' + r'$ with $m,m' \in \mathbb{Z}$ and $0 \leq r,r' < 1$ we find just as in the previous case that $r\Omega + r'\Omega'$ is also a period lying in the parellelogram, and so the only possibility is that $r = r' = 0$ since it contains no other periods than the vertices.

□

This prompts the following definition:

Definition 1.3. We will say that a function f is elliptic if it has a primitive set of periods containing two periods.

1.2 Existence of elliptic functions

We are now going to prove the existence of elliptic functions. To do so, let us advance the definition of one of the functions that shall be of crucial importance throughout the rest the text, the third theta function. First, let $v, \tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$ and define $q := q(\tau) = e^{i\pi\tau}$. Now we consider the power series

$$\Theta_3(v \mid \tau) = \sum_{m=-\infty}^{\infty} e^{(m^2\tau+2mv)i\pi} = \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi imv}, \text{ for } v, \tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0.$$

Let us assume that τ is fixed and consider $\Theta_3(v \mid \tau)$ as a function of v.
To see that this series converges to an analytic function, notice that the ratio of two consecutive terms has modulus

$$|q^{2m+1} e^{2\pi iv}| \leqslant |q|^{2m+1} e^{2\pi|v|}$$

and since $|q| < 1$, $\lim_{m\to\infty} |q|^{2m+1} = 0$ so that $\Theta_3(v \mid \tau)$ is a series of analytic functions which converge uniformly inside the disk $|v| \leqslant c$ for arbitrary $c \in \mathbb{C}$ and thefore $\Theta_3(v \mid \tau)$ is itself an analytic function. For brevity, we will denote it by $\Theta_3(v)$. Observe that the change of variable $v \to v+1$ leaves all the terms of the series unchanged, so that $\Theta_3(v) = \Theta_3(v+1)$, while

$$\begin{aligned}\Theta_3(v+\tau) &= \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi imv} q^{2m} = q^{-1} e^{-2\pi iv} \sum_{m=-\infty}^{\infty} q^{(m+1)^2} e^{2\pi i(m+1)v} \\ &= q^{-1} e^{-2\pi iv} \Theta_3(v) = A(v)\Theta_3(v),\end{aligned}$$

where

$$A(v) = q^{-1} e^{-2\pi iv}.$$

Notice that here we are also abusing notation a bit, since $A(v)$ does depend indirectly on τ through q. Taking logarithms and deriving two times we get

$$\begin{aligned}\tfrac{d^2}{dv^2} \ln\Theta_3(v+\tau) &= \tfrac{d^2}{dv^2} \ln\Theta_3(v), \\ \tfrac{d^2}{dv^2} \ln\Theta_3(v+1) &= \tfrac{d^2}{dv^2} \ln\Theta_3(v);\end{aligned}$$

so that

$$\phi(v) := \frac{d^2}{dv^2} \ln\Theta_3(v).$$

is an elliptic function. Notice that, since $\frac{d}{dv} \ln\Theta_3(v) = \frac{\Theta_3'(v)}{\Theta_3(v)}$, $\frac{d}{dv} \ln\Theta_3(v)$ only has poles of order one at the zeros of $\Theta_3(v)$ and thus $\phi(v)$ only has poles of order one at the zeros of $\Theta_3(v)$. But $\Theta_3(v)$ is a nonconstant analytic function, so its set of zeros cannot have an accumulation point, which together with the previous observation goes on to say that $\phi(v)$ is meromorphic.

1.3 Liouville's theorems

It is clear that given some fixed $c \in \mathbb{C}$, any elliptic function with $\{\Omega, \Omega'\}$ as a primitive set of periods is completely determined by its values in the parallelogram

$$\Pi_c = \left\{ z \in \mathbb{C} : z = c + r\Omega + r'\Omega' \text{ , where } 0 \leq r, r' < 1 \right\}$$

From now on we will call this Π_c the fundamental parallelogram at c and we will assume furthermore that $\mathrm{Im}\ \frac{\Omega'}{\Omega} > 0$, so that if we run through its vertices $c, c+\Omega, c+\Omega', c+\Omega+\Omega\prime$ in that order it corresponds to the positive orientation.

Theorem 1.2. *The sum of the residues of an elliptic function with respect to any fundamental parallelogram* Π *is equal to zero*

Proof.

$$\int_{\partial\Pi} f(z)dz = \int_c^{c+\Omega} f(z)dz + \int_{c+\Omega}^{c+\Omega+\Omega'} f(z)dz + \int_{c+\Omega+\Omega'}^{c+\Omega'} f(z)dz + \int_{c+\Omega'}^{c} f(z)dz.$$

The first and third integrals cancel each other with a change of variables $z = \zeta + \Omega'$ and the same happens with the second and fourth integrals (by periodicity they are integrals of the same function in opposite directions). □

Definition 1.4. Given $a \in \mathbb{C}$, we will say that $z \in \mathbb{C}$ is an a-point of f if $f(z) = a$, and its multiplicity as an a-point is the least integer k such that $f^{(k)}(z) \neq 0$

Corollary 1.2. The number of poles with multiplicity of a nonconstant elliptic funtion f in a fundamental parallelogram is equal to the number of a-points with multiplicity, for arbitrary a.

Proof. Let

$$\varphi(z) = \frac{f'(z)}{f(z) - a}$$

which is itself an elliptic function. Now if ζ is a pole of order k of f, we have in a neighborhood of ζ

$$f(z) = \frac{g_1(z)}{(z-\zeta)^k}$$

for some $g_1(z)$ analytic with $g_1(\zeta) \neq 0$. Thus

$$\varphi(z) = \frac{f'(z)}{f(z)-a} = \frac{g_1'(z)(z-\zeta) - kg_1(z)}{g_1(z) - a(z-\zeta)^k} \cdot \frac{1}{z-\zeta} = h_1(z)\frac{1}{z-\zeta}$$

with $h_1(\zeta) = -k$ and so

$$\operatorname{res}_{z=\zeta} \varphi(z) = -k,$$

where $\operatorname{res}_{z=\zeta} \varphi(z)$ denotes the residue of $\varphi(z)$ at ζ.
In a similar fashion, if ζ is an a-point of f of multiplicity k we have in a neighborhood of ζ

$$f(z) = a + (z-\zeta)^k g_2(z)$$

with $g_2(z)$ analytic and $g_2(\zeta) \neq 0$, so that again expanding φ

$$\varphi(z) = \frac{g_2'(z)(z-\zeta) + kg_2(z)}{g_2(z)} \cdot \frac{1}{z-\zeta} = h_2(z)\frac{1}{z-\zeta}$$

but in this case $h_2(\zeta) = k$, and so

$$\operatorname{res}_{z=\zeta} \varphi(z) = k$$

Since the a-points of f are all the singular points of $\varphi(z)$, and the sum of all of its residues equals zero, the corollary is proved. □

Theorem 1.3. *(Liouville's theorem) There does not exist a nonconstant elliptic function that is regular in a fundamental parallelogram.*

Proof. In that case the number of poles would be zero, and by the previous result the number of a-points would be zero for arbitrary a, which is absurd. □

Corollary 1.3. Given an elliptic function f, the sum of the orders of its poles must be at least 2.

Proof. The case where f is constant is trivial. The only case that would contradict the assertion would be for f to have a simple pole at a single point ζ_0. But then the residue of f at ζ_0 would be different from 0, contradicting theorem 1.2. □

Chapter 2

Theta functions

Recall how we proceeded to define the third theta function in section 1.2. First, we fix $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$ and let $q := q(\tau) = e^{i\pi\tau}$. Now the theta functions can be defined through the following power series:

$$\Theta_0(v \mid \tau) = \sum_{m=-\infty}^{\infty} (-1)^m q^{m^2} e^{2\pi i m v} \tag{2.1}$$

$$\Theta_1(v \mid \tau) = i \sum_{m=-\infty}^{\infty} (-1)^m q^{\left(m-\frac{1}{2}\right)^2} e^{\pi i (2m-1) v} \tag{2.2}$$

$$\Theta_2(v \mid \tau) = \sum_{m=-\infty}^{\infty} q^{(m-\frac{1}{2})^2} e^{\pi i (2m-1) v} \tag{2.3}$$

$$\Theta_3(v \mid \tau) = \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi i m v} \tag{2.4}$$

We will assume for convenience that τ is fixed and that the theta functions depend only on v, so for brevity we will denote

$$\Theta_i(v) := \Theta_i(v \mid \tau),\ i = 0,1,2,3.$$

Now let

$$A(v) := A(v \mid \tau) = q^{-1} e^{-2\pi i v}. \tag{2.5}$$

By straightforward substitutions we obtain the following indentities:

$$\begin{aligned} &\Theta_k(v+1) = \Theta_k(v) \text{ for } k = 0,3 \text{ and } \Theta_k(v+1) = -\Theta_k(v) \text{ for } k = 1,2 \\ &\Theta_k(v+\tau) = A(v)\Theta_k(v) \text{ for } k = 2,3 \text{ and } \Theta_k(v+\tau) = -A(v)\Theta_k(v) \text{ for } k = 0,1. \end{aligned} \tag{2.6}$$

Moreover, all of the theta functions can be easily expressed in terms of $\Theta_3(v)$ as follows:

$$\begin{aligned} \Theta_0(v) &= \Theta_3\left(v + \frac{1}{2}\right) = \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi i m v} e^{\pi i m} = \sum_{m=-\infty}^{\infty} (-1)^m q^{m^2} e^{2\pi i m v}, \\ \Theta_1(v) &= i e^{-\pi i \left(v - \frac{\tau}{4}\right)} \Theta_3\left(v + \frac{1-\tau}{2}\right) \\ &= i e^{-\pi i \left(v - \frac{\tau}{4}\right)} \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi i m v} e^{\pi i m} e^{-\pi i m \tau} \\ &= i \sum_{m=-\infty}^{\infty} (-1)^m q^{\left(m-\frac{1}{2}\right)^2} e^{\pi i (2m-1) v}, \\ \Theta_2(v) &= e^{-\pi i \left(v - \frac{\tau}{4}\right)} \Theta_3\left(v - \frac{\tau}{2}\right) = e^{-\pi i \left(v - \frac{\tau}{4}\right)} \sum_{m=-\infty}^{\infty} q^{m^2} e^{2\pi i m v} e^{-\pi i m v} \\ &= \sum_{m=-\infty}^{\infty} q^{\left(m-\frac{1}{2}\right)^2} e^{\pi i (2m-1) v}. \end{aligned} \tag{2.7}$$

2.1 Zeros of theta functions

Let us recall the identities in (2.6) and, in particular, $\Theta_1(-v) = -\Theta_1(v)$. Because it is analytic, we inmediately deduce that $\Theta_1(0) = 0$. Moreover, since $\Theta_1(v+1) = -\Theta_1(v)$ and $\Theta_1(v+\tau) = -A(v)\Theta_1(v)$, we see that $\Theta_1(m+n\tau) = 0$ for all $m,n \in \mathbb{Z}$. Let us prove that these are in fact all its zeros. We will proceed using the well-known fact from complex analysis that, given a function f analytic in an open domain U with n zeros in U counting multiplicities, one has

$$\frac{1}{2\pi i}\int_{\partial U}\frac{f'(z)}{f(z)} = n$$

Recall that $A(v) = q^{-1}e^{-2\pi iv} = e^{-i\pi(\tau+2v)}$, so in particular $A(v) \neq 0$. Together with the equations

$$\Theta_1(v+1) = \Theta_1(v)$$

and

$$\Theta_1(v+\tau) = -A(v)\Theta_1(v),$$

we deduce that it is only necessary to study the zeros of $\Theta_1(v)$ inside the parallelogram Π_c of vertices $\frac{\pm 1 \pm \tau}{2}$ (where $c = \frac{-1-\tau}{2}$).
Derivating the two previous equations with respect to v yields

$$\begin{aligned}\Theta_1'(v+1) &= \Theta_1'(v)\\ \Theta_1'(v+\tau) &= -A'(v)\Theta_1(v) - A(v)\Theta_1'(v)\end{aligned}$$

so that

$$\begin{aligned}\frac{\Theta_1'(v+1)}{\Theta_1(v+1)} &= \frac{\Theta_1'(v)}{\Theta_1(v)}\\ \frac{\Theta_1'(v+\tau)}{\Theta_1(v+\tau)} &= \frac{-A'(v)\Theta_1(v) - A(v)\Theta_1'(v)}{-A(v)\Theta_1(v)} = \frac{A'(v)}{A(v)} + \frac{\Theta_1'(v)}{\Theta_1(v)} = -2\pi i + \frac{\Theta_1'(v)}{\Theta_1(v)}.\end{aligned}$$

(Recall that $A(v) = q^{-1}e^{-2\pi iv} = e^{-i\pi(2v+\tau)}$).
Thus, when we integrate $\frac{\Theta_1'}{\Theta_1}$ along the boundary of the parallelogram, the integrals along the vertical sides will cancel each other while at the horizontal lines only the term $2\pi i$ will remain, and therefore

$$\frac{1}{2\pi i}\int_{\partial\Pi}\frac{\Theta_1'(z)}{\Theta_1(z)} = 1.$$

We conclude that all the zeros of $\Theta_1(v)$ are given by $n+m\tau$, $n,m \in \mathbb{Z}$ and they are all simple zeros. If we look at the relations in 2.7, we can see that all the zeros of the theta functions are simple and are given by

function	$\Theta_0(v)$	$\Theta_1(v)$	$\Theta_2(v)$	$\Theta_3(v)$
its zeros	$m+\left(n+\frac{1}{2}\right)\tau$	$m+n\tau$	$m+\frac{1}{2}+n\tau$	$m+\frac{1}{2}+\left(n+\frac{1}{2}\right)\tau$

2.2 The relation $\Theta_3^4 = \Theta_2^4 + \Theta_0^4$

Let $\Theta_i = \Theta_i(0)$ for $i = 0,2,3$ and $\Theta_1' = \Theta_1'(0)$ (this particularity for $\Theta_1(v)$ will be justified in subsequent sections). We will call these constants the theta constants. Let us now fix arbitrary $a,b \in \mathbb{C}$ and consider the function

$$h(v) = \frac{a\Theta_2^2(v) + b\Theta_3^2(v)}{\Theta_0^2(v)}$$

Using the identities in (2.7) to make the substitutions $v \to v+1$ and $v \to v+\tau$, we check that h is an elliptic function. We may now choose a fundamental parallelogram Π so that only the zero $\frac{\tau}{2}$ of $\Theta_0(v)$

lies inside of it. Since $\frac{\tau}{2}$ is neither a zero of $\Theta_2(v)$ nor of $\Theta_3(v)$ we may choose $a,b \neq 0$ such that $a\Theta_2^2(\frac{\tau}{2}) + b\Theta_3^2(\frac{\tau}{2}) = 0$. Recall that in the previous section we said that all the zeros of the theta functions are simple so that at $\frac{\tau}{2}$, h will have a pole of order no more than one. But we have already seen in Liouville's theorem's section, corollary 1.3, that it cannot have a single pole of order one, so it must be constant by theorem 1.2. Substituting $v = 0$ and $v = \frac{\tau}{2}$, respectively, in the relation

$$\Theta_2(v) = e^{-\pi i(v-\frac{\tau}{4})}\Theta_3(v-\frac{\tau}{2}),$$

we get

$$\Theta_2(\frac{\tau}{2}) = e^{-\frac{\pi i\tau}{4}}\Theta_3(0), \text{ and } \Theta_2(0) = e^{\frac{\pi i\tau}{4}}\Theta_3(-\frac{\tau}{2}) = e^{\frac{\pi i\tau}{4}}\Theta_3(\frac{\tau}{2}).$$

Hence,

$$a\Theta_2^2(\frac{\tau}{2}) + b\Theta_3^2(\frac{\tau}{2}) = aB^2\Theta_3^2 + bB^2\Theta_2^2, \text{ where } B = e^{-\frac{\pi i\tau}{4}}.$$

For the particular choice of $a = -\Theta_2^2$ and $b = \Theta_3^2$, the relation $aB^2\Theta_3^2 + bB^2\Theta_2^2 = 0$ is satisfied and thus h is constant or, in other words, there is some $c \in \mathbb{C}$ such that

$$-\Theta_2^2(v)\Theta_2^2 + \Theta_3^2(v)\Theta_3^2 = c\Theta_0^2(v).$$

To compute c, set $v = \frac{1}{2}$. The function Θ_2 vanishes at this point, yielding $\Theta_3^2(\frac{1}{2})\Theta_3^2 = c\Theta_0^2(\frac{1}{2})$. But $\Theta_0(v) = \Theta_3(v+\frac{1}{2})$, and from this we easily derive $\Theta_0 = \Theta_3(\frac{1}{2})$ and $\Theta_0(\frac{1}{2}) = \Theta_3(1)$. All of this implies

$$\Theta_0^2\Theta_3^2 = c\Theta_3^2,$$

and so

$$c = \Theta_0^2.$$

Thus

$$\Theta_3^2(v)\Theta_3^2 - \Theta_2^2(v)\Theta_2^2 = \Theta_0^2(v)\Theta_0^2,$$

and in particular for $v = 0$ we obtain the desired relation

$$\Theta_3^4 = \Theta_2^4 + \Theta_0^4. \tag{2.8}$$

2.3 Representation of theta functions by infinite products

The numbers $m + \frac{1}{2} + (n+\frac{1}{2})\tau$, $m,n \in \mathbb{Z}$ are the zeros of the function

$$\Theta_3(v) = \sum_{m=-\infty}^{\infty} q^{m^2}e^{2\pi ikv}.$$

Set $s = e^{2\pi iv}$. The substitution $v \to s$ sends the zeros of $\Theta_3(v)$ to the points

$$e^{2\pi i(m+\frac{1}{2})}e^{2\pi i(n+\frac{1}{2})\tau} = -q^{2n+1}, \text{ where } q = e^{\pi i\tau}.$$

Let us put these points into two sets:

$$\Lambda_1 = \{-q^{-1}, -q^{-3}, -q^{-5}, \ldots\}$$
$$\Lambda_2 = \{-q^{1}, -q^{3}, -q^{5}, \ldots\}$$

The limit point of Λ_1 is ∞ while that of Λ_2 is 0.
To proceed, we need to briefly recall some results on the convergence of series. Recall the definition of uniform convergence:

Definition 2.1. We say that a sequence of functions f_n converges uniformly to a function f on a set E if for any $\varepsilon > 0$ there exists some $n \in \mathbb{N}$ such that $|f(x) - f_m(x)| < \varepsilon$ for every $m > n$ and $x \in E$.

Thus, knowing that $\sum_{k=1}^{\infty} |q^{2k-1}|$ converges, it is straightforward that the sequence of functions $g_n(s) = \sum_{k=1}^{n} |q^{2k-1}s|$ converges uniformly to $g(s) = |s| \sum_{k=1}^{\infty} |q^{2k-1}|$. Moreover, $g_n(s)$ is bounded on every compact subset $K \subset \mathbb{C}$, so we can guarantee that $\prod_{k=1}^{\infty}(1+q^{2k-1}s)$ converges uniformly on every compact subset $K \subset \mathbb{C}$ (see Walter Rudin's Real and complex analysis[4]; theorem 15.4.)
Hence, on every compact subset of $\mathbb{C}$,

$$h_1(s) = \prod_{k=1}^{\infty}(1+q^{2k-1}s)$$

is the uniform limit of analytic functions, so h_1 is analytic in $\mathbb{C}$ (see Complex analysis by Joseph Bak and Donald J.Newman [5]; theorem 7.6.). It can be seen that its set of zeros if precisely Λ_1 (again theorem 15.4 from Rudin's Real and complex analysis).
Consider also the function

$$h_2(s) = \prod_{k=1}^{\infty}(1+q^{2k-1}s^{-1}).$$

It is clear that $h_2(s) = h_1(\frac{1}{s})$, so it is an entire function except at $s = 0$, and its set of zeros is Λ_2.
Now consider the function $h(s) = h_1(s)h_2(s)$ and let $\tilde{h}(v) = h(e^{2\pi iv})$. From what we have seen, the set of zeros of $\tilde{h}$ is that of $\Theta_3(v)$. We also remark the important fact that, since $e^{2\pi iv} \neq 0$ for all $v \in \mathbb{C}$, we avoid the unique pole of h at $s = 0$ and thus $\tilde{h}(v)$ is entire in $\mathbb{C}$.
The transformation $v \to v+1$ leaves the value $s = e^{2\pi iv}$ unchanged, so $\tilde{h}(v+1) = \tilde{h}(v)$. On the other hand, the change of variables $v \to v+\tau$ replaces s with $e^{2\pi iv}e^{2\pi i\tau} = sq^2$; hence,

$$\begin{aligned}\tilde{h}(v+\tau) &= \prod_{k=1}^{\infty}\left(1+q^{2k+1}s\right)\prod_{k=1}^{\infty}\left(1+q^{2k-3}s^{-1}\right) = \frac{1}{1+qs}\left[\prod_{k=1}^{\infty}\left(1+q^{2k-1}s\right)\right](1+q^{-1}s^{-1})\left[\prod_{k=1}^{\infty}\left(1+q^{2k-1}s^{-1}\right)\right] \\ &= \frac{1+q^{-1}s^{-1}}{1+qs}\tilde{h}(v) = q^{-1}e^{-2\pi iv}\tilde{h}(v)\end{aligned}$$

Recall that $\Theta_3(v+\tau) = A(v)\Theta_3(v) = q^{-1}e^{-2\pi iv}\Theta_3(v)$, and so the function $\frac{\Theta_3(v)}{\tilde{h}(v)}$ is an entire elliptic function, and therefore a constant as we have seen when proving Liouville's theorem. Therefore,

$$\Theta_3(v) = c\prod_{k=1}^{\infty}(1+q^{2k-1}e^{2\pi iv})(1+q^{2k-1}e^{-2\pi iv}). \tag{2.9}$$

We also gather here for future use similar expressions for the rest of the theta functions:

$$\Theta_0(v) = c\prod_{k=1}^{\infty}(1-q^{2k-1}e^{2\pi iv})(1-q^{2k-1}e^{-2\pi iv}) \tag{2.10}$$

$$\Theta_1(v) = 2\sin(\pi v)q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1-q^{2k}e^{2\pi iv})(1-q^{2k}e^{-2\pi iv}) \tag{2.11}$$

$$\Theta_2(v) = 2\cos(\pi v)q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1+q^{2k}e^{2\pi iv})(1+q^{2k}e^{-2\pi iv}) \tag{2.12}$$

These expressions are easily obtained using that of $\Theta_3(v)$ and substituting it in the definition of the other theta functions, but the calculations are lengthy and not very enlightening.
Now, let us prove that

$$c = \prod_{k=1}^{\infty}(1-q^{2k}). \tag{2.13}$$

Consider the sequence of functions

$$F_n(s) = \prod_{k=1}^{n}(1-q^{2k-1}s)(1-q^{2k-1}s^{-1}) = \sum_{k=-n}^{n} a_k(n)s^k.$$

This sequence converges uniformly to the function

$$\prod_{k=1}^{\infty}(1-q^{2k-1}s)(1-q^{2k-1}s^{-1}) = \frac{1}{c}\Theta_0(v) = \frac{1}{c}\sum_{k=-\infty}^{\infty}(-1)^k q^{k^2}s^k.$$

Comparing the coefficients of degree zero in s we get

$$\frac{1}{c} = \lim_{n\to\infty} a_0(n).$$

For every $n \in \mathbb{N}$, observing the coefficient of s^n in the product $\prod_{k=1}^{n}(1-q^{2k-1}s)(1-q^{2k-1}s^{-1})$ we conclude that

$$a_n(n) = (-1)^n q^{1+3+\ldots+(2n-1)} = (-1)^n q^{n^2}.$$

The last equality is obtained by noticing that

$$1+3+\ldots+(2n-1) = (1+2+\ldots+2n) - (2+4+\ldots+2n) = \frac{2n(2n+1)}{2} - 2\frac{n(n+1)}{2} = n^2.$$

Moreover,

$$\frac{F_n(q^2s)}{F_n(s)} = \frac{(1-q^{2n+1}s)(1-q^{-1}s^{-1})}{(1-qs)(1-q^{2n-1}s^{-1})} = -\frac{1-q^{2n+1}s}{qs-q^{2n}},$$

and so

$$(qs-q^{2n})\sum_{k=-n}^{n} a_k(n)q^{2k}s^k = -(1-q^{2n+1}s)\sum_{k=-n}^{n} a_k(n)s^k,$$

i.e.,

$$\sum_{k=-n}^{n} a_k(n)(1-q^{2(n+k)})s^k = \sum_{k=-n}^{n} a_k(n)(q^{2n+1}-q^{2k+1})s^{k+1}.$$

Now, if we compare the coefficients for s in both sums we get

$$a_0(n) = \frac{a_1(n)(1-q^{2(n+1)})}{q^{2n+1}-q^1};$$

comparing the coefficients for s^2

$$a_1(n) = \frac{a_2(n)(1-q^{2(n+2)})}{q^{2n+1}-q^3};$$

and so on. Substituting these equations recursively we eventually reach the expression

$$a_0(n) = a_n(n)\frac{\prod_{k=1}^{n}(1-q^{2(n+k)})}{\prod_{k=0}^{n-1}(q^{2n+1}-q^{2k+1})} = q^{n^2}\frac{\prod_{k=1}^{n}(1-q^{2(n+k)})}{\prod_{k=0}^{n-1}(q^{2k+1}-q^{2n+1})},$$

where we have canceled the term $(-1)^n$ in $a_n(n) = (-1)^n q^{n^2}$ by changing the sign of every factor in the denominator.
We can rewrite this expression in a more convenient way. To do so, we need only observe that

$$\begin{aligned}\prod_{k=0}^{n-1}(q^{2k+1}-q^{2n+1}) &= (q^1-q^{2n+1})(q^3-q^{2n+1})\ldots(q^{2n-1}-q^{2n+1})\\ &= q^{1+3+\ldots+(2n-1)}(1-q^{2n})(1-q^{2n-2})\ldots(1-q^2)\\ &= q^{n^2}\prod_{k=1}^{n}(1-q^{2k}),\end{aligned}$$

hence

$$a_0(n) = q^{n^2} \frac{\prod_{k=1}^{n}(1-q^{2(n+k)})}{\prod_{k=0}^{n-1}(q^{2k+1}-q^{2n+1})} = \frac{\prod_{k=1}^{n}(1-q^{2(n+k)})}{\prod_{k=1}^{n}(1-q^{2k})}.$$

To conclude, we are now going to prove that $\lim_{n\to\infty}\prod_{k=1}^{n}(1-q^{2(n+k)}) = 1$.
First, let $|q|^2 = \alpha < 1$. Since $|q|^{2(n+k)} \leqslant |q|^{2n} = \alpha^n$, we get

$$1-\alpha^n \leqslant |1-q^{2(n+k)}| \leqslant 1+\alpha^n,$$

and so

$$(1-\alpha^n)^n \leqslant \prod_{k=1}^{n} |1-q^{2(n+k)}| \leqslant (1+\alpha^n)^n.$$

Taking logarithms, this yields

$$n\ln(1-\alpha^n) \leqslant \ln\left(\prod_{k=1}^{n} |1-q^{2(n+k)}|\right) \leqslant n\ln(1+\alpha^n).$$

Considering the well-known facts from analysis that $\ln(1+x) \underset{x\to 0}{\sim} x$ and $\lim_{n\to\infty} nx^n = 0$ when $|x| < 1$, we conclude

$$\lim_{n\to\infty} n\ln(1\pm\alpha^n) = 0;$$

hence

$$\lim_{n\to\infty} \ln\left(\prod_{k=1}^{n} |1-q^{2(n+k)}|\right) = 0,$$

i.e.

$$\lim_{n\to\infty} \prod_{k=1}^{n} |1-q^{2(n+k)}| = 1.$$

We have proved converge in modulus, but we will need some further consideration to prove convergence.
Let us then consider the argument function $\arg : \mathbb{C} \to [-\pi, \pi)$.
It can be seen that the following two inequalities hold:

$$-\arctan\left(\frac{|q|^n}{\sqrt{1-|q|^{2n}}}\right) \leqslant \arg(1-q^n) \leqslant \arctan\left(\frac{|q|^n}{\sqrt{1-|q|^{2n}}}\right).$$

The idea is that the problem of maximizing $\arg(1-q^n)$ restricted to $|q| = 1$ is equivalent to maximizing $\left|\frac{y}{x}\right|$ over a circle of radius 1 centered at $(1,0)$, and the second problem can be easily solved with basic analysis techniques using derivatives.
Now, since $|q| < 1$, $\sum_{k=1}^{\infty} |q|^n$ converges. Moreover, $\arctan(x) \sim x$ when $x \to 0$ and $\lim_{n\to\infty}(1-|q|^{2n}) = 1$, so

$$\lim_{n\to\infty} \frac{\arctan\left(\frac{|q|^n}{\sqrt{1-|q|^{2n}}}\right)}{|q|^n} = 1$$

and the limit test for series guarantees the convergence of $\sum_{k=1}^{\infty} \arctan\left(\frac{|q|^n}{\sqrt{1-|q|^{2n}}}\right)$.
Now, for every $n \in \mathbb{N}$ let $\alpha_n = \arg(1-q^n)$. The previous inequality implies that the series $\sum_{k=0}^{\infty} \alpha_k$ converges, and so does in particular the subseries $\sum_{k=1}^{\infty} \alpha_{2k}$.
Let now $\beta_n = \sum_{k=1}^{n} \alpha_{2(n+k)}$. It is a basic fact that the convergence of $\sum_{k=1}^{\infty} \alpha_{2k}$ implies

$$\lim_{n\to\infty} \beta_n = 0.$$

On the other hand

$$\arg\left(\prod_{k=1}^{n} 1-q^{2(n+k)}\right) = \beta_n + n'(2\pi)$$

for some appropriate $n' \in \mathbb{Z}$.
In other words,

$$\prod_{k=1}^{n}(1-q^{2(n+k)}) = \left|\prod_{k=1}^{n}(1-q^{2(n+k)})\right|(\cos(\beta_n)+i\sin(\beta_n)),$$

and since β_n tends to zero while the product converges in modulus, we have

$$\lim_{n\to\infty}\prod_{k=0}^{n}\left(1-q^{2(n+k)}\right) = \left[\lim_{n\to\infty}\prod_{k=0}^{n}\left|1-q^{2(n+k)}\right|\right](\cos(0)+i\sin(0)) = 1.$$

After this long detour, going back to c we simply have

$$c = \lim_{n\to\infty}\frac{1}{a_0(n)} = \prod_{k=1}^{\infty}(1-q^{2k}).$$

2.4 The relation $\Theta_1' = \pi\Theta_0\Theta_2\Theta_3$

Formulas 2.9-2.12 imply that

$$\Theta_0 = \Theta_0(0) = c\prod_{k=1}^{\infty}(1-q^{2k-1})^2 \tag{2.14}$$

$$\Theta_2 = \Theta_2(0) = 2q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1+q^{2k})^2 \tag{2.15}$$

$$\Theta_3 = \Theta_3(0) = c\prod_{k=1}^{\infty}(1+q^{2k-1})^2 \tag{2.16}$$

$$\Theta_1' = \Theta_1'(0) = 2\pi q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1-q^{2k})^2 \tag{2.17}$$

The last equation needs some justification. Using formula 2.11, we get

$$\begin{aligned}\Theta_1'(0) &= \lim_{v\to 0}\frac{\Theta_1(v)}{v} = \lim_{v\to 0}\frac{2\sin(\pi v)q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1-q^{2k}e^{2\pi iv})(1-q^{2k}e^{-2\pi iv})}{v}\\ &= \lim_{v\to 0}\frac{2\sin(\pi v)}{v}q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1-q^{2k})^2 = 2\pi q^{\frac{1}{4}}c\prod_{k=1}^{\infty}(1-q^{2k})^2\end{aligned}$$

where in the last equality we have used the equivalence $\sin x \underset{x\to 0}{\sim} x$.
Now, since $\prod_{k=1}^{\infty}(1-q^{2k})^2 = c^2$, we have $\Theta_1' = 2\pi q^{\frac{1}{4}}c^3$. Therefore, the equation

$$\Theta_1' = \pi\Theta_0\Theta_2\Theta_3$$

will follow from

$$\prod_{k=1}^{\infty}(1-q^{2k-1})(1+q^{2k})(1+q^{2k-1}) = 1. \tag{2.18}$$

This is easy to prove. Indeed, notice that

$$\prod_{k=1}^{m}(1-q^{2k-1})\prod_{k=1}^{m}(1-q^{2k}) = \prod_{k=1}^{2m}(1-q^k),$$

and taking limits

$$\prod_{k=1}^{\infty}(1-q^{2k-1})\prod_{k=1}^{\infty}(1-q^{2k}) = \prod_{k=1}^{\infty}(1-q^k),$$

i.e.

$$\prod_{k=1}^{\infty}(1-q^{2k-1}) = \prod_{k=1}^{\infty}(1-q^k)(\prod_{k=1}^{\infty}1-q^{2k})^{-1} = \prod_{k=1}^{\infty}(1-q^k)(1-q^{2k})^{-1}.$$

On the other hand, it is straightforward that

$$\prod_{k=1}^{\infty}(1+q^{2k})(1+q^{2k-1}) = \prod_{k=1}^{\infty}(1+q^k),$$

and thus

$$\prod_{k=1}^{\infty}(1-q^{2k-1})(1+q^{2k})(1+q^{2k-1}) = \prod_{k=1}^{\infty}(1-q^k)(1-q^{2k})^{-1}(1+q^k) = \prod_{k=1}^{\infty}(1-q^{2k})(1-q^{2k})^{-1} = 1$$

as we wanted.

2.5 Dedekind's η-function and the functions f, f_1, f_2.

Let

$$\eta(\tau) = q^{\frac{1}{12}}\prod_{k=1}^{\infty}\left(1-q^{2k}\right).$$

This function is called Dedekind's eta function. Let us also define the three following functions:

$$f(\tau) = q^{-\frac{1}{24}}\prod_{k=1}^{\infty}\left(1+q^{2k-1}\right),$$

$$f_1(\tau) = q^{-\frac{1}{24}}\prod_{k=1}^{\infty}\left(1-q^{2k-1}\right),$$

$$f_2(\tau) = \sqrt{2}q^{\frac{1}{12}}\prod_{k=1}^{\infty}\left(1+q^{2k}\right).$$

Remember that $q = q_\tau = e^{i\pi\tau}$, so these functions really depend on τ.
Together, these functions allow us to express the theta constants as

$$\Theta_1' = 2\pi\eta^3(\tau),$$
$$\Theta_3 = \eta(\tau)f^2(\tau),$$
$$\Theta_0 = \eta(\tau)f_1^2(\tau),$$
$$\Theta_2 = \eta(\tau)f_2^2(\tau).$$

The relation $\Theta_3^4 = \Theta_2^4 + \Theta_0^4$ implies that

$$f^8 = f_1^8 + f_2^8.$$

We have already seen that

$$\prod_{k=1}^{\infty}(1-q^{2k-1})(1+q^{2k})(1+q^{2k-1}) = 1,$$

and so

$$ff_1f_2 = \sqrt{2}.$$

The functions f, f_1, f_2 can be expressed in terms of η as follows:

$$f(\tau) = \frac{e^{-\frac{\pi i}{24}}\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}; \tag{2.19}$$

$$f_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}; \tag{2.20}$$

$$f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}. \tag{2.21}$$

The necessary calculations are simple comprobations and will be omitted here.

Chapter 3

The modular equation

In this chapter we are going to study the behaviour of the theta functions, Dedekind's η-function and f, f_1, f_2 under several changes of variables of τ. This study will prompt the definition of some new functions $u(\tau), v_c(\tau)$, $c = 0,1,2,3,4,\infty$; that will satisfy the modular equation

$$v^6 - u^5 v^5 + 4u + u^6 = 0,$$

so that given some τ and considering $u(\tau)$ as a parameter for the previous equation, its six roots on v are given by $v = v_c, c = 0,1,2,3,4,\infty$.
We begin considering transformations of the theta functions.

3.1 Transformations of theta functions induced by transformations of τ

We have already seen in the first section how the theta functions are transformed by the changes of variable $v \to v+1$ and $v \to v+\tau$. But if we recall the definition of the theta functions, they are in fact functions of two variables, namely v and τ; that is, $\Theta_i(v) = \Theta_i(v \mid \tau)$, although we assumed τ to be fixed throughout the previous sections. We are now going to check that the changes of variable $\tau \to \tau+1$ and $\tau \to -\frac{1}{\tau}$ also induce simple transformations of the theta functions. For $\tau \to \tau+1$ it is quite easy, since $q = e^{i\pi\tau}$ is transformed to $q' = e^{i\pi(\tau+1)} = e^{i\pi\tau}e^{i\pi} = -q$, and so using formulas 2.1-2.4 we get:

$$\begin{gathered}\Theta_0(v \mid \tau+1) = \Theta_3(v \mid \tau), \quad \Theta_3(v \mid \tau+1) = \Theta_0(v \mid \tau) \\ \Theta_i(v \mid \tau+1) = e^{\frac{\pi i}{4}}\Theta_i(v \mid \tau) \quad \text{for } i = 1,2\end{gathered} \tag{3.1}$$

For the change of variable $\tau \to -\frac{1}{\tau}$, however, we have to get more creative. For the sake of clarity, let $\tau' = -\frac{1}{\tau}$ and define

$$g(v) = e^{i\pi\tau' v^2}\frac{\Theta_3(\tau' v \mid \tau')}{\Theta_3(v \mid \tau)}.$$

Using 2.6 we check that $g(v+1) = g(v)$ and $g(v+\tau) = g(v)$, so that $g(v)$ is a doubly periodic function. The zeros of the denominator are of the form $(m+\frac{1}{2})\tau + (n+\frac{1}{2})$ and the zeros of the numerator are determined by $\tau' v = (m+\frac{1}{2})\tau' + (n+\frac{1}{2})$, and multiplying both sides by $-\tau \neq 0$ we get

$$v = (m+\frac{1}{2}) - (n+\frac{1}{2})\tau,$$

so that the zeros of the numerator coincide with those of the denominator, and it is clear that they have the same multiplicity. Therefore, $g(v)$ is an entire elliptic function and so it is a constant by virtue of Liouville's theorem, $g(v) = A \in \mathbb{C}$. We now have

$$\Theta_3(\tau' v \mid \tau') = Ae^{-i\pi\tau' v^2}\Theta_3(v \mid \tau), \tag{3.2}$$

and recalling how the rest of the theta functions are related to $\Theta_3(v)$ in 2.7, by replacing v consecutively with $v+\frac{1}{2}$,$v+\frac{\tau}{2}$,$v+\frac{1+\tau}{2}$ in 3.2 we get

$$\Theta_2(\tau' v \mid \tau') = Ae^{-i\pi\tau' v^2}\Theta_0(v \mid \tau), \tag{3.3}$$

$$\Theta_0(\tau' v \mid \tau') = Ae^{-i\pi\tau' v^2}\Theta_2(v \mid \tau), \tag{3.4}$$

$$\Theta_1(\tau' v \mid \tau') = iAe^{-i\pi\tau' v^2}\Theta_1(v \mid \tau), \tag{3.5}$$

Let us calculate formula 3.3 as an example. From 2.7 we have

$$\Theta_3\left(v-\frac{\tau}{2}\right) = \Theta_2(v)e^{i\pi\left(v-\frac{\tau}{4}\right)},$$

and substituting $v \mapsto v+\tau$

$$\Theta_3\left(v+\frac{\tau}{2}\right) = \Theta_2(v+\tau)e^{i\pi\left(v+\frac{3}{4}\tau\right)} = \Theta_2(v)e^{-2i\pi v}e^{-i\pi\tau}e^{i\pi\left(v+\frac{3}{4}\tau\right)} = \Theta_2(v)e^{-i\pi\left(v+\frac{\tau}{4}\right)},$$

where we have used 2.6. Making now the substitution $v \mapsto v+\frac{1}{2}$ in 3.2 yields

$$\Theta_3\left(\tau' v+\frac{\tau'}{2} \mid \tau'\right) = Ae^{-i\pi\tau'\left(v+\frac{1}{2}\right)^2}\Theta_3\left(v+\frac{1}{2} \mid \tau\right) = Ae^{-i\pi\tau' v^2}e^{-i\pi\tau'\left(v+\frac{1}{4}\right)}\Theta_0(v),$$

where in the last equality we used the fact that $\Theta_3\left(v+\frac{1}{2}\right) = \Theta_0(v)$.
Finally, using equation $\Theta_3\left(v+\frac{\tau}{2}\right) = \Theta_2(v)e^{-i\pi\left(v+\frac{\tau}{4}\right)}$ to substitute $\Theta_3\left(\tau' v+\frac{\tau'}{2} \mid \tau'\right)$ we obtain

$$e^{-i\pi\left(v\tau'+\frac{\tau'}{4}\right)}\Theta_2(v\tau' \mid \tau') = Ae^{-i\pi\tau' v^2}e^{-i\pi\tau'\left(v+\frac{1}{4}\right)}\Theta_0(v),$$

and after cancelling $e^{-i\pi\tau'\left(v+\frac{1}{4}\right)}$ we get 3.3.
Now, taking the product of equations 3.2-3.4 and setting $v=0$, we get

$$\Theta_2(0 \mid \tau')\Theta_3(0 \mid \tau')\Theta_0(0 \mid \tau') = A^3\Theta_2(0 \mid \tau)\Theta_3(0 \mid \tau)\Theta_0(0 \mid \tau), \tag{3.6}$$

while taking the derivative of 3.5 at $v=0$ yields

$$\tau'\Theta_1'(0 \mid \tau') = iA\Theta_1'(0 \mid \tau). \tag{3.7}$$

Recall that in section 2.4 we saw $\Theta_1' = \pi\Theta_0\Theta_2\Theta_3$, which together with equations 3.6 and 3.7 implies $A^2 = -i\tau$, and so

$$A = \pm\sqrt{-i\tau},$$

and thus

$$\Theta_3(0 \mid \tau') = \pm\sqrt{-i\tau}\Theta_3(0 \mid \tau). \tag{3.8}$$

Now notice that if τ is purely imaginary, $q = e^{i\pi\tau} > 0$ and so $\Theta_3(0 \mid \tau) = \sum_{m=-\infty}^{\infty} q^{m^2} > 0$. Since τ is purely imaginary if and only if $-\frac{1}{\tau} = \tau'$ is purely imaginary, evaluating 3.8 at $\tau = i$, for example, we get

$$A = \sqrt{-i\tau};$$

and in particular

$$\Theta_3\left(0 \mid -\frac{1}{\tau}\right) = \sqrt{-i\tau}\Theta_3(0 \mid \tau). \tag{3.9}$$

3.2 Transformations of Dedekind's η-function and of f, f_1, f_2

Recall the identity we saw in section 2.5

$$2\pi\eta^3(\tau) = \Theta_1'(0 \mid \tau),$$

where the derivative is taken with respect to v. From the relation $\Theta_1'(0 \mid \tau+1) = e^{\frac{\pi i}{4}}\Theta_1'(0 \mid \tau)$ we get

$$\eta(\tau+1) = e^{\frac{i\pi}{12}}\eta(\tau). \tag{3.10}$$

Substituting $A = \sqrt{-i\tau}$ in 3.7 we get

$$\Theta_1'\left(0 \mid -\frac{1}{\tau}\right) = \left(\sqrt{-i\tau}\right)^3\Theta_1'(0 \mid \tau),$$

hence

$$\eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\eta(\tau). \tag{3.11}$$

Now, equations 2.19-2.21 allow us to easily obtain rules of transformation for f, f_1, f_2 by mere substitution:

$$f(\tau+1) = e^{-\frac{i\pi}{24}}f_1(\tau), \tag{3.12}$$

$$f_1(\tau+1) = e^{-\frac{i\pi}{24}}f(\tau), \tag{3.13}$$

$$f_2(\tau+1) = e^{\frac{i\pi}{12}}f_2(\tau), \tag{3.14}$$

$$f_1\left(-\frac{1}{\tau}\right) = f_2(\tau), \tag{3.15}$$

$$f_2\left(-\frac{1}{\tau}\right) = f_1(\tau). \tag{3.16}$$

For $f(-\frac{1}{\tau})$, however, we cannot obtain a simple transformation law using the same method. Nevertheless, if we use the fact that

$$f(\tau)f_1(\tau)f_2(\tau) = \sqrt{2}$$

and make the substitution $\tau \to -\frac{1}{\tau}$, using 3.15 and 3.16, we get

$$f\left(-\frac{1}{\tau}\right)f_1(\tau)f_2(\tau) = \sqrt{2},$$

and so

$$f\left(-\frac{1}{\tau}\right) = f(\tau). \tag{3.17}$$

To conclude this section, we are going to prove the relation

$$f(\tau)f\left(\frac{\tau-1}{\tau+1}\right) = \sqrt{2}. \tag{3.18}$$

First, notice that equations 2.20 and 2.21 imply $f_1(2\tau)f_2(\tau) = \sqrt{2}$. On the other hand, substituting by $2\tau-1$ in equation 3.13 we get

$$f_1(2\tau) = e^{-\frac{i\pi}{24}}f(2\tau-1);$$

while combining 3.15 and 3.12 yields

$$f_2(\tau) = f_1(-\frac{1}{\tau}) = e^{\frac{i\pi}{24}}f\left(1-\frac{1}{\tau}\right).$$

Therefore

$$f(2\tau-1)f\left(1-\frac{1}{\tau}\right)=\sqrt{2},$$

and setting $x=2\tau-1$, then $1-\frac{1}{\tau}$ becomes $\frac{x-1}{x+1}$, so the previous relation can be rewritten as

$$f(\tau)f\left(\frac{\tau-1}{\tau+1}\right)=\sqrt{2}.$$

Notice that $\mathrm{Im}(\tau)>0$ if and only if $\mathrm{Im}(2\tau-1)>0$, so there is no problem with the domain of f.

3.3 Transformations of order 5

Definition 3.1. We will call Möbius transformation or fractional linear transformation any transformation given by

$$\tau\to\frac{a\tau+b}{c\tau+d},$$

where $a,b,c,d\in\mathbb{C}$ are constants.

Throughout the following sections, we will asign to every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ the Möbius transformation $\tau\mapsto\frac{a\tau+b}{c\tau+d}$.
The transformations $\tau\mapsto\tau+1$ and $\tau\mapsto\frac{1}{\tau}$ correspond then to the matrices $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, respectively. Since there will be no possible confusion with any other operation, we will denote the transformation $\tau\mapsto\frac{a\tau+b}{c\tau+d}$ by $\tau\mapsto A\tau$, where $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This has the advantage that the composition of transformations corresponds with the transformation by the product matrix, that is:

$$A(B\tau)=(AB)\tau,\ \text{for any matrices } A,B\in\mathbb{C}^4.$$

This is easily checked: let

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\ \text{and}\ B=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

so that

$$A(B\tau)=\frac{a(\frac{a'\tau+b'}{c'\tau+d'})+b}{c(\frac{a'\tau+b'}{c'\tau+d'})+d}=\frac{aa'\tau+ab'+bc'\tau+bd'}{ca'\tau+cb'+dc'\tau+dd'}=\frac{(aa'+bc')\tau+ab'+d'b}{(ca'+dc')\tau+cb'+dd'}=(AB)\tau.$$

We are now going to consider the group $SL_2(\mathbb{Z})=\{A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\mid \det A=ad-bc=1\}$. It is quite easy to prove that it is in fact a group under multiplication just by using the properties of determinants and the inversion formula $(A)^{-1}=\frac{1}{\det A}\mathrm{adj}(A)$.
We are now going to state a result about the group $SL_2(\mathbb{Z})$ that will prove to be very useful for our purposes:

Theorem 3.1. *The group $SL_2(\mathbb{Z})$ is generated by the elements $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*

Proof. See Serre's A course in arithmetic [6], chapter 7 section 1. □

We now observe that, under our new notation, equations (3.10) and (3.11) become

$$\eta(T\tau) = e^{\frac{i\pi}{\tau}}\eta(\tau),$$
$$\eta(S\tau) = \sqrt{-i\tau}\eta(\tau).$$

Therefore, the previous theorem allows us to write $\eta(A\tau)$ in terms of $\eta(\tau)$ for any $A \in SL_2(\mathbb{Z})$. We can do the same for $f(A\tau)$, but with the slight incovenience that since $f(\tau+1) = e^{-\frac{i\pi}{24}}f_1(\tau)$ we will also need to consider the functions $f_1(\tau)$ and $f_2(\tau)$. Let now $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be an integer matrix with determinant 5 and consider the relatively prime numbers $c = \frac{r}{\gcd(p,r)}$, $d = -\frac{p}{\gcd(p,r)}$. They satisfy $cp + dr = 0$ and, moreover, since they are relatively prime we may find integers a and b such that $ad - bc = 1$.Thus

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p' & q' \\ 0 & s' \end{pmatrix},$$

with $p's' = 5$. We also note the fact that

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p & q \\ 0 & s \end{pmatrix} = \begin{pmatrix} p & q+ns \\ 0 & s \end{pmatrix},$$

therefore we can reduce P to the form $\begin{pmatrix} p & q \\ 0 & s \end{pmatrix}$ with $-\frac{s}{2} \leqslant q \leqslant \frac{s}{2}$.

We can also change the sign of any matrix P since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$, so we may assume $p, s > 0$.

This together with the fact that 5 is prime leaves us with only two possibilities: either $p = 1$ and $s = 5$ or $p = 5$ and $s = 1$.

Thus, any integer matrix P with determinant 5 can be reduced to one of the following forms:

$$P_\infty = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \quad P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \quad P_{\pm 1} = \begin{pmatrix} 1 & \pm 1 \\ 0 & 5 \end{pmatrix}, \quad P_{\pm 2} = \begin{pmatrix} 1 & \pm 2 \\ 0 & 5 \end{pmatrix}.$$

The purpose of this is to consider the functions $f(P_c\tau)$ and study their behaviour under changes of parameter of the form $\tau \mapsto A\tau$, $A \in SL_2(\mathbb{Z})$. Since they correspond to the right multiplication of P_c by A, we may reduce P_cA to one of the matrices P_d, $d = 0,1,2,3,4,\infty$, allowing us to express $f(P_c\tau)$ in terms of $f(P_d\tau)$.

To make calculations easier, however, one doesn't exactly study the functions $f(P_c\tau)$. Instead, one defines

$$v_c(\tau) = f\left(\frac{\tau + c'}{5}\right), \; c = 0,1,2,3,4;$$
$$v_\infty(\tau) = f(5\tau),$$

where c' is chosen such that $c' \equiv 0 \pmod{48}$ and $c' \equiv c \pmod 5$. We will consider the three transformations $\tau \mapsto \tau + 2$, $\tau \mapsto -\frac{1}{\tau}$ and $\tau \mapsto \frac{\tau-1}{\tau+1}$.

The reason why it is more convenient to study these functions as well as all the calculations can be found in Prasolov and Soloviev's Elliptic functions and elliptic integrals [1], sections 7.10 to 7.12; but here we will just recollect the results in the following table:

$$\begin{array}{cccccccc} & u & v_\infty & v_0 & v_1 & v_2 & v_3 & v_4 \\ \tau \mapsto \tau+2 & \varepsilon u & \varepsilon v_\infty & \varepsilon v_2 & \varepsilon v_3 & \varepsilon v_4 & \varepsilon v_0 & \varepsilon v_1 \\ \tau \mapsto -\frac{1}{\tau} & u & v_0 & v_\infty & v_4 & v_2 & v_3 & v_1 \\ \tau \mapsto \frac{\tau-1}{\tau+1} & \frac{\sqrt{2}}{u} & -\frac{\sqrt{2}}{v_1} & -\frac{\sqrt{2}}{v_4} & -\frac{\sqrt{2}}{v_0} & -\frac{\sqrt{2}}{v_2} & -\frac{\sqrt{2}}{v_3} & -\frac{\sqrt{2}}{v_\infty} \end{array} \tag{3.19}$$

where $\varepsilon = e^{-\frac{\pi i}{12}}$.

3.4 Functions invariant under certain transformations of τ

In the next section we will finally derive the modular equation, but to do so we need one more theoretical result whose proof would unfortunately take us too long.
Let

$$F(\tau) = f^{24}(\tau) + \frac{2^{12}}{f^{24}(\tau)} = q^{-1}\prod_{k=1}^{\infty}\left(1+q^{2k-1}\right)^{24} + 2^{12}q\prod_{k=1}^{\infty}\left(1+q^{2k-1}\right)^{-24}. \tag{3.21}$$

Recall the relations 3.12, 3.13, 3.17 and 3.18. Combining the first two relations one obtains $f(\tau+2) = e^{-\frac{i\pi}{12}} f(\tau)$ and so together with the other two relations we see that $F(\tau)$ is invariant under the changes of parameter $\tau \to \tau+2, \tau \to -\frac{1}{\tau}$ and $\tau \to \frac{\tau-1}{\tau+1}$. Actually, a much stronger result holds:

Theorem 3.2. *Let $g(\tau)$ be a meromorphic function defined in the upper half plane $H = \{\tau \in \mathbb{C} \mid Im\ \tau > 0\}$, $g : H \mapsto \mathbb{C}$; and such that it is invariant under the transformations $\tau \to \tau+2, \tau \to -\frac{1}{\tau}$ and $\tau \to \frac{\tau-1}{\tau+1}$. If under the change of parameter $q = e^{i\pi\tau}$ the resulting function $\tilde{g}(q) = g\left(\frac{\log(q)}{i\pi}\right)$ is meromorphic, then $g(\tau) = R(F(\tau))$ where R is some rational function; $R \in \mathbb{C}(X)$.*

In fact, a bit more can be said about this.
The equation $F(\tau) = \alpha$ is solvable for any $\alpha \in \mathbb{C}$. Therefore, if $R(F(\tau))$ is finite for every τ with $F(\tau) \neq \infty$, then R is a polynomial, because otherwise it would have a non-constant denominator with a zero at some point $\alpha \in \mathbb{C}$ and solving $F(\tau) = \alpha$ we would have $R(F(\tau)) = \infty$. A full discussion about this section can be found in Elliptic functions and elliptic integrals [1], sections 7.16 to 7.20.

3.5 Deriving the modular equation

With the help of 3.19 we find that the functions uv_c and u/v_c are transformed by the following laws:

	uv	$\frac{u}{v}$
$\tau \longmapsto \tau+2$	$e^{-\frac{\pi i}{2}}uv$	$e^{\frac{\pi i}{3}}\frac{u}{v}$
$\tau \mapsto \tau-\frac{1}{\tau}$	uv	$\frac{u}{v}$
$\tau \mapsto \frac{\tau-1}{\tau+1}$	$-\frac{2}{uv}$	$-\frac{v}{u}$

In this table we understand that, although the subscript c of v does not appear explicitly, it undergoes the same transformation as in 3.19. For example, the transformation $\tau \mapsto -\frac{1}{\tau}$ sends uv_∞ to uv_0.
Let us consider the functions

$$A_c = \left(\frac{u}{v_c}\right)^3 + \left(\frac{v_c}{u}\right)^3,$$
$$B_c = (uv_c)^2 - \frac{4}{(uv_c)^2}.$$

Their corresponding transformation table is given by:

	A	B
$\tau \mapsto \tau+2$	$-A$	$-B$
$\tau \mapsto -\frac{1}{\tau}$	A	B
$\tau \mapsto \frac{\tau-1}{\tau+1}$	$-A$	$-B$

where the subscript changes in the same fashion as in the previous the table. Then, the function

$$\prod_c (A_c - B_c)^2, \quad c = 0,1,2,3,4,\infty$$

does not vary under any of the previous transformations of τ.
Recall that $f(\tau) = q^{-\frac{1}{24}}\prod_{k=1}^{\infty}(1+q^{2k-1})$ with $q := q(\tau) = e^{-i\pi\tau}$. Thus, letting

$$p(q) = \prod_{k=1}^{\infty}(1+q^{2k-1})$$

we may write $f(\tau) = q^{-\frac{1}{24}} p(q)$ and $f(5\tau) = q^{-\frac{5}{24}} p(q^5)$. This will allow us to write $A_\infty(\tau)$ and $B_\infty(\tau)$ in a more convenient form.

$$\begin{aligned} A_\infty(\tau) &= \left(\frac{f(\tau)}{f(5\tau)}\right)^3 + \left(\frac{f(5\tau)}{f(\tau)}\right)^3 = \frac{f(\tau)^6 + f(5\tau)^6}{f(\tau)^3 f(5\tau)^3} = \frac{q^{-\frac{6}{24}} p(q)^6 + q^{-\frac{30}{24}} p(q^5)^6}{q^{-\frac{18}{24}} p(q)^3 p(q^5)^3} \\ &= \frac{q^{\frac{1}{2}} p(q)^6 + q^{-\frac{1}{2}} p(q^5)^6}{p(q)^3 p(q^5)^3}, \\ B_\infty(\tau) &= (f(\tau) f(5\tau))^2 - \frac{4}{(f(\tau) f(5\tau))^2} = \frac{(f(\tau) f(5\tau))^4 - 4}{(f(\tau) f(5\tau))^2} = \frac{q^{-1}(p(q)p(q^5))^4 - 4}{q^{-\frac{1}{2}}(p(q)p(q^5))^2} \\ &= \frac{q^{-\frac{1}{2}}(p(q)p(q^5))^4 - 4q^{\frac{1}{2}}}{(p(q)p(q^5))^2}. \end{aligned}$$

In the following discussion, we will change our point of view for convenience and consider the functions A_∞ and B_∞ as functions of q or of τ depending on what we are trying to prove.
We know that $p(q)$ is analytic inside the unit disk, and it is inmediate that $p(0) = 1$. Hence, we may find a neighborhood U_0 of 0 in wich $p(q)$ and $p(q^5)$ are analytic and non-zero. Using the previously obtained expressions for $A_\infty(q)$ and $B_\infty(q)$, we see that in said neighborhood

$$q^{\frac{1}{2}} A_\infty(q) = \frac{q p(q)^6 + p(q^5)^6}{p(q)^3 p(q^5)^3}, \text{ and } q^{\frac{1}{2}} B_\infty(q) = \frac{(p(q)p(q^5))^4 - 4q}{(p(q)p(q^5))^2}$$

are also analytic. Evaluating at $q = 0$ we see that both functions equal 1.
The purpose of this is to use Taylor's theorem to write

$$q^{\frac{1}{2}} A_\infty(q) = 1 + o_1(q),\ q^{\frac{1}{2}} B_\infty(q) = 1 + o_2(q);$$

where $o_1(q)$ and $o_2(q)$ denote as usual little oes of q when $q \to 0$. Thus we have

$$\lim_{q\to 0} A_\infty(q) - B_\infty(q) = \lim_{q\to 0} q^{-\frac{1}{2}}(o_1(q) - o_2(q)) = \lim_{q\to 0} \frac{(o_1(q) - o_2(q))}{q^{\frac{1}{2}}} = 0,$$

i.e., $A_\infty(q) - B_\infty(q)$ vanishes at $q = 0$ or, equivalently, when $\mathrm{Im}(\tau) \to \infty$ (since $q = e^{i\pi\tau}$). But this also proves that $A_\infty(q) - B_\infty(q)$ doesn't have an essential singularity at $q = 0$, in fact it doesn't have a singularity at all, and moreover it is finite for all q.
This is in fact true for all $A_c(\tau) - B_c(\tau)$. Indeed, $c' \equiv 0 \pmod{48}$ while equations 3.12 and 3.13 combined yield $f(\tau + 2) = e^{-\frac{i\pi}{12}} f(\tau)$. Therefore, the following is straightforward:

$$u(5\tau - c') = f(5\tau) = v_\infty(\tau).$$

Also,

$$v_c(5\tau - c') = f\left(\frac{5\tau - c' + c'}{5}\right) = f(\tau) = u(\tau)$$

and therefore

$$A_c(5\tau - c') = A_\infty(\tau),\quad B_c(5\tau - c') = B_\infty(\tau);$$

and because $\mathrm{Im}(\tau) \to \infty$ if and only if $\mathrm{Im}(5\tau - c') \to \infty$, it is also true that $A_\infty(q) - B_\infty(q)$ vanishes at $q = 0$ (i.e., when $\mathrm{Im}(\tau) \to \infty$). Therefore, $\prod_c (A_c - B_c)^2$ doesn't have any singularities and theorem 3.2 guarantees that

$$\prod_c (A_c - B_c)^2 = R(F(\tau)),\ R \text{ some rational function.}$$

Furthermore, because $\prod_c (A_c - B_c)^2$ is finite for every τ, we may conclude that R is in fact a polynomial. Using this fact, we can prove that $\prod_c (A_c - B_c)^2$ is constant.
Indeed, we know that as $\mathrm{Im}(\tau) \to \infty$, $\prod_c (A_c - B_c)^2 \to 0$. Let then

$$\tau(t) = ti,$$

and notice that $q(t) = e^{i\pi\tau(t)} = e^{-\pi t} \xrightarrow{t\to+\infty} 0$, and therefore

$$|f(\tau(t))| = |q^{-\frac{1}{24}}(t)\prod_{k=1}^{\infty}(1+q^{2k-1}(t))| \xrightarrow{t\to+\infty} +\infty.$$

But then

$$|F(\tau(t))| = \left| f^{24}(\tau(t)) + \frac{2^{12}}{f^{24}(\tau(t))} \right| \xrightarrow{t\to+\infty} \infty,$$

so as $t \to +\infty$, $F(\tau(t))$ tends to infinity in norm while $R(F(\tau(t))) \to 0$, and it is a basic fact from algebra that then R has to be a constant since we already know it is a polynomial. Hence, $\prod_c (A_c - B_c)^2$ is constantly equal to zero and for some $c = 0,1,2,3,4,\infty$ $A_c(\tau) - B_c(\tau) = 0$ for all τ, but then all $A_c(\tau) - B_c(\tau)$ are equal to zero because of equalities

$$A_c(5\tau - c') = A_\infty(\tau), \quad B_c(5\tau - c') = B_\infty(\tau);$$

This result can be neatly written as follows:

$$\left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3 = (uv)^2 - \frac{4}{(uv)^2}$$

or equivalently,

$$v^6 - u^5v^5 + 4uv + u^6 = 0. \tag{3.20}$$

We have finally arrived to the modular equation, the keystone for solving the general quintic equation. What's interesting about this equation is that fixing $u(\tau) = f(\tau)$ we may consider it as function of v, in wich case its six roots turn out to be $v = v_c(\tau)$ for $c = 0,1,2,3,4,\infty$.

3.6 Solving quintic equations

In order to get our hands on the quintic, we need to transform the modular equation into something of degree 5. To do so, let

$$w_c = \frac{(v_\infty - v_c)(v_{c+1} - v_{c-1})(v_{c+2} - v_{c-2})}{\sqrt{5}u^3}, \text{ for } c = 0,1,2,3,4.$$

(the subscripts are understood modulo 5, except of course when it is ∞). Again we obtain one (last) table:

$$\begin{array}{cccccc} & w_0 & w_1 & w_2 & w_3 & w_4 \\ \tau \mapsto \tau+2 & -w_2 & -w_3 & -w_4 & -w_0 & -w_1 \\ \tau \mapsto -\frac{1}{\tau} & w_0 & w_2 & w_1 & w_4 & w_3 \\ \tau \mapsto \frac{\tau-1}{\tau+1} & -w_0 & -w_3 & -w_4 & -w_2 & -w_1 \end{array} \tag{3.22}$$

The transformations $\tau \to \tau + 2$ and $\tau \to -\frac{1}{\tau}$ are straightforward. For $\tau \to \frac{\tau-1}{\tau+1}$ we need one extra observation.

Recall the modular equation, 3.20. We have said that for a fixed τ and regarded as a polynomial in v, its six roots are given by the $v_c(\tau)$. Therefore, since u^6 is the independent term Vieta's theorem implies that

$$\prod v_c = u^6.$$

With this in mind, let's carry out the computations for w_1 as an example:

$$\begin{aligned} w_1 &= \frac{(v_\infty - v_1)(v_2 - v_0)(v_3 - v_4)}{\sqrt{5}u^3} = \frac{1}{\sqrt{5}}\left(\frac{v_\infty}{u} - \frac{v_1}{u}\right)\left(\frac{v_2}{u} - \frac{v_0}{u}\right)\left(\frac{v_3}{u} - \frac{v_4}{u}\right) \\ &\xrightarrow{(\tau\to\frac{\tau-1}{\tau+1})} \frac{1}{\sqrt{5}}\left(\frac{u}{v_0} - \frac{u}{v_1}\right)\left(\frac{u}{v^4} - \frac{u}{v_2}\right)\left(\frac{u}{v_\infty} - \frac{u}{v_3}\right) = \frac{u^3(v_1 - v_0)(v_2 - v_4)(v_3 - v_\infty)}{\sqrt{5}\prod v_c} \\ &= \frac{(v_1 - v_0)(v_2 - v_4)(v_3 - v_\infty)}{\sqrt{5}u^3} = -w_3 \end{aligned}$$

The rest are obtained in the same manner.
Consider now the following polynomial:

$$\prod_{i=0}^{4}(w-w_i) = w^5 + a_1 w^4 + a_2 w^4 + a_3 w^2 + a_4 w + a_5. \tag{3.23}$$

Recalling how the coefficients of a polynomial may be expressed in terms of its roots, we easily conclude from the table 3.22 that a_1^2, a_2, a_3^2, a_4 and a_5^2 are invariant under the changes $\tau \mapsto \tau+2$, $\tau \mapsto -\frac{1}{\tau}$ and $\tau \to \frac{\tau-1}{\tau+1}$. Also, the way we have defined the w_i's, it is clear that the coefficients of this polynomial are finite whenever $u \neq \infty, 0$. Since these are the only possible values of u for wich $u^{24}+2^{12}u^{-24} = F(\tau)$ is infinite, the last observation from section 3.4 allows us to conclude that the a_i's are polynomials on $F(\tau) := u^{24}+2^{12}u^{-24} = q^{-1}\prod_{k=1}^{\infty}\left(1+q^{2k-1}\right)^{24} + 2^{12}q\prod_{k=1}^{\infty}\left(1+q^{2k-1}\right)^{-24}$. We have already discussed how the infinite products that appear are analytic inside the unit disk, so that there is only one pole of order 1 given by the factor q^{-1} of $q^{-1}\prod_{k=1}^{\infty}(1+q^{2k-1})^{24}$. The upshot of this observation is that a polynomial in ζ will have degree n if and only if it has a pole of order n at $q=0$.
With this in mind, one may calculate the smallest appearing power of q for each of the a_i's to find out their degrees. To clarify what we mean exactly by "smallest appearing power of q", recall that

$$f(\tau) = q^{-\frac{1}{24}}\prod_{k=1}^{\infty}(1+q^{2k-1}).$$

The infinite product, as we have just said, is analytic inside the unit disk, which allows us to express it as an infinite series

$$\prod_{k=1}^{\infty}(1+q^{2k-1}) = \sum_{n=0}^{\infty}\alpha_n q^n;$$

so that

$$f(\tau) = q^{-\frac{1}{24}}\prod_{k=1}^{\infty}(1+q^{2k-1}) = \sum_{n=0}^{\infty}\alpha_n q^{n-\frac{1}{24}},$$

and since $\alpha_0 = 1$ we can say that the smallest appearing power of q is $q^{-\frac{1}{24}}$. This will make our work much easier, since the coefficients a_i are products of the functions $v_c(\tau) = f\left(\frac{\tau+c'}{5}\right)$, so we will be able to know if they have a pole at $q=0$, and if so its order, just by looking at the smallest appearing powers of q in the functions $v_c(\tau)$.

It is easy to see that for $c \neq \infty$ the first term in the expansion of $v_c(\tau)$ is $\left(e^{\frac{\pi i(\tau+c')}{5}}\right)^{-\frac{1}{24}} = \left(e^{\frac{\pi i c'}{5}}\right)^{-\frac{1}{24}} q^{-\frac{1}{120}}$, while for $c=\infty$ it is $q^{-\frac{5}{24}}$.
Letting $\alpha = e^{-\frac{4\pi i}{5}}$, it can be easily checked that $e^{-\frac{\pi i c'}{120}} = \alpha^{c'}$ just by using the fact that $c' \equiv 0 \pmod{48}$.
Hence, the first term in the expansion of w_z is

$$\frac{q^{-\frac{5}{24}}q^{-\frac{1}{120}}\left(\alpha^{z+1}-\alpha^{z-1}\right)q^{-\frac{1}{120}}\left(\alpha^{z+2}-\alpha^{z-2}\right)}{\sqrt{5}q^{-\frac{1}{8}}} = \lambda q^{-\frac{1}{10}},$$

where $\lambda = \frac{\alpha^{2z}(\alpha^3-\alpha-\alpha^{-1}+\alpha^3)}{\sqrt{5}} = \alpha^{2z}$, since

$$a^3-\alpha-\alpha^{-1}+\alpha^{-3} = 2(\cos\frac{12\pi}{5}+\cos\frac{4\pi}{5}) = 2(\cos\frac{2\pi}{5}+\cos\frac{4\pi}{5}) = \sqrt{5}.$$

Because in the expression of a_s in terms of the w_i's there appears sums of products of s different roots w_i, the expansion of a_s begins with the term $q^{-\frac{s}{10}}$. Thus, the functions a_1^2, a_2, a_3^2, a_4 are constant while a_5^2 is a linear polynomial of $u^{24}+2^{12}u^{-24} = q^{-1}+\ldots$, because its expansion begins with $(\alpha^2\alpha^4\alpha^6\alpha^8)^2q^{-1} = q^{-1}$. In both expressions q^{-1} appears with coefficient 1, so

$$A_5^2 = u^{24} + \frac{2^{12}}{u^{24}} + C.$$

We are now going to calculate the value of the constants C, a_1, a_2, a_3, a_4, and for this we need only calculate the value of the v_c's for one τ.
For convenience, let $\tau = i$. Since $-\frac{1}{i} = i$, by 3.15 we have

$$f_1(i) = f_2(i).$$

Moreover, recalling their expressions as infinite products of q we have that for a purely imaginary τ, f, f_1, and f_2 are real and positive. Therefore, relations $f^8 = f_1^8 + f_2^8$ and $f f_1 f_2 = \sqrt{2}$ together with $f_1(i) = f_2(i)$ imply that $f = \sqrt[4]{2}$.
Now, since $(2-i)(2+i) = 5$, $\frac{i-2}{5} = -\frac{1}{2+i}$ and so

$$v_3(i) = f\left(\frac{i+48}{5}\right) = f\left(\frac{i-2}{5} + 10\right) = e^{-\frac{10\pi i}{24}} f\left(\frac{i-2}{5}\right) = e^{-\frac{10\pi i}{24}} f(i+2) = e^{-\frac{\pi i}{2} f(i)} = -i\sqrt[4]{2}.$$

Similarly, $v_2(i) = i\sqrt[4]{2}$.
But these are two roots of the modular equation when $\tau = i$, which takes the form

$$v^6 - a^5 v^5 + a^9 v + a^6 = 0,$$

where $a = \sqrt[4]{2}$. Dividing by $(v - v_2)(v - v_3) = v^2 - a^2$ yields

$$v^4 - a^5 v^3 + a^2 v^2 + a^7 v + a^4$$

This equation turns out to have two double roots. Indeed, assume that for some $\alpha, \beta \in \mathbb{C}$ we have

$$v^4 - a^5 v^3 + a^2 v^2 + a^7 v + a^4 = (v - \alpha)^2 (v - \beta)^2.$$

Comparing coefficients, this will happen if and only if

$$\begin{aligned} \alpha + \beta &= a, \\ \alpha\beta &= -a^2. \end{aligned}$$

But these are too the equations for the roots of $v^2 - av - a^2$, which we can easily solve to obtain

$$\begin{aligned} \alpha &= \frac{a(1+\sqrt{5})}{2}, \\ \beta &= \frac{a(1-\sqrt{5})}{2}. \end{aligned}$$

So, the rest of the v_i's must assume either the value α or β. Knowing this, we can skip a lot of computations: observe that

$$v_\infty(i) = f(5i) = f(-\frac{1}{5i}) = f(\frac{i}{5}) = v_0(i).$$

We have also mentioned that for purely imaginary values of τ, $f(\tau)$ assumes real and positive values, so that necessarily

$$v_\infty(i) = v_0(i) = \alpha$$

since $\beta < 0 < \alpha$. The remaining values are necessarily the other two roots of the modular equation, i.e.,

$$v_1(i) = v_4(i) = \beta.$$

With this at hand, it is easy to calculate the corresponding w_i's for $\tau = i$. They are

$$w_0 = 0, w_1 = w_2 = i\sqrt{5}, w_3 = w_4 = -i\sqrt{5},$$

and thus the corresponding fifth degree polynomial is

$$w(w - i\sqrt{5})^2 (w + i\sqrt{5})^2 = w(w^2 + 5)^2.$$

This implies that

$$a_5^2(i) = 0,$$

and so

$$C = -\left(u^{24}(i) + \frac{2^{12}}{u^{24}(i)}\right) = -2^6 - 2^6 = -2^7.$$

Hence

$$a_5^2(i) = u^{24} + \frac{2^{12}}{u^{24}} - 2^7 = \left(u^{12} - \frac{2^6}{u^{12}}\right)^2,$$

and therefore

$$a_5 = \pm\left(u^{12} + \frac{2^{12}}{u^{12}}\right).$$

Recalling that $A_5 = w_0 w_1 w_2 w_3 w_4$ and $u(\tau) = q^{-\frac{1}{24}} \prod_{k=1}^{\infty}(1+q^{2k-1})$ it is easily seen that

$$\lim_{q\to 0} q^{\frac{1}{2}} a_5 = -\lim_{q\to 0} q^{\frac{1}{2}} u = 1,$$

so that

$$a_5 = -u^{12} + \frac{2^6}{u^{12}}.$$

Thus, equation 3.23 takes the form

$$w(w^2+5)^2 = u^{12} - 64u^{-12}.$$

Using relations $f^8 = f_1^8 + f_2^8$ and $f f_1 f_2 = \sqrt{2}$ one can check that

$$u^{12} - \frac{2^6}{u^{12}} = \frac{f^{24} - 64}{f^{12}} = \left(\frac{f_1^8 - f_2^8}{f^2}\right)^2.$$

Thus,

$$\sqrt{w(\tau)} = \pm\frac{f_1^8(\tau) - f_2^8(\tau)}{f^2(w^2(\tau)+5)}.$$

Now, setting

$$y(\tau) = \frac{f_1^8(\tau) - f_2^8(\tau)}{f^2(\tau)(w^2(\tau)+5)},$$

we have

$$y^5 + 5y = y(y^4+5) = y(w^2+5) = \frac{f_1^8 - f_2^8}{f^2}.$$

Now, given a quintic equation of the form $y^5 + 5y = a$, $a \in \mathbb{C}$; if we can find some τ such that

$$\frac{f_1^8(\tau) - f_2^8(\tau)}{f^2(\tau)} = a, \tag{3.24}$$

then we can easily find the roots of $y^5 + 5y = a$ by first calculting all the $v_c(\tau)$, then the $w_z(\tau)$ and finally the $y_z(\tau)$, which will be the roots of $y^5 + 5y = a$.
In fact, we can simplify 3.24 a bit. Squaring it, we get

$$f_1^{16}(\tau) + f_2^{16}(\tau) - 2f_1^8(\tau) f_2^8(\tau) = a^2 f^4(\tau).$$

Squaring the relation $f^8 = f_1^8 + f_2^8$ one gets $f^{16} = f_1^{16} + f_2^{16} + 2f_1^8 f_2^8$. This together with $f f_1 f_2 = \sqrt{2}$ yields $f^{16}(\tau) - \frac{64}{f^8(\tau)} = a^2 f^4(\tau)$, and multiplying by $f^8(\tau)$ gives

$$f^{24}(\tau) - a^2 f^{12}(\tau) - 64 = 0,$$

which is a quadratic equation for $t = f^{12}(\tau)$. For a full discussion on the solvability of equation 3.24, see Elliptic functions and elliptic integrals by Prasolov and Soloviev [1],sections 7.16 to 7.18.

Chapter 4

The Bring-Jerrard form of a quintic equation

For completeness, we are going to briefly discuss how the general quintic

$$x^5 + px^4 + qx^3 + rx^2 + sx + t = 0 \qquad (*)$$

can be reduced to the Bring-Jerrard form

$$x^5 + x + u = 0.$$

This is basically done in two steps. First, for a suitable quadratic transformation

$$y = x^2 + ax + b,$$

the corresponding values of y for each root of (*) satisfy a quintic equation of the form

$$y^5 + A_1 y^2 + A_2 y + A_3 = 0.$$

This is called the principal quintic form.

The principal quintic can in turn be simplified to the form

$$z^5 + B_1 z + B_2 = 0$$

by a quartic transformation

$$z = y^4 + ay^3 + by^2 + cy + d.$$

Finally, the scaling $\zeta = \frac{1}{\sqrt[4]{B_1}} z$ transforms the previous equation into

$$\zeta^5 + \zeta + u = 0.$$

To begin, we first need one definition:

Definition 4.1. Given two polynomials $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $q(x) = b_0 + b_1 x + \ldots + b_m x^m$ over a commutative ring R, we will call the resultant of p and q, and denote it by $\mathrm{Res}(p(x), q(x))$, the following determinant:

$$\mathrm{Res}(p(x), q(x)) = \begin{vmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_n & a_{n-1} & \cdots & \vdots & b_m & b_{m-1} & \cdots & \vdots \\ 0 & a_n & \ddots & \vdots & 0 & b_m & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{n-1} & \vdots & \vdots & \ddots & b_{m-1} \\ 0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_m \end{vmatrix}$$

In the previous matrix it was assumed for simplicity that $n = m$, but the way to construct it for any n, m is straightforward considering that the resulting matrix needs to be $(n+m) \times (n+m)$.

The importance of the resultant for our purposes is that, given two bivariate polynomials $p(x,y), q(x,y) \in \mathbb{C}[X,Y]$, if one considers them as polynomials $\bar{p}(x), \bar{q}(x)$ in X over the ring $\mathbb{C}[Y]$, the resultant $\mathrm{Res}(\bar{p}(x), \bar{q}(x))$ is a polynomial in Y whose roots are precisely the y-coordinates of the common roots of $p(x,y)$ and $q(x,y)$. For simplicity, one usually denotes the resultant in the variable X as

$$\mathrm{Res}_x(p(x,y), q(x,y)) := \mathrm{Res}(\bar{p}(x), \bar{q}(x))$$

Knowing this, let us proceed with the first transformation. Let

$$p(x,y) = p(x) = x^5 + px^4 + qx^3 + rx^2 + sx + t = 0$$

and

$$q(x,y) = x^2 + ax + b - y.$$

Notice that solving $p(x)$ and then calculating y from the Tschirnhausen transformation $y = x^2 + ax + b$ is the same as finding the y-coordinates of the common roots of $p(x,y)$ and $q(x,y)$.
Hence, we consider

$$\mathrm{Res}_x(p(x,y), q(x,y)) = y^5 + c_1 y^4 + c_2 y^3 + c_3 y^2 + c_4 y + c_5,$$

where

$$\begin{aligned} c_1 &= -p^2 + 2q + pa - 5b, \\ c_2 &= q^2 - 2pr + 2s - pqa + 3ra + qa^2 + 4p^2 b - 8qb - 4pab + 10b^2. \end{aligned}$$

(The calculations for this are quite tedious to do by hand. In wolframalpha.com, one can use the command "Collect[Resultant[$x^5 + px^4 + qx^3 + rx^2 + sx + t$, $y - (x^2 + ax + b)$, x],y]" and check the coefficients for y^4 and y^3).
One then solves for b in $c_1 = 0$ in terms of a and substitutes in c_2 to solve $c_2 = 0$ as a quadratic polynomial in a.

For the final step, consider the quintic equation

$$y^5 + uy^2 + vy + w = 0$$

together with the quartic Tschirnhausen transformation

$$z = y^4 + py^3 + qy^2 + ry + s.$$

Using resultants as before yields a quintic equation for z:

$$z^5 + d_1 z^4 + d_2 z^3 + d_3 z^2 + d_4 z + d_5 = 0,$$

where

$$\begin{aligned} d_1 &= -5s + 3pu + 4v, \\ d_2 &= 10s^2 - 12psu + 3p^2u^2 - 3qu^2 + 2q^2 v - 16sv + 5puv + 6v^2 + 5pqw + r(3qu + 4pv + 5w), \\ d_3 &= e_3 r^3 + e_2 + e_1 r + e_0, \end{aligned}$$

with e_3, e_2, e_1 some polynomials in p, q, s.
The expressions we have chosen for d_2 and d_3 reveal that r is going to have a special role. Indeed, one first solves

$$3qu + 4pv + 5w = 0$$

and obtains $q = \frac{-5w - 4pv}{3u}$ (where $u \neq 0$, for otherwise the quintic would already be in Bring-Jerrard form). Then, one finds p from $d_1 = 0$ and substitutes the obtained values for p and q in d_2, so that $d_2 = 0$ can be solved as a quadratic in s. Finally, one then solves $d_3 = 0$ as a cubic equation in r.

Bibliography

[1] Viktor Prasolov and Yury Solovyev. *Elliptic functions and elliptic integrals*. American Mathematical Society, 1997.

[2] Vladimir G. Tkachev. *Elliptic functions introduction course* . https://users.mai.liu.se/vlatk48/teaching/lect2-agm.pdf

[3] Ian Stewart. *Galois theory*. Chapman and Hall/CRC, 2004.

[4] Walter Rudin. *Real and complex analysis.* McGraw Hill international editions, 1987.

[5] Joseph Bak and Donald J. Newman. *Complex analysis.* Springer, 2010.

[6] Jean-Pierre Serre. *A course in arithmetic.* Springer, 1996.