Universidad Nacional de Tucumán
Facultad de Ciencias Exactas y Tecnología
Departamento de Matemática

Funciones elípticas y Curvas elípticas

Tesis para obtener el grado de Magister en Matemática

MARÍA de las MERCEDES GANIM

Director: Dr. ROBERTO MIATELLO
Directora Asociada: Lic. MARÍA LUISA OLIVER

2015

Agradecimientos

Primero que nada quiero agradecer a Dios y a mis padres, José y Rosa, por la vida, la fe, sus enseñanzas y los buenos momentos compartidos.

A José Luis mi marido, a mis hijos Pablo, Sabrina, Damián y José Manuel quienes me acompañan y apoyan siempre, aún cuando les quito tiempo de descanso por mi estudio y trabajo.

A mis hermanos Nelly, José, Rodolfo, Luis, Viviana y Valeria, porque están siempre disponibles para mí. A mis cuñados y sobrinos porque me acompañan en los buenos y malos momentos.

Saliendo un poco de la familia y entrando a la matemática ···

A Marita y Nina, mis jefas-colegas-amigas. Me ayudaron a encontrar mi lugar académico, exigiéndome a ser mejor cada día, apoyándome siempre y brindándome su amistad.

A mis compañeras del grupo NUGIM Nina, Marita, Eugenia R., Cecilia, Eugenia G., Nadia, Matesa, Cuqui, Nachy y Mara, por aceptarme como soy y trabajar sin descanso.

A Isabel L. por ser una colega-amiga silenciosa, que sabe decir las palabras justas.

A Eugenia G, gracias por dedicar tu tiempo para enseñarme y ayudarme con el latex.

Al profe Roberto M., mi director, gracias por su infinita paciencia, por su tiempo, por sus explicaciones, por aclararme un montón de cosas, por las correcciones, por no dejarme flaquear.

A Marita, mi co-directora y guía, un ejemplo a seguir. Siempre me hiciste sentir capaz. Gracias por tus conocimientos y dedicación, por tus aportes, por leer y corregir, varias veces, los borradores de esta tesis.

A la profe Isabel D. por tener fe en mi y brindarme su apoyo.

A Adriana, gracias por tus aportes, paciencia y dedicación.

A Marcela y Ana, quienes estuvieron a la par, especialmente con expedientes y papeles.

A mi cátedra, a los integrantes del Departamento de Matemática y a las autoridades de la FACET.

A mis profesores y maestros.

A mis alumnos.

¡Muchas Gracias!

.

Resumen

Trabajos de importantes matemáticos y físicos del siglo XIX sobre las integrales elípticas, impulsaron el estudio de las funciones elípticas, pero recién a partir de la segunda mitad del siglo XX este tema logra un desarrollo espectacular, particularmente por sus propiedades teóricas y por su importancia en Algebra y Teoría de Números.

El objetivo de este trabajo, es desarrollar la teoría de las funciones y curvas elípticas con una mirada clásica desde la Variable Compleja. Las funciones elípticas son funciones meromorfas doblemente periódicas, asociadas a un lattice Ω y constituyen un cuerpo que denotamos por $\mathbb{C}(\Omega)$. Existen dos funciones elípticas básicas: $\wp$ y $\wp'$ llamadas "funciones de Weierstrass" vinculadas por una ecuación diferencial cuyos coeficientes son invariantes respecto del lattice. Estas funciones proporcionan un sistema de generadores del cuerpo $\mathbb{C}(\Omega) = \mathbb{C}(\wp, \wp')$ y determinan una parametrización meromorfa de la curva elíptica E $y^2 = 4x^3 - g_2x - g_3$. Los coeficientes g_2 y g_3 se obtienen de las Series de Eisenstein G_{2k} de peso 4 y 6 respectivamente, al ser evaluadas en el lattice. Esto resuelve el problema de uniformización euclídea de las curvas elípticas. La demostración se obtiene a partir de las propiedades de la función j (invariante modular).

La parametrización de una curva elíptica mediante las funciones de Weierstrass y la ley de grupo, proporcionan las fórmulas de adición. Es decir, $\wp$ y $\wp'$ establecen un isomorfismo aditivo entre puntos de un toro complejo con retículo Ω y el grupo abeliano $E(\mathbb{C})$ de los puntos complejos de la curva elíptica correspondiente.

Se definen las funciones y las formas modulares a partir de la acción, en el semiplano superior complejo H, de $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{R})$ dada por $\gamma(z) = \dfrac{az+b}{cz+d}$, $z \in H$, ya que constituye un grupo de automorfismos holomorfos.

Las funciones modulares son funciones meromorfas de H^* y periódicas respecto de un subgrupo de $SL(2,\mathbb{Z})$. Estas funciones modulares elípticas respecto de subgrupos discretos, hicieron posible el estudio de las funciones elípticas. La función j es una función meromorfa en H^* con un único polo simple de residuo 1, ubicado en el infinito que cumple: $j(\gamma(z)) = j(z)$, para toda $\gamma \in SL(2,\mathbb{Z})$, poniendo de manifiesto su invariancia respecto del grupo modular. La función queda determinada por sus valores en un dominio fundamental F por la acción del grupo modular $PSL(2,\mathbb{Z})$ en H. Actualmente se define: $j(z) := 1728\,\dfrac{{g_2}^3(z)}{\Delta}$, $z \in H$.

Se demuestra que las formas modulares no cuspidales M_{2k} son generadas por múltiplos complejos de G_{2k} para $k < 6$ y para los demás son suma directa de éstos con un múltiplo de la función discriminante Δ (forma modular cuspidal de peso 12).

Del desarrollo de G_{2k} en el infinito, se obtiene una normalización de las funciones de Eisenstein donde los coeficientes involucran los números de Bernoulli y la función $\sigma_{2k-1}(n)$, suma de la potencia $2k-1$ de los divisores de n. Esto ilustra el hecho general de que los coeficientes de Fourier de las formas modulares son funciones aritméticas importantes.

Como aplicación se describe la utilización de curvas elípticas en Criptografía, área de creciente importancia que actualmente forma parte de los estándares industriales.

Introducción

La teoría de las funciones elípticas es una línea de estudio importante del análisis complejo del siglo XIX, conectado a nombres como Gauss, Abel, Jacobi y Weierstrass.

Sin duda uno de los grandes temas de trabajo de Legendre fueron las funciones elípticas, dedicándose con pasión y perseverancia al estudio de las integrales elípticas[1] que aparecían tantas veces en la matemática y en sus aplicaciones. Entre 1811 y 1817 publicó resultados, propiedades y aplicaciones de las integrales elípticas a diferentes problemas de geometría y de mecánica. Y alrededor de 1827, Legendre con sus discípulos C. Jacobi y N.H. Abel, completaron su trabajo y publicaron el "Tratado de funciones elípticas".

A partir de estos resultados, se abrió un importante campo de investigación, logrando un avance espectacular a partir de los aportes de Liouville, de C. Hermite y de K. Weierstrass, entre otros.

Si bien fueron matemáticos y físicos quienes impulsaron el estudio de las funciones elípticas, recién en la segunda mitad del siglo XX, este tema logró la atención de grandes matemáticos, a quienes se debe el descubrimiento de importantes propiedades teóricas, especialmente para el Álgebra y Teoría de Números.

Actualmente, las investigaciones sobre las funciones elípticas son variadas y se trabaja en el campo de las funciones de variable compleja. En este sentido, fueron apareciendo sus propiedades características, tales como su doble período, las cuales necesitan de un mayor formalismo matemático, para su comprensión y demostración.

Por otro lado, enunciados sencillos tales como, *si dos triángulos tienen áreas y perímetros iguales, ¿son congruentes?*, dieron lugar al desarrollo de la *teoría de curvas elípticas*. Actualmente el estudio de las *curvas elípticas* es un área central de investigación en teoría de números, vinculadas a las *formas modulares* y con aplicaciones a los sistemas criptográficos, especialmente en aquellos sistemas en los que se apoyan las transacciones financieras por Internet.

La teoría de las curvas elípticas tiene importantes aplicaciones, de ellas se mencionan:

- *El problema de los números congruentes* enunciado por un matemático persa en el siglo XaC, un número racional N se dice congruente si existe un triángulo con aristas racionales cuya área es N. Este fue uno de los siete problemas del milenio que *Clay Mathematics Institute* dotó en el año 2000, con un premio de un millón de dólares para

[1] Históricamente las integrales elípticas se utilizaron para calcular longitudes de arcos de elipses y las funciones elípticas fueron estudiadas como inversas de éstas, por ello su nombre.

quien aportara la solución a cualquiera de ellos. La solución se apoya en la conjetura de Birch−Swinnerton−Dyer sobre curvas elípticas. Se demostró que N es un número congruente si y sólo si la curva elíptica $y^2 = x^3 - N^2x = x(x-N)(x+N)$ tiene un punto racional diferente de $(0,0), (\pm N, 0)$ y del punto infinito de la curva.

- *Teorema de Fermat.* En 1985, G. Frey observó que si $A^n + B^n = C^n$ era un contraejemplo del último teorema de Fermat, entonces la curva elíptica de ecuación $y^2 = x(x-A^n)(x+B^n)$ tendría discriminante $-(A^nB^n(A^n+B^n))^2 = -(ABC)^{2n}$. Tal curva contradice la conjetura de Taniyama. En 1995 A. Wiles[2] pudo demostrar el último teorema de Fermat a partir de la conexión, esbozada por Frey y demostrada por Ken Ribet en 1985, de que una demostración de la llamada Conjetura de Taniyama-Shimura conduciría directamente a una demostración del último teorema de Fermat. En resumen, la conjetura de Taniyama-Shimura establece que cada curva elíptica puede asociarse unívocamente con un objeto matemático denominado forma modular. Si el último teorema de Fermat fuese falso, entonces existiría una curva elíptica tal que no puede asociarse con ninguna forma modular y por lo tanto la conjetura de Taniyama-Shimura sería falsa. Por lo tanto, Taniyama-Shimura demuestra el último teorema de Fermat.

- En 1985 Koblitz y Miller aseguraron que la Criptografía con Curvas Elípticas (ECC - Elliptic curve cryptography) que es una variante de la criptografía asimétrica o de clave pública basada en las curvas elípticas, puede usar claves más cortas, ser más rápida y proporcionar un nivel de seguridad equivalente al de los métodos tradicionales, RSA (algoritmo descripto en 1977 por Rivest, Shamir y Adleman del Instituto Tecnológico de Massachusetts) o ELGamal (cifrado descripto en 1984 por el egipcio Taher Elgamal), pero utilizando un número menor de dígitos. El obtener claves más pequeñas resulta muy útil para la seguridad en aplicaciones basadas en circuitos integrados y tarjetas inteligentes.

En este trabajo, el objetivo principal es introducirnos en la teoría de las funciones elípticas con una mirada clásica desde la Teoría de Variable Compleja, para luego establecer su relación y vínculo con las curvas elípticas y las formas modulares.

El material que se desarrolla en esta tesis, se basa principalmente en el libro *Complex Functions* de *Jones and Singerman* [2]. En él se estudian las funciones elípticas como funciones meromorfas con doble período, asociadas a un lattice Ω, en el plano complejo $\mathbb{C}$. Para el abordaje y profundización de la relación con curvas elípticas y formas modulares fueron fundamentales los textos *A Course in Arithmetic* de *Serre* [3] y *Elliptic curves* de *Knapp* [4].

[2] Sir Andrew John Wiles (nació en Cambridge, Inglaterra, en 1953) es un matemático británico. Alcanzó fama mundial en 1993 por exponer la demostración del último teorema de Fermat, que aunque en esa oportunidad resultó fallida, finalmente logró completarla correctamente en 1995.

En la primera Sección se revisan las ideas principales y propiedades de las funciones meromorfas con simple y doble período. De las propiedades del conjunto de períodos, se establece que, excluyendo las funciones constantes, en $\mathbb{C}$ sólo existen funciones simple o doblemente periódicas que sean analíticas o meromorfas. Y con su representación por exponenciales, se muestra que *toda función de período $\omega \in \mathbb{C}$ se puede expresar como función con período conocido* para luego encontrar un desarrollo de Fourier.

En la segunda Sección se estudian los lattices Ω, asociados a una función meromorfa doblemente periódica. Se define Congruencia módulo Ω y región fundamental. Se demuestra que el paralelogramo P, con vértices $0\,,\ \omega_1\,,\ \omega_1+\omega_2\,,\ \omega_2$, es un paralelogramo fundamental del lattice $\Omega = \langle \omega_1, \omega_2 \rangle$ de $\mathbb{C}$ y se denomina *paralelogramo especial* a cada paralelogramo fundamental P del lattice Ω tal que su frontera no contiene ceros ni polos de la función f periódica. Concepto imprescindible para las demostraciones.

A partir de una correspondencia particular, entre pares de lados de un paralelogramo fundamental, se encuentra el espacio resultante $\mathbb{T}$ que se conoce como *toro bidimensional*. De la correspondencia entre Ω-órbita sobre $\mathbb{C}$ y puntos de $\mathbb{T}$, es claro que $\mathbb{T}$ resulta ser el espacio cociente $\mathbb{C}/\Omega$. Luego, una función doblemente periódica f se considera como una función definida sobre el toro $\mathbb{T}$ y recíprocamente toda función definida sobre $\mathbb{T}$ se puede considerar como una función doblemente periódica sobre $\mathbb{C}$.

Una *función elíptica* es toda función meromorfa, doblemente periódica respecto de un lattice de $\mathbb{C}$. Esta definición se incluye de manera formal en la tercera Sección del trabajo. Allí se define *orden* de una función elíptica f como el número de soluciones de la ecuación $f(z) = \infty$ y se demuestra que es igual al número de polos y al número de ceros de la función en el interior del paralelogramo especial, contando multiplicidades. También se demuestran los siguientes resultados:

- Una función elíptica que no tiene polos es constante.
- La suma de los residuos de una función elíptica, en el interior de un paralelogramo especial es cero.
- Una función elíptica no constante tiene igual cantidad de polos que de ceros.
- Dada una función elíptica respecto del lattice Ω, la suma de sus ceros y la suma de sus polos, contados con su multiplicidad, son números conguentes $(mod\,\Omega)$.
- No existen funciones elípticas con un polo simple.
- El cociente de dos funciones elípticas que tienen el mismo lattice de períodos, las mismas clases de polos y las mismas clases de ceros, con el mismo orden, es una constante diferente de cero.
- Si dos funciones elípticas tienen el mismo lattice de períodos, las mismas clases de polos con las mismas partes principales difieren en una constante.

Fue *Weierstrass* quien propuso la función más simple que cumple con lo requerido, función que hoy lleva su nombre, la **función $\wp(z)$ de Weierstrass**:

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega\in\Omega}{}' \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \quad \left(\sum{}' \text{ indica } \omega \neq 0\right)$$

Fijado un lattice, hay dos funciones elípticas básicas: $\wp(z)$ y $\wp'(z)$, llamadas *las funciones de Weierstrass*. En la cuarta Sección, se muestran características principales de estas dos funciones, se demuestra el teorema que establece la ecuación diferencial que ellas satisfacen y se muestra que sus coeficientes son invariantes respecto del lattice. Se determina la importancia del discriminante de la ecuación y se encuentran valores críticos.

A partir de la estructura de cuerpo del conjunto generado por las funciones de Weierstrass, en la Sección cinco, se enuncian dos teoremas para construir funciones elípticas *con ceros y polos dados* y *con polos y parte principal dada*, en esos polos.

En la Sección seis, a partir de las propiedades topológicas, se visualiza a $\mathbb{C}/\Omega$ como un toro de $\mathbb{R}^3$ por el efecto de $\widehat{\wp}$ sobre $\mathbb{C}/\Omega$ que identifica cada clase $[z]$ con $[-z]$. Por ser un toro complejo es una variedad compleja sobre $\mathbb{R}$ de dimensión compleja 1, es de la forma $T_\Omega = \mathbb{C}/\Omega$, donde Ω es un lattice en $\mathbb{C}$, o sea $\Omega = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$ donde $\omega_1\,, \omega_2$ son linealmente independientes sobre $\mathbb{R}$. Se establece que dos *toros* son *conformemente equivalentes* o biholomorfos, si los lattices que los determinan son $\mathbb{C}$-equivalentes, es decir, uno de ellos se obtiene del otro mediante una homotecia y rotación.

La Sección siete se refiere a *Curvas Elípticas*, es decir al conjunto de soluciones de una ecuación cúbica particular con coeficientes en $\mathbb{C}$. Con un sistema de referencia adecuado y sustituciones convenientes, toda curva elíptica se expresa en la *forma de Weierstrass*, donde la función $\wp$, asociada al lattice Ω en $\mathbb{C}$, satisface la ecuación diferencial

$$(\wp')^2 = 4x^3 - g_2 x - g_3\ , \quad \textit{siendo} \quad g_2 = 60\sum_{\omega\in\Omega}{}'\omega^{-4}\ , \quad g_3 = 140\sum_{\omega\in\Omega}{}'\omega^{-6}$$

Se analizan y estudian estos particulares coeficientes, invariantes respecto del lattice y vinculados con las Series de Eisenstein de peso 4 y 6 respectivamente. Se estudian las curvas elípticas reales y se demuestra el teorema de las equivalencias entre *coeficientes reales* de una curva elíptica, función $\wp$ real y lattice real. Se visualizan las diferentes gráficas, según el signo del discriminante de la ecuación.

A partir del teorema de adición para funciones trigonométricas, se analiza un procedimiento general para funciones racionales y se obtiene un teorema de adición para funciones elípticas. Esto pertenece a la Sección ocho, donde además se obtienen dos formas del teorema para la función $\wp$ y se muestra que toda función elíptica tiene un teorema de adición.

En la última Sección se establece la correspondencia entre funciones elípticas, curvas elípticas y *formas modulares*. A partir de las definiciones de *función modular*, de *forma modular de peso* $2k$ y de *forma cuspidal*, se muestra que las Series de Eisenstein y la *función discriminante* son ejemplos particulares de las formas modulares de peso $2k$, no cuspidal y cuspidal respectivamente. El *orden de* f *en* p, que denotamos con $(v_p(f))$, resulta un concepto fundamental al momento de relacionar las formas modulares con las curvas elípticas. Se demuestra que si $f(z)$ es una función modular de peso $2k$, no idénticamente nula, entonces

$$v_\infty(f) + \frac{v_\rho(f)}{3} + \frac{v_i(f)}{2} + \sum_{p \neq i,\, \rho} v_p(f) = \frac{k}{6}$$

donde i es la unidad imaginaria, $\rho = e^{2\pi i/3}$ y p un punto del semiplano superior H. Se demuestra que las formas no cuspidales son generadas por múltiplos complejos de G_{2k} para k menor que 6 y para los demás son suma directa de éstos con un múltiplo de la función discriminante. Por lo tanto, potencias de las series de Eisenstein de peso 4 y 6 generan el espacio de las formas modulares $\mathbf{M}_{2k}$.

Se define *invariante modular* j. Se prueba que es una función modular de peso 0, holomorfa en el semiplano superior H, que tiene un polo simple en el ∞ e induce una biyección de H/Γ sobre $\mathbb{C}$.

Se prueba que *toda curva elíptica no singular proviene de un lattice en* $\mathbb{C}$ y que dada una curva elíptica no singular $y^2 = 4x^3 - c_2\,x - c_3$, existe Ω lattice de $\mathbb{C}$ tal que $c_2 = g_2(\Omega)$, $c_3 = g_3(\Omega)$. En consecuencia $(\wp_\Omega(z)\,,\, \wp'_\Omega(z))$ parametriza la curva no singular dada, para $z \in \mathbb{C}$. Existe entonces una biyección entre *toros complejos* $\mathbb{C}/\Omega$ y curvas elípticas no singulares. Luego, toda curva elíptica se puede parametrizar (uniformizar) con dos funciones elípticas sobre un lattice apropiado.

A partir del desarrollo de Fourier de G_{2k} en ∞, se obtienen expresiones particulares, como la normalización de las funciones de Eisenstein donde los coeficientes involucran los números de Bernoulli: $B_k \in \mathbb{Q}$ y la función $\sigma_{2k-1}(n)$, suma de la potencia $2k-1$ de los divisores de n. Esto ilustra el hecho general de que los coeficientes de Fourier de las formas modulares son funciones aritméticas importantes.

En el Apéndice A y como aplicación en teoría de números se demuestran dos teoremas relacionados con el orden de magnitud de los coeficientes de las formas modulares. El gran matemático *Ramanujan*[3] fue quien estudió los coeficientes del desarrollo de Fourier de una forma cuspidal particular: *función discriminante normalizada*. Se incluye como proposición a las dos conjeturas, enunciadas por Ramanujan y referidas a estos coeficientes $\tau(n)$.

Finaliza con la pregunta abierta de Lehmer: ¿Es $\tau(n)$ no nulo para $n \geq 1$?. Esto pone en evidencia que la temática, desarrollada en este trabajo, tiene aplicaciones importantes y aristas que deben ser investigadas.

[3] Srinivasa Ramanujan (1887, 1920) fue uno de los genios matemáticos más grandes de la India. Hizo contribuciones sustanciales a la teoría analítica de números, sobre las funciones elípticas, a fracciones continuas y en series infinitas.

En el Apéndice B se describe la utilización de las curvas elípticas en Criptografía ya que, en los últimos años, esta aplicación ha adquirido una creciente importancia, llegando en la actualidad a formar parte de estándares industriales, garantizando la misma seguridad que la de los métodos criptográficos tradicionales.

Se incluyen como referencias bibliográficas sólo las más relevantes.

Índice

1. Conceptos Preliminares

1.1. Períodos

Definición 1.1.1. *Sea f una función definida en el plano complejo $\mathbb{C}$. Un número $\omega \in \mathbb{C}$ se llama período de f si*

$$\forall z \in \mathbb{C} \qquad f(z+\omega) = f(z) \tag{1.1}$$

y f recibe el nombre de **función periódica** *si $\omega \neq 0$.*

Por ejemplo las funciones $\cos z$ y $\operatorname{sen} z$ tienen período 2π ; $\exp z$ tiene período $2i\pi$ y $\operatorname{sen}(2\pi z/\omega)$ tiene período ω, $\omega \neq 0$.

Nota

- Toda función tiene período $\omega = 0$
- Si una función meromorfa[4] f, periódica con período $\omega \neq 0$, tiene un polo en el punto z, entonces tiene también un polo en el punto $z+\omega$.
- El conjunto Ω_f de los períodos de una función f tiene dos importantes propiedades: una algebraica válida para toda función f y una topológica válida para funciones meromorfas no constantes.

Estas propiedades se demuestran en los siguientes teoremas:

Teorema 1.1.2. *Si Ω_f es un conjunto de períodos de una función f definida sobre $\mathbb{C}$, entonces Ω_f es un subgrupo aditivo de $\mathbb{C}$.*

Demostración. Sean α , $\beta \in \Omega_f$ entonces $\forall z \in \mathbb{C}$;

$$\begin{aligned} f(z+(\alpha+\beta)) &= f((z+\alpha)+\beta) \\ &= f(z+\alpha) \\ &= f(z) \end{aligned}$$

estas igualdades valen por la asociatividad en $\mathbb{C}$ y porque α y β son períodos de f. Por lo tanto $\alpha + \beta \in \Omega_f$.

Mas aún $\forall \alpha \in \Omega_f$, $\forall z \in \mathbb{C}$

$$\begin{aligned} f(z-\alpha) &= f(z-\alpha+\alpha) \\ &= f(z), \end{aligned}$$

luego $(-\alpha) \in \Omega_f$.

Finalmente $f(z+0) = f(z)$, entonces $0 \in \Omega_f$, es decir que 0 es el neutro respecto de la suma en Ω_f. Por lo tanto Ω_f es subgrupo aditivo de $\mathbb{C}$. □

[4] Meromorfa es toda función que es analítica excepto por polos.

Definición 1.1.3. *Un subconjunto Δ de un espacio topológico se dice* ***discreto*** *si $\forall\, x \in \Delta$, existe un entorno U de x tal que $U \cap \Delta = \{x\}$.*

Ejemplos:

- El conjunto de los números enteros $\mathbb{Z}$ es un subconjunto discreto de $\mathbb{R}$.
- Cualquier subconjunto finito de $\mathbb{R}^n$ es discreto.
- $\{\frac{1}{n},\, n \in \mathbb{Z},\, n \neq 0\}$ es un subconjunto discreto de $\mathbb{R}$.

  Sin embargo, $\{\frac{1}{n},\, n \in \mathbb{Z},\, n \neq 0\} \cup \{0\}$ no es discreto, ya que todo entorno de 0 contiene números reales de la forma $\{\frac{1}{n},\, n \in \mathbb{Z}\}$.

Teorema 1.1.4. *Si Ω_f es el conjunto de los períodos de una función f meromorfa no constante, definida sobre $\mathbb{C}$, entonces Ω_f es un subconjunto discreto de $\mathbb{C}$.*

Demostración. Si Ω_f no fuera discreto, entonces $\exists \omega \in \Omega_f$ tal que $\forall U$, entorno de ω, U contiene puntos de $\Omega_f \setminus \{\omega\}$.

Si se supone que tales entornos son discos centrados en ω con radio $r \approx 0$, se obtiene una sucesión de períodos $\omega_n \neq \omega$ con $\lim_{n\to\infty} \omega_n = \omega$. Como $\omega,\, \omega_n \in \Omega_f$ se tiene que

$$f(\omega) = f(0+\omega) = f(0) = f(\omega_n)$$

Si $f(0) = \infty$, entonces f tiene una sucesión convergente de polos. Esto es imposible ya que, si existe un punto de acumulación en el plano finito, las funciones $\dfrac{1}{f}$ y f serían constantes, luego se llega a una contradicción.

Si $f(0) \neq \infty$, entonces la función meromorfa g que cumple que $g(z) = f(z) - f(0)$ tiene una sucesión convergente de ceros y por lo tanto resulta ser idénticamente nula. Luego si $g \equiv 0$ entonces la función f es constante.

En todos los casos se encuentra una contradicción, que surge de suponer que Ω_f no es discreto. □

Sólo existen tres tipos de subgrupos aditivos discretos de $\mathbb{C}$, los isomorfos a $\{0\}$, a $\mathbb{Z}$ y a $\mathbb{Z} \times \mathbb{Z}$ respectivamente.

Teorema 1.1.5. *Si Ω un subgrupo discreto de $\mathbb{C}$, entonces es uno de los siguientes tipos:*

(1) $\Omega = \{0\}$.

(2) $\Omega = \{n\omega_1 \,|\, n \in \mathbb{Z}\}$ *para algún* $\omega_1 \in \mathbb{C} \setminus \{0\}$ *fijo y por lo tanto* Ω *es isomorfo a* $\mathbb{Z}$.

(3) $\Omega = \{m\,\omega_1 + n\,\omega_2 \,|\, m, n \in \mathbb{Z}\}$ *con* ω_1, ω_2 *fijos de* $\mathbb{C}$, *donde* ω_1, ω_2 *son linealmente independientes (sobre* $\mathbb{R}$*), es decir* $\omega_1 \neq 0$, $\omega_2 \neq 0$ *y* $\dfrac{\omega_1}{\omega_2} \notin \mathbb{R}$ *; en tal caso,* Ω *es isomorfo a* $\mathbb{Z} \times \mathbb{Z}$.

Demostración. Se supone que $\Omega \neq \{0\}$.

Primero se muestra que $\exists\, \omega_1 \in \Omega \setminus \{0\}$ con módulo mínimo $|\omega_1|$ (el período no nulo más cercano al origen).

Como Ω es discreto, $\exists\, \varepsilon > 0$ tal que el disco $|z| < \varepsilon$ no contiene elementos de $\Omega \setminus \{0\}$. Entonces $\forall \omega \in \Omega$ el disco $|z - \omega| < \varepsilon$ no contiene elementos de $\Omega \setminus \{\omega\}$.

Se supone por el contrario que $z \in \Omega$ satisface $0 < |\, z - \omega| < \varepsilon$ luego, $(z - \omega) \in \Omega$, por la estructura de grupo de Ω. Este elemento es un período y se encuentra a una distancia menor que ε de 0, lo cual es imposible. Fig.1.1. Entonces cada $\omega \in \Omega$ es centro de un disco

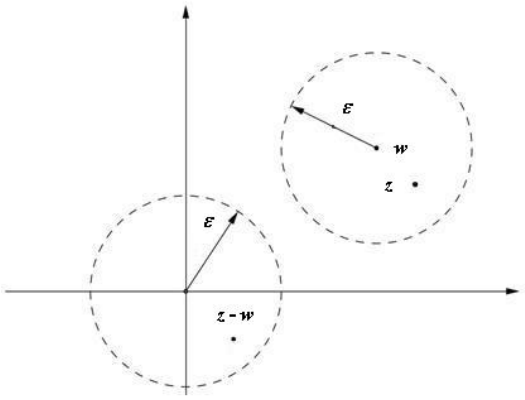


Figura 1.1: *Entornos*

de radio ε (independiente de ω), que no contiene ningún otro elemento de Ω. Por lo tanto, los discos de radio $\frac{1}{2}\varepsilon$, centrados en elementos ω de Ω son disjuntos dos a dos.

Se elige un disco $|z| < r$ suficientemente grande tal que contenga por lo menos un elemento de $\Omega \setminus \{0\}$ junto con su entorno de radio $\frac{1}{2}\varepsilon$. Este disco tiene área πr^2 y puede contener solamente un número finito h, de discos disjuntos de radio $\frac{1}{2}\varepsilon$ Fig.1.2, a lo sumo $h = 4r^2\varepsilon^{-2}$. Sólo un número finito de elementos de $\Omega \setminus \{0\}$ se encuentran en el interior

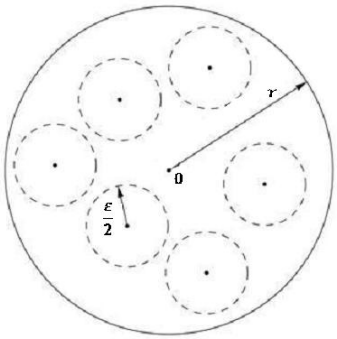


Figura 1.2: *Disco de radio r*

del disco de radio r centrado en 0 y, de este conjunto finito, se puede designar con ω_1 al período, no nulo, con *módulo mínimo*. La elección de ω_1 no es única, $(-\omega_1)$ también sirve.

Sea $\mathbf{L} = \{\lambda\omega_1 \,|\, \lambda \in \mathbb{R}\}$ la recta por 0 y por ω_1 en $\mathbb{C}$. Entonces Ω contiene al conjunto $\{n\omega_1 \,|\, n \in \mathbb{Z}\}$ y este subgrupo se encuentra en $\mathbf{L}$. Fig. 1.3.

Si se supone que $\Omega \subseteq \mathbf{L}$, entonces se exige que $\Omega = \{\, n\,\omega_1 \,|\, n \in \mathbb{Z}\}$. Luego Ω es un conjunto de períodos de tipo (2) según lo enunciado en el Teorema 1.1.5.

Si por el contrario, se supone que Ω contiene algún $\omega \neq n\,\omega_1\,, \forall\, n \in \mathbb{Z}$, como $\Omega \subseteq \mathbf{L}$ se tiene que $\omega = \lambda\,\omega_1$ para algún $\lambda \in (\mathbb{R} \setminus \mathbb{Z})$, entonces $n < \lambda < n+1$ para algún $n \in \mathbb{Z}$.

Por su estructura de grupo, Ω contiene a ω y a $n\,\omega_1$ con $n \in \mathbb{Z}$ luego, contiene a

$$\omega - n\,\omega_1 = (\lambda - n)\,\omega_1$$

sin embargo $0 \neq |\,(\lambda - n)\,\omega_1| < |\,\omega_1|$ lo cual contradice la hipótesis de mínimo de $|\,\omega_1|$.

Por lo tanto se concluye que $\Omega = \{\, n\,\omega_1 \,|\, n \in \mathbb{Z}\}$, luego, Ω es de tipo (2).

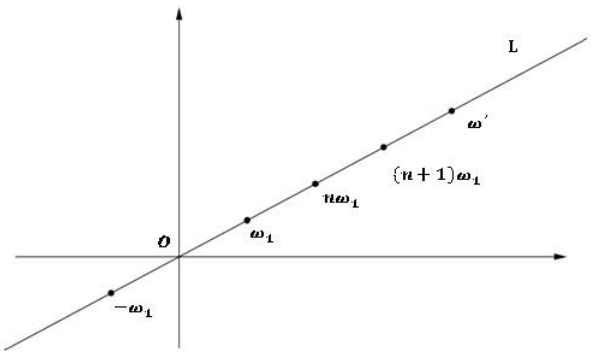


Figura 1.3: *Recta de períodos*

Se supone ahora que $\Omega \nsubseteq \mathbf{L}$. Por un argumento similar al utilizado para ω_1 , se puede mostrar que $\Omega \setminus \mathbf{L}$ tiene un elemento ω_2 con módulo mínimo. Entonces Ω contiene al subgrupo

$$\Delta = \{\, m\,\omega_1 + n\,\omega_2 \,|\, m\,,\, n \in \mathbb{Z}\}$$

y ya que $\omega_2 \notin \mathbf{L}$, ω_1 y ω_2 son linealmente independientes sobre $\mathbb{R}$. Luego Δ contiene los vértices de una teselación de $\mathbb{C}$, por paralelogramos congruentes. Fig.1.4.

Se muestra entonces que $\Omega = \Delta$. Por el párrafo anterior es claro que $\Delta \subset \Omega$, falta probar que $\Delta \supset \Omega$.

Se supone por el contrario que $\exists\,\omega \in \Omega$ con $\omega \neq m\,\omega_1 + n\,\omega_2\,; \forall\, m, n \in \mathbb{Z}$.

Sea $\omega = \lambda\,\omega_1 + \mu\,\omega_2$ con $\lambda, \mu \in \mathbb{R}$, con al menos uno de los escalares que no sea entero. Se puede suponer que $|\lambda| \leq \frac{1}{2}$, $|\mu| \leq \frac{1}{2}$.

Si $\mu = 0$ entonces $\omega = \lambda\,\omega_1 \in \mathbf{L}$ con $|\,\omega\,| = |\,\lambda\,|\,|\omega_1| < |\,\omega_1\,|$,
pero por la propiedad de mínimo de $|\,\omega_1\,|$, se tiene que $|\,\omega\,| = 0$, luego $\omega = 0$, por lo tanto se deduce que $\omega \in \Delta$, en contra de lo supuesto.

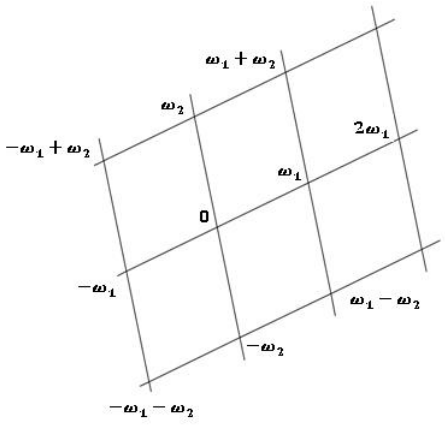


Figura 1.4: *Lattice o retículo*

Si $\lambda = 0$ entonces $\omega = \mu\,\omega_2$ y de nuevo $\omega = 0$, esta vez porque $|\,\omega_2\,|$ es el mínimo. Por lo tanto, $\lambda\,\omega_1$ y $\mu\,\omega_2$ son no nulos, luego son linealmente independientes sobre $\mathbb{R}$, tal que:

$$|\,\omega\,| < |\,\lambda\,\omega_1\,| + |\,\mu\,\omega_2| \leq \frac{1}{2}|\,\omega_1\,| + \frac{1}{2}|\,\omega_2\,| \leqq |\,\omega_2\,|$$

ya que $|\,\omega_1\,| \leqq |\,\omega_2\,|$. La primera desigualdad es estricta porque $\{\,\omega_1, \omega_2\,\}$ es linealmente independiente sobre $\mathbb{R}$.

Si $\omega \in \Omega \setminus \mathbf{L}$, $(\mu \neq 0)$, por ser $|\,\omega_2\,|$ mínimo, se tiene que $\omega = 0$. Esto contradice el hecho de que λ, $\mu \neq 0$ luego $\omega \in \Delta$. Por lo tanto $\Omega = \Delta$ y se tiene el caso (3). □

Definición 1.1.6. *Si una función compleja f tiene como su conjunto de períodos a $\Omega_f = \{\,n\,\omega_1\,|\,n \in \mathbb{Z}\}$ con $\omega_1 \in \mathbb{C} \setminus \{0\}$ fijo, entonces se dice que f es simplemente periódica y ω_1 recibe el nombre de* ***período fundamental o primitivo*** *de f.*

Definición 1.1.7. *Si una función compleja f tiene como su conjunto de períodos a $\Omega_f = \{\,m\,\omega_1 + n\,\omega_2\,|\,m\,,\,n \in \mathbb{Z}\}$ con ω_1, ω_2 fijos de $\mathbb{C}$ y ω_1, ω_2 linealmente independientes (sobre $\mathbb{R}$), entonces se dice que f es doblemente periódica. Los grupos Ω_f reciben el nombre de* ***lattice o retículo*** *y cualquier par de elementos $\{\,\omega_1, \omega_2\,\}$ tal que $\Omega_f = \langle \omega_1\,,\,\omega_2 \rangle$, se llama* ***base*** *ordenada del lattice.*

El lattice más utilizado es el retículo de paralelogramos. Fig.1.4.

En $\mathbb{C}$ sólo existen funciones periódicas con *período simple o doblemente periódicas*, aparte de las funciones constantes donde $\Omega = \mathbb{C}$ y de las funciones *no meromorfas* en las que Ω puede ser cualquier subgrupo de $\mathbb{C}$, no necesariamente discreto. Es decir, no existe otra clase de funciones analíticas o meromorfas periódicas.

1.2. Funciones simplemente periódicas

Proposición 1.2.1. *Toda función compleja meromorfa f, con un período arbitrario ω se trasforma en una función F de período conocido 2π.*

Demostración. Sea $\omega \neq 0$ un período de f, el período fundamental si f es simple o uno de los fundamentales si es doblemente periódica.

Al sustituir

$$\zeta = \frac{2\pi}{\omega} z \tag{1.2}$$

se obtiene $F(\zeta) = f\left(\frac{\omega}{2\pi}\zeta\right)$, que resulta una función meromorfa de período 2π. Por lo tanto mediante una simple transformación que se reduce a una rotación y dilatación en el z-plano, respecto del origen de coordenadas, la función f con período arbitrario ω se trasforma en la función F de período real conocido 2π. □

1.2.1. Representación por exponenciales

La más simple de todas las funciones con período ω es la exponencial $e^{2\pi i \frac{z}{\omega}}$ y cualquier función con período ω se puede expresar en términos de esta función.

Sea D una región[5] con la propiedad:

$$z \in D \Rightarrow z \pm \omega \in D$$

Se define D' en el ζ-plano, como la imagen de D por el mapeo

$$\zeta = e^{2\pi i \frac{z}{\omega}} \tag{1.3}$$

luego D' resulta ser una región.

Si D fuera todo el *plano*, entonces D' resulta ser todo el plano excluido el 0.

Si D fuera una *franja horizontal*, definida por $a < Im(2\pi\frac{z}{\omega}) < b$ entonces D' resulta el anillo $e^{-b} < |\zeta| < e^{-a}$.

Si se supone que f es meromorfa en D y cuyo período es ω, entonces existe una única función F en D' tal que

$$F(\zeta) := f(z) \tag{1.4}$$

donde $\zeta = e^{2\pi i \frac{z}{\omega}}$; z es único salvo un múltiplo aditivo de ω y este múltiplo no influye en el valor de $f(z)$. Luego F es meromorfa.

Recíprocamente, si F es meromorfa en D', entonces la ecuación (1.4) define una función f con período ω.

[5] Una **región** es un conjunto abierto y conexo, con alguno, todos o ningún punto frontera.

Observación 1.2.2. *Una función meromorfa simplemente periódica se puede expresar en términos de las funciones exponencial y trigonométrica estándar, sólo se requiere que el conjunto de períodos contenga un subgrupo isomorfo al conjunto de los números enteros* $\mathbb{Z}$. *Dada la función simplemente periódica* f *y* $\Omega_f = \{n\,\omega_1 \,|\, n \in \mathbb{Z}\}$ *su conjunto de períodos, si se reemplaza* z *por* $\omega_1\, z$ *se puede considerar que* $\Omega_f = \mathbb{Z}$.

Por ejemplo si se reemplaza $\operatorname{sen} z$ *por* $\operatorname{sen}(2\pi z)$ *o* $\exp z$ *por* $\exp(2\pi i z)$, *se tiene:*

$$f(z) = f(z+n) \qquad \forall n \in \mathbb{Z}.$$

Definición 1.2.3. *Dos números complejos* z_1 *y* z_2 *se dicen* ***congruentes módulo*** $\mathbb{Z}$ *si y sólo si* $z_1 - z_2 \in \mathbb{Z}$.

Se denota con $z_1 \equiv z_2\,(mod\,\mathbb{Z})$.

Esto define una relación de equivalencia en $\mathbb{C}$, en la que las *clases de equivalencias* son las clases laterales de $\mathbb{Z}$ y f toma el mismo valor en puntos congruentes.

Cada número complejo es congruente precisamente a un punto en la franja vertical infinita

$$S = \{z \in \mathbb{C} \,|\, 0 \leq Re(z) < 1\} \tag{1.5}$$

luego el comportamiento de la función f sobre $\mathbb{C}$, está determinado por su comportamiento sobre la franja S. Esta imagen se repite sobre cada franja paralela $S + n$, $n \in \mathbb{Z}$.

La función

$$z \mapsto \exp(2\pi i z) = \zeta \tag{1.6}$$

tiene a $\mathbb{Z}$ como su conjunto de períodos y su restricción al conjunto S es una biyección entre la franja vertical S y $\mathbb{C} \setminus \{0\}$.

Si f es una función simplemente periódica de $\mathbb{C}$ en el conjunto $\mathbb{X}$, entonces

$$\zeta \mapsto f\left(\frac{1}{2\pi i} \ln \zeta\right)$$

es una función de $\mathbb{C} \setminus \{0\}$ en $\mathbb{X}$.

Ejemplo. *Sea* $f(z) = \operatorname{sen}(2\pi z)$, *por definición*

$$\operatorname{sen}(2\pi z) = \frac{1}{2i}\left(\exp(2\pi i z) - \exp(-2\pi i z)\right)$$

si se escribe en términos de (1.6) se obtiene

$$\zeta \mapsto \frac{1}{2i}\left(\zeta - \frac{1}{\zeta}\right)$$

Análogamente, si $f(z) = \cos(2\pi z)$, se obtiene

$$\zeta \mapsto \frac{1}{2}\left(\zeta + \frac{1}{\zeta}\right)$$

Ejemplo. *Se considera* $f(z) = \tan(\pi z)$. *Esta función tiene una única clase de polos en* $z = n + \frac{1}{2}$ $(n \in \mathbb{Z})$ *luego, a partir de la definición se obtiene*

$$\zeta \mapsto \frac{-i(\zeta - 1)}{\zeta + 1}$$

que tiene un polo simple en $\zeta = -1 = \exp(2\pi i(n + \frac{1}{2}))$

Teorema 1.2.4. *Las funciones periódicas* f *cuyos conjuntos de períodos contienen a los números enteros, son funciones de* $\zeta = \exp(2\pi iz)$*; luego* f *es meromorfa sobre* $\mathbb{C}$ *si y sólo si la composición es meromorfa sobre* $\mathbb{C} \setminus \{0\}$ *y los polos de* f *sobre* $\mathbb{C}$ *se corresponden uno a uno con los polos de su recíproca sobre* $\mathbb{C} \setminus \{0\}$.

La idea de la demostración se basa en lo siguiente:

Si se considera la función meromorfa f, sus polos son discretos y, por un argumento similar al utilizado en la demostración del Teorema 1.1.5, se puede encontrar un rectángulo

$$R = \{z \,|\, 0 \leq Re(z) < 1\,,\; y_1 < Im(z) < y_2\}$$

dentro de la franja infinita S definida en la ecuación (1.5) tal que R no contiene polos de la función f.

La función $z \to \exp(2\pi iz)$ mapea los segmentos $\{x + iy_j \,|\, 0 \leq x < 1\}$ de R sobre $\{\exp(-2\pi y_j)\exp(-2\pi ix) \,|\, 0 \leq x < 1\}$ para $j = 1, 2$. Estas imágenes son círculos de radio $r_j = \exp(-2\pi y_j)$ en el plano imagen. Luego R se mapea en una región anular dada por $r_2 < |\exp(2\pi iz)| < r_1$, en el interior de la cual la transformación es analítica. Fig. 1.5.

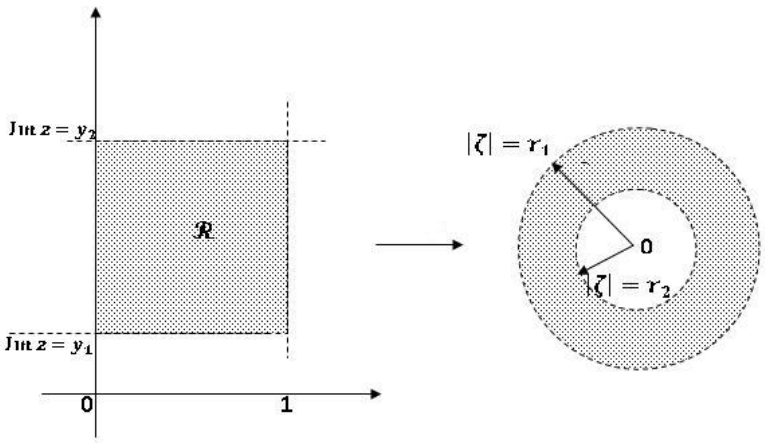


Figura 1.5:

El desarrollo en serie alrededor de cero, está dado por:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n \, e^{2\pi i z n} \qquad \textit{válido en } y_1 < Im(z) < y_2$$

Si se reemplaza $\exp(2\pi i z n) = \cos(2\pi n z) + i \operatorname{sen}(2\pi n z)$, se obtienen las series de Fourier (J.B.J. Fourier, 1768-1830):

$$f(z) = a_0 + \sum_{n=1}^{\infty} \Big[A_n \cos(2\pi n z) + B_n \operatorname{sen}(2\pi n z) \Big]$$

donde $A_n = a_n + a_{-n}$ y $B_n = i(a_n - a_{-n})$ para $n \geq 1$.

Este desarrollo es válido en la franja horizontal $y_1 < Im(z) < y_2$ que consta de R y sus trasladados $R + m, \quad m \in \mathbb{Z}$.

Diferentes elecciones del rectángulo R dan lugar a diferentes series de Fourier para f, válidos en franjas horizontales disjuntas.

1.3. Grupos Topológicos

Definición 1.3.1. *Un **grupo topológico** es un espacio topológico G que tiene estructura de grupo, en el cual la multiplicación de elementos del grupo y la inversa son operaciones continuas.*

Es decir, los mapeos:

$$\begin{aligned} m : G \times G &\longrightarrow G \quad \textit{definido por} \quad m(g,h) = gh \\ i : G \times G &\longrightarrow G \quad \textit{definido por} \quad i(g) = g^{-1} \end{aligned}$$

son continuos.

Ejemplos. .

i.- $\mathbb{C}$ *con su estructura de grupo aditivo es un grupo topológico ya que las operaciones* $m(z,w) = z + w$ *;* $i(z) = -z$ *son continuas.*

ii.- *El círculo* $S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\}$ *con la multiplicación de los números complejos como operación del grupo.*

iii.- $\mathbb{GL}(n, \mathbb{C})$ *con la multiplicación de matrices como operación del grupo.*
Se obtiene la topología sobre este grupo al identificar a las matrices $(a_{i\,j}) \in \mathbb{C}^{n \times n}$ *con los puntos* $(a_{11}, a_{12}, \cdots, a_{1n}, a_{21}, \cdots, a_{nn}) \in \mathbb{C}^{n \times n}$. *Las operaciones* $\boldsymbol{m}$ *e* $\boldsymbol{i}$ *de este grupo se expresan en términos de las funciones coordenadas* a_{ij} *luego, son continuas. Análogamente* $\mathbb{GL}(n, \mathbb{R})$ *es un grupo topológico.*

iv.- $\mathbb{PGL}(n,\mathbb{C})$, *el grupo lineal proyectivo, es el grupo cociente* $\mathbb{GL}(n,\mathbb{C})/\mathbb{K}$ *con la multiplicación de clases laterales de* $\{\lambda I \,|\, \lambda \neq 0\}$ *como operación del grupo.*
En este grupo la matriz $A \in \mathbb{GL}(n,\mathbb{C})$ *se identifica con* $\lambda A, \lambda \in \mathbb{C} \setminus \{0\}$. *Se induce la topología al identificar el punto* $(a_{11}, a_{12}, \cdots, a_{1n}, a_{21}, \cdots, a_{nn}) \in \mathbb{C}^{n^2}$ *con el punto* $(\lambda a_{11}, \lambda a_{12}, \cdots, \lambda a_{nn}) \in \mathbb{C}^{n^2}$. *Análogamente* $\mathbb{PGL}(n,\mathbb{R})$ *es un grupo topológico.*

Proposición 1.3.2. *En un grupo topológico* G *el mapeo* r_g *definido por*

$$r_g(x) = xg \qquad (x, g \in G)$$

es una biyección continua con inversa continua $r_{(g^{-1})}$

La función r_g es el homeomorfismo de G en G que se conoce como *traslación derecha.*
Si $x\,,\, y \in G$ entonces $r_{(x^{-1}y)}(x) = y$.
Por lo tanto existe un homeomorfismo sobre G, de un punto fijo arbitrario de G sobre cualquier otro punto de G. En otras palabras, el grupo de homeomorfismos de G es transitivo. Esto significa que cualquier punto de G, es topológicamente equivalente a cualquier otro punto de G; en el caso de $\mathbb{C}$ y S^1 esta visualización es evidente.

En particular, cada entorno de un punto dado en G es homeomorfo al entorno de la *identidad* $e \in G$. Por lo tanto se puede definir un *subgrupo discreto* Ω de G, con la propiedad de que exista U entorno de e en G tal que $U \cap \Omega = \{e\}$. Esta idea de traslación de entornos desde un punto arbitrario es precisamente la *identificación elemental* ya usada en la demostración del Teorema 1.1.5. Una extensión de ese teorema afirma que los subgrupos discretos de $\mathbb{R}^n$ son isomorfos a $\{0\}$ o a $\mathbb{Z}^m$ donde $1 \leq m \leq n$. Sin embargo, en general es difícil describir a los subgrupos discretos Ω de un grupo topológico arbitrario G.

Definición 1.3.3. *Sea* G *un grupo topológico y* $\boldsymbol{N}$ *la colección de todos los subconjuntos abiertos de* G *que contienen a* e.

Si $x \in G$, *entonces* $\{r_x(U) \,|\, U \in \boldsymbol{N}\}$ *es la colección de todos los conjuntos abiertos que contienen a* x, *así los conjuntos abiertos en* G *se determinan por los elementos de* $\boldsymbol{N}$.

Si $U, V \in \boldsymbol{N}$ *entonces* $UV \in \boldsymbol{N}$ *y* $U^{-1} \in \boldsymbol{N}$ *donde* $UV = \{uv \,|\, u \in U, v \in V\}$ *y* $U^{-1} = \{u^{-1} \,|\, u \in U\}$.

Si $V = V^{-1}$ *entonces* V *recibe el nombre de* ***conjunto abierto simétrico***.

Lema 1.3.4. *Si* $U \in \boldsymbol{N}$ *entonces existe un conjunto abierto simétrico* $V \in \boldsymbol{N}$ *tal que* $V \cdot V \subseteq U$.

Demostración. Se denota con W al conjunto $r^{-1}(U) = \{(x\,,\, y) \in G \times G \,|\, x\,y \in U\}$. Como la función $r : G \times G \longrightarrow G$ es continua y $(e,e) \in W$, se sigue que W es un entorno abierto de (e,e) en $G \times G$, luego por definición de topología producto, $\exists\, V_1\,,\, V_2 \in \mathbf{N}$ tal que $V_1 \times V_2 \subseteq W$ y por lo tanto $V_1 V_2 \subseteq U$.

Si se considera $V_3 = V_1 \cap V_2$, entonces $V_3 V_3 \subseteq U$. Luego si se denota con $V = V_3 \cap V_3^{-1}$ entonces $V \in \mathbf{N}$, luego V es un conjunto abierto simétrico y $V \cdot V \subseteq U$. □

Teorema 1.3.5. *Si Ω es un subgrupo discreto de un grupo topológico G y si $\mathbb{K}$ es un subconjunto compacto de G, entonces $\Omega \cap \mathbb{K}$ es finito.*

Corolario. *En un grupo topológico compacto, todo subgrupo discreto es finito.*

Observación

- La condición que Ω sea subgrupo es necesaria, por ejemplo: si G fuera el grupo aditivo $(\mathbb{R}, +)$, $\Omega = \{\frac{1}{n} \mid n = 1, 2, 3, \cdots\}$ y $\mathbb{K} = [0, 1]$, entonces Ω es un subconjunto discreto de G, pero no es subgrupo, $\mathbb{K}$ es compacto y $\Omega \cap \mathbb{K}$ es infinito.
- Se podría utilizar el Teorema 1.3.5 para demostrar, de una manera más corta, el Teorema 1.1.5, pero se eligió una demostración más simple, usando la métrica euclídea de $\mathbb{R}^2$.

.

2. Lattices y Regiones fundamentales

2.1. Lattice o retículo

En la Definición 1.1.7 se estableció que un grupo de períodos $\Omega \subset \mathbb{C}$ recibe el nombre de **lattice o retículo** si tiene la forma $\Omega = \{m\,\omega_1 + n\,\omega_2 \,|\, m\,,\ n\ \in \mathbb{Z}\}$, con $\{\omega_1,\, \omega_2\}$ linealmente independiente sobre $\mathbb{R}$.

El lattice se denota con $\Omega_{(\omega_1\,,\omega_2)}$ y $\{\omega_1\,,\omega_2\}$ es una **base** ordenada de Ω, es decir un par de generadores linealmente independientes de Ω ($\omega_1 \neq 0$, $\omega_2 \neq 0$ y $\dfrac{\omega_1}{\omega_2} \notin \mathbb{R}$).

Existen otras bases para Ω, por ejemplo $\{\omega_1\,,\omega_1 + \omega_2\}$.

Si $\omega \in \Omega_{(\omega_1\,,\omega_2)}$ entonces $\exists\, m\,,\ n\ \in \mathbb{Z}$ tal que

$$\begin{aligned} \omega &= m\,\omega_1 + n\,\omega_2 \\ &= (m-n)\,\omega_1 + n\,(\omega_1 + \omega_2) \end{aligned} \tag{2.1}$$

con $m - n\,,\ n\ \in \mathbb{Z}$. En general si $\omega_1'\,,\omega_2' \in \Omega_{(\omega_1\,,\omega_2)}$, entonces

$$\begin{aligned} \omega_1' &= a\,\omega_1 + b\,\omega_2 \\ \omega_2' &= c\,\omega_1 + d\,\omega_2 \end{aligned} \tag{2.2}$$

donde a , b , c y $d \in \mathbb{Z}$.

Teorema 2.1.1. *Las ecuaciones (2.2) determinan una base* $\{\omega_1{}',\, \omega_2{}'\}$ *para* $\Omega_{(\omega_1\,,\omega_2)}$ *si y sólo si* $ad - bc = \pm 1$.

Demostración. Es conveniente escribir (2.2) en forma matricial:

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = A \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \tag{2.3}$$

donde

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Si $ad - bc = \pm 1$ entonces existe la inversa de la matriz A, llamada A^{-1} cuyos elementos son números enteros y se tiene que:

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

Así $\omega_1\,,\,\omega_2 \in \Omega_{(\omega_1'\,,\omega_2')}$ y por lo tanto $\Omega_{(\omega_1\,,\omega_2)} \subseteq \Omega_{(\omega_1'\,,\omega_2')}$. La inclusión recíproca es obvia, luego por igualdad de conjuntos $\Omega_{(\omega_1\,,\omega_2)} = \Omega_{(\omega_1'\,,\omega_2')}$, donde $\{\omega_1{}',\, \omega_2{}'\}$ es base de Ω.

Recíprocamente, si se considera que las ecuaciones (2.2) determinan una base $\{\omega_1{}',\, \omega_2{}'\}$ para $\Omega_{(\omega_1\,,\omega_2)}$, al expresar los elementos $\omega_1\,,\,\omega_2$ en términos de esta base se tiene:

$$\begin{aligned}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} &= B\cdot\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix}\\ &= B\cdot A\cdot\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\end{aligned} \tag{2.4}$$

para alguna matriz B con elementos enteros. Como por hipótesis $\omega_1\,,\,\omega_2$ son linealmente independientes sobre $\mathbb{R}$ y el conjunto de los números complejos $\mathbb{C}$ es un espacio vectorial de dimensión dos sobre $\mathbb{R}$, ellos forman una base para $\mathbb{C}$.

De la ecuación (2.4), se sigue que la matriz $B\cdot A$ induce la transformación lineal identidad en $\mathbb{C}$, luego $B\cdot A = I$ y por lo tanto

$$|\,B\,|\,|\,A\,| = 1.$$

Como las matrices A y B tienen elementos enteros, los valores de sus determinantes son números enteros. Entonces $|A| = \pm 1$, es decir $ad - bc = \pm 1$. □

Es fácil ver que existen infinitos conjuntos de enteros $a\,,\,b\,,\,c\,,\,d$ que satisfacen

$$ad\,-\,bc = \pm\,1$$

Luego cualquier lattice Ω tiene infinitas bases.

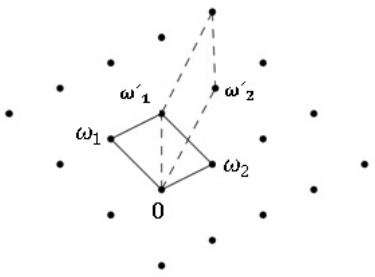


Figura 2.1: Dos bases para el lattice

Teorema 2.1.2 (Condición necesaria y suficiente para que $\omega \in \Omega$ pertenezca a una base)**.** *El elemento $\omega = a\omega_1 + b\omega_2 \in \Omega_{(\omega_1\,,\omega_2)}$ es un elemento de una base para Ω si y sólo si a y b son coprimos, ó ($a = \pm 1$ y $b = 0$) ó ($a = 0$ y $b = \pm 1$).*

La demostración es un simple cálculo.

2.1.1. Congruencia módulo Ω

Definición 2.1.3. *Sea Ω un lattice y $z_1\,,\, z_2 \in \mathbb{C}$, se dice que z_1 y z_2 son **congruentes módulo** Ω si y sólo si $z_1 - z_2 \in \Omega$.*

Se denota con $z_1 \sim z_2\,(mod\,\Omega)$. Se puede ver fácilmente que la congruencia $mod\,\Omega$ es una relación de equivalencia sobre $\mathbb{C}$. Las clases de equivalencia son las clases laterales $z + \Omega$ de Ω en el grupo aditivo $\mathbb{C}$.

Alternativamente se puede considerar la acción Ω sobre $\mathbb{C}$ como transformación de grupos: cada $\omega \in \Omega$ induce una traslación t_ω sobre $\mathbb{C}$ tal que

$$t_\omega \,:\, z \mapsto z + \omega$$

y como

$$t_{\omega_1+\omega_2} = t_{\omega_1} \circ t_{\omega_2}$$

se tiene un isomorfismo de grupos $\Omega \cong \{\, t_\omega \,|\, \omega \in \Omega\}$.

Entonces dos puntos $z_1\,,\, z_2 \in \mathbb{C}$, son congruentes módulo Ω si y sólo si ellos yacen en una misma **órbita** bajo la acción de Ω.

Luego una órbita se forma con puntos congruentes entre sí.

2.2. Regiones fundamentales

Definición 2.2.1. *Un subconjunto $P \subsetneqq \mathbb{C}$ conexo y cerrado es una **región fundamental** para Ω, lattice de $\mathbb{C}$ si:*

(i) $\forall\, z \in \mathbb{C}$, *$P$ contiene al menos un punto de la misma Ω-órbita de z.*

(ii) Dos puntos del interior de P no pertenecen a la misma Ω-órbita.

La forma de una región fundamental P es arbitraria, la más sencilla es un polígono euclídeo con un número finito de lados. En ese caso se dice que P es un **polígono fundamental** para el lattice Ω.

Si P es un paralelogramo, entonces P recibe el nombre de **paralelogramo fundamental** para Ω.

Proposición 2.2.2. *El paralelogramo P con vértices $0\,,\, \omega_1\,,\, \omega_1+\omega_2\,,\, \omega_2$, es un paralelogramo fundamental del lattice $\Omega_{(\omega_1,\omega_2)}$.*

Demostración. Sea $z \in \mathbb{C}$, $z = \lambda\omega_1 + \mu\omega_2$ con $\lambda\,,\mu \in \mathbb{R}$ y ω_1, ω_2 linealmente independientes sobre $\mathbb{R}$.

Si

$$\begin{aligned}
&\lambda = [\lambda] + \lambda_1\,, \quad 0 \le \lambda_1 < 1\,, \quad ([\lambda]\,\text{denota parte entera de } \lambda)\\
&\mu = [\mu] + \mu_1\,, \quad 0 \le \mu_1 < 1\,, \quad [\mu] \in \mathbb{Z}, \quad \text{entonces}\\
&z = [\lambda]\,\omega_1 + [\mu]\,\omega_2 + \lambda_1\omega_1 + \mu_1\omega_2 \quad \text{luego}\\
&[\lambda]\,\omega_1 + [\mu]\,\omega_2 \in \Omega \quad y\\
&\lambda_1\,\omega_1 + \mu_1\,\omega_2 = u \in \mathring{P}
\end{aligned}$$

Por lo tanto $z \sim u \pmod{\Omega}$, se verifica el punto (i) de la definición.

Para demostrar (ii):
Se supone que $\exists\, u_1\,, u_2 \in \mathring{P}$ tal que $u_1 \sim u_2 \pmod{\Omega}$ con $u_1 \neq u_2$. Sean

$$\begin{aligned}
u_1 &= \lambda_1\,\omega_1 + \mu_1\,\omega_2\,, \qquad 0 < \lambda_1 < 1\,, \quad 0 < \mu_1 < 1\\
u_2 &= \lambda_2\,\omega_1 + \mu_2\,\omega_2\,, \qquad 0 < \lambda_2 < 1\,, \quad 0 < \mu_2 < 1\\
u_1 - u_2 &= (\lambda_1 - \lambda_2)\,\omega_1 + (\mu_1 - \mu_2)\,\omega_2\,, \quad \text{luego}\,(u_1 - u_2) \in \Omega.
\end{aligned}$$

Entonces sus coeficientes deben ser números enteros, luego $\lambda_1 = \lambda_2$ y $\mu_1 = \mu_2$. Por lo tanto $u_1 = u_2$ que contradice lo supuesto. □

Corolario. *Los puntos que están situados en los lados del paralelogramo de períodos, que son distintos de los vértices, se dividen en pares de puntos congruentes.*

Los vértices del paralelogramo de períodos, representan una cuaterna de puntos congruentes entre sí.

Las condiciones (i) y (ii) aseguran que si P es cualquier región fundamental para el lattice Ω, entonces P y sus imágenes, bajo la acción de Ω, es decir sus traslaciones $P+\omega$, con $\omega \in \Omega$, cubren completamente el plano $\mathbb{C}$, solapándose solamente los puntos de sus fronteras.

Este tipo de cubrimiento se conoce como *teselación* de $\mathbb{C}$, la Fig.2.2 muestra un ejemplo. Se obtienen diferentes teselaciones de $\mathbb{C}$ si se toman regiones fundamentales diferentes es decir, cuando se eligen distintas bases de Ω.

Si P es cualquier región fundamental para Ω, entonces para $t \in \mathbb{C}$ fijo, el conjunto:

$$P + t = \{\, z + t \,|\, z \in P\}$$

que se denota con $t(P)$, es también una región fundamental. Esto es de utilidad cuando se quiere encontrar regiones fundamentales contenidas en un conjunto particular de puntos. Por ejemplo "encontrar una región fundamental que tenga a cero como punto interior".

Para obtener regiones fundamentales arbitrarias se propone el siguiente procedimiento:

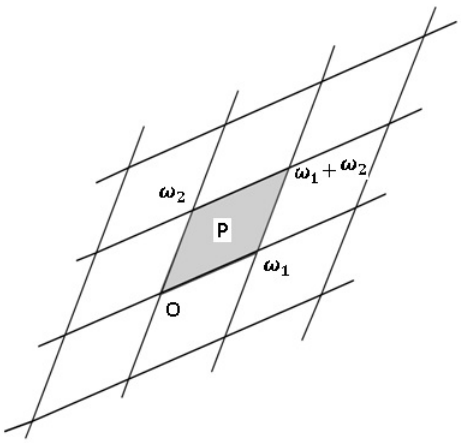


Figura 2.2: Paralelogramo fundamental

Sea P un paralelogramo fundamental para $\Omega_{(\omega_1,\omega_2)}$ con vértices 0, ω_1, $\omega_1+\omega_2$, ω_2. La transformación $z \mapsto z+\omega_2$ mapea un lado de P sobre el lado opuesto. Si se corta una región S del interior de P, que interseca un lado y se la pega sobre el lado opuesto, sobre el exterior de P, se obtiene la región fundamental $(P-S) \cup (S+\omega_2)$ Fig.2.3.

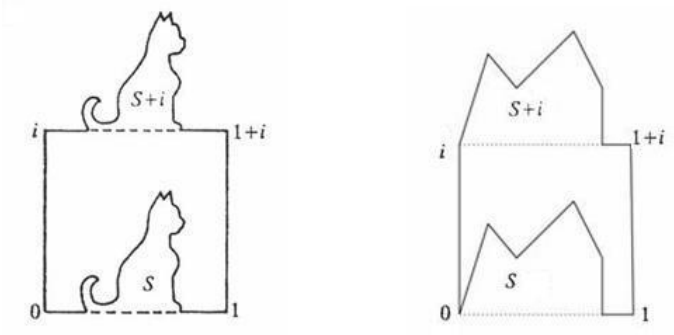


Figura 2.3: Regiones fundamentales arbitrarias, con $\omega_2 = i$

Análogamente, se pueden usar las transformaciones $z \mapsto z-\omega_2$ y $z \mapsto z \pm \omega_1$. Realizando varias veces el proceso de corte y pegue se obtiene una región fundamental conveniente.

La región fundamental para un lattice determinado no es única, pero su área es invariante y por lo tanto puede ser considerada función del lattice.

Sea $X \subseteq \mathbb{C}$ un conjunto medible y sea $\mu(\mathbb{X})$ la medida del área de $\mathbb{X}$. Como la traslación $z \mapsto z+\omega$ es una isometría de $\mathbb{C}$, se tiene que $\mu(\omega(\mathbb{X})) = \mu(\mathbb{X})$.

Teorema 2.2.3. *Si P_1 y P_2 son polígonos fundamentales del lattice Ω, entonces*

$$\mu(P_1) = \mu(P_2).$$

Demostración. Sea $\mathring{P}_j$ el interior de P_j $(j = 1, 2)$ por lo tanto $\mu(P_j) = \mu(\mathring{P}_j)$.

Ahora

$$P_1 \supseteq P_1 \cap \bigcup_{\omega\in\Omega} \omega(\mathring{P}_2) = \bigcup_{\omega\in\Omega} (P_1 \cap \omega(\mathring{P}_2))$$

Como $\mathring{P}_2$ es interior de la región fundamental P_2, los conjuntos $(P_1 \cap \omega(\mathring{P}_2))$ son disjuntos puesto que dos polígonos fundamentales tienen, a lo sumo, puntos comunes en la frontera, luego

$$\begin{aligned}\mu(P_1) &\geqslant \sum_{\omega\in\Omega} \mu(P_1 \cap \omega(\mathring{P}_2)) \\ &= \sum_{\omega\in\Omega} \mu((-\omega)(P_1) \cap \mathring{P}_2) \\ &= \sum_{\omega\in\Omega} \mu(\omega\,(P_1\,) \cap \mathring{P}_2\,)\end{aligned}$$

ya que $\omega \in \Omega \Rightarrow (-\omega\,) \in \Omega$. Como P_1 es una región fundamental

$$\bigcup_{\omega\in\Omega} \omega\,(P_1\,) = \mathbb{C}$$

luego

$$\bigcup_{\omega\in\Omega} \left[\omega\,(P_1) \cap \mathring{P}_2\right] = \mathring{P}_2$$

entonces

$$\sum_{\omega\in\Omega} \mu(\omega\,(P_1\,) \cap \mathring{P}_2) \geqslant \mu(\mathring{P}_2\,) = \mu(\,P_2\,)$$

de lo que resulta

$$\mu(\,P_1\,) \geqslant \mu(\,P_2\,).$$

Si se intercambia P_1 con P_2 y se trabaja de manera análoga se encuentra que

$$\mu(\,P_2\,) \geqslant \mu(\,P_1\,).$$

Por lo tanto

$$\mu(\,P_1\,) = \mu(\,P_2\,).$$

Los polígonos asociados a un lattice tienen igual área. Luego el área es invariante. □

Si se aplica este resultado a la región fundamental de la Fig.2.4, se demuestra el Teorema de Pitágoras. Con *corte, pegue y rotación* se construye una región, unión de dos cuadrados, elegidos convenientemente para su demostración.

Definición 2.2.4. *Se llama* ***paralelogramo especial*** *a cada paralelogramo fundamental P del lattice Ω tal que su frontera ∂P no contiene ceros ni polos de la función f periódica respecto de Ω.*

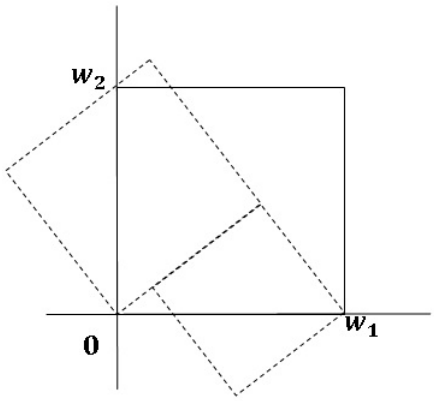


Figura 2.4: Teorema de Pitágoras

2.3. El toro

Sea f una función doblemente periódica respecto del lattice $\Omega = \Omega_{(\omega_1,\omega_2)}$, entonces su comportamiento sobre $\mathbb{C}$ está determinado por su comportamiento sobre la región fundamental P para Ω. Este comportamiento se repite en todas las traslaciones $P+\omega$, $\omega \in \Omega$.

Se elige como P al paralelogramo de vértices 0, ω_1, $\omega_1 + \omega_2$, ω_2. Luego se considera a f como una función doblemente periódica definida sobre P y tal que f toma los mismos valores sobre *puntos fronteras congruentes*.

En la Fig.2.5 se identifican claramente los pares de lados congruentes del paralelogramo fundamental. El espacio resultante $\mathbb{T}$ se conoce como **toro bidimensional**.

Luego, una función doblemente periódica f suele considerarse como una función definida sobre el toro $\mathbb{T}$ y recíprocamente toda función definida sobre $\mathbb{T}$ puede ser considerada como una función doblemente periódica sobre $\mathbb{C}$.

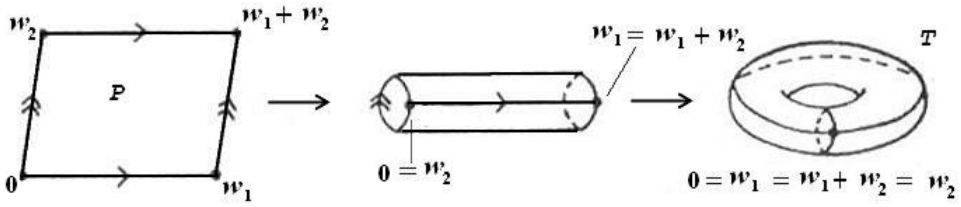


Figura 2.5: Toro bidimensional

Por definición de región fundamental, es claro que existe una correspondencia uno a uno entre Ω-órbita sobre $\mathbb{C}$ y puntos de $\mathbb{T}$. Por ello se puede pensar a $\mathbb{T}$ como el conjunto de las Ω-órbitas, es decir, como el conjunto cociente $\mathbb{C}/\Omega$ de las clases laterales de Ω en $\mathbb{C}$.

Como Ω es un subgrupo normal del grupo aditivo $\mathbb{C}$, el conjunto cociente $\mathbb{T} = \mathbb{C}/\Omega$ tiene estructura de grupo abeliano. Y al existir una función continua del conjunto cerrado y acotado P sobre $\mathbb{T}$, dada por la identificación de los puntos fronteras, se sigue que $\mathbb{T}$ es compacto.

Esta construcción de $\mathbb{T}$ a partir de la acción de Ω sobre $\mathbb{C}$ se generaliza de la siguiente manera:

Proposición 2.3.1. *Sea $\mathbb{X}$ un espacio topológico y G un grupo de homeomorfismos de $\mathbb{X}$. La acción de G sobre $\mathbb{X}$ particiona a $\mathbb{X}$ en G-órbitas.*

Se denota la G-órbita de x con $[x]_G$, es decir:

$$y \in [x]_G \Longleftrightarrow g(x) = y \quad \text{para algún } g \in G.$$

El conjunto de G-órbitas se denota con $\mathbb{X}/G$ y se lo llama *espacio-órbita* o *espacio cociente* de $\mathbb{X}$ sobre G.

Definición 2.3.2. *Se define el mapeo proyección:*

$$p : \mathbb{X} \longrightarrow \mathbb{X}/G \quad \text{tal que} \quad p(x) = [x]_G$$

Se induce la topología en $\mathbb{X}/G$ al definir que "un conjunto $V \subseteq \mathbb{X}/G$ es abierto si y sólo si $p^{-1}(V)$ es abierto en $\mathbb{X}$".

Con esta definición es clara la continuidad del mapeo p, que además es abierto ya que si U es abierto en $\mathbb{X}$ entonces

$$p^{-1}(p(U)) = \bigcup_{g \in G} g(U)$$

es también abierto (cada $g \in G$ es un homeomorfismo) y así $p(U)$ es abierto.

Ejemplo. .
1) *Si $\mathbb{Z}$ actúa sobre $\mathbb{R}$ por traslación,*

$$x \mapsto x + n \quad \forall\, x \in \mathbb{R}\,,\, n \in \mathbb{Z}\,,$$

entonces $\mathbb{R}/\mathbb{Z}$ es homeomorfo al círculo S^1.
2) *El cociente de la esfera S^2 por el grupo G, generado por el mapeo antipodal:*

$$map\,(x_1\,,\, x_2\,,\, x_3) \mapsto (-x_1\,,\, -x_2\,,\, -x_3)$$

es homeomorfo al plano proyectivo real.

Si se retorna al toro $\mathbb{T} = \mathbb{C}/\Omega$, es claro que $\forall\, z\,,\, [z] = [z]_\Omega \in \mathbb{T}$, $\quad p^{-1}([z])$ está en la Ω-órbita de z: $[z] = z + \Omega$, por lo tanto es discreto.

Sea d la menor de las distancias entre dos puntos cualesquiera de $p^{-1}([z])$. Se tiene que $d > 0$ ya que por ser discreto hay un período con módulo mínimo. Sea U un disco abierto de radio a lo sumo $\dfrac{d}{2}$, con centro en cualquier punto de $p^{-1}[z]$, entonces U contiene a lo

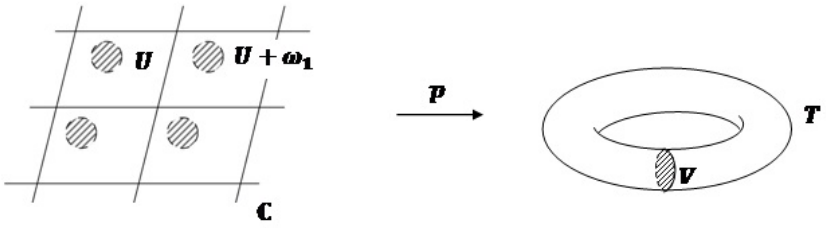


Figura 2.6: Homeomorfismo del plano complejo y el toro

sumo un punto de cada Ω-órbita. Si se define $V = p(U)$, entonces el mapeo $p : U \longrightarrow V$ es biyectivo, abierto y continuo y por lo tanto es un homeomorfismo.

Así, todo punto $[z] \in \mathbb{T}$ tiene un entorno V homeomorfo a un conjunto abierto en $\mathbb{C}$. Tal conjunto resulta ser un espacio al que se lo llama ***superficie***. El *toro* es la más simple superficie compacta, excluyendo a la *esfera*.

Note que $p^{-1}(V)$ consta de conjuntos abiertos disjuntos de la forma $U + \omega, \quad \omega \in \Omega$, los que se mapean homeomórficamente sobre V por p, Fig. 2.6. De este modo resulta $\mathbb{C}$ un espacio cubrimiento de $\mathbb{T}$ y p un mapeo cubrimiento.

.

3. Funciones elípticas

3.1. Ideas principales

El estudio de las funciones elípticas es muy interesante por sus propiedades teóricas además de su importancia para el álgebra y la teoría de números. Su nombre se debe a que estas funciones sugen como funciones inversas de las integrales elípticas, según los escritos de grandes matemáticos como *Abel* y *Jacobi*.

En forma intuitiva, *una función elíptica es una función definida sobre el plano complejo, meromorfa y periódica en dos direcciones.*

Definición 3.1.1. *Una función meromorfa* $f : \mathbb{C} \to \Sigma$ *es* ***elíptica*** *con respecto al lattice* $\Omega \subseteq \mathbb{C}$ *si* f *es periódica con respecto a* Ω.
Es decir, si

$$f(z+\omega) = f(z) \qquad \forall\, z \in \mathbb{C}, \forall\, \omega \in \Omega$$

entonces cada $\omega \in \Omega$ *es un período de* f.

Si f es una función elíptica con respecto a Ω, lattice de $\mathbb{C}$, entonces se puede considerar a f como una función $f : \mathbb{T} \to \Sigma$, donde $\mathbb{T}$ es el toro $\mathbb{T} = \mathbb{C}/\Omega$ y Σ la esfera.

Por la compacidad del toro, para las *funciones elípticas* con dominio en el toro $\mathbb{T}$, se pueden probar resultados similares a los de las *funciones racionales sobre la esfera.*

Sea f elíptica con respecto al lattice Ω y no constante. Para todo punto c de la esfera, las soluciones de $f(z) = c$ son aisladas y cada solución tiene multiplicidad finita (soluciones congruentes tienen la misma multiplicidad), ya que cualquier polígono fundamental P de Ω es compacto y contiene un número finito de soluciones.

Se puede suponer que P es un paralelogramo especial. Si fuera necesario se traslada P a $P + t$, $t \in \mathbb{C}$ a fin de que no existan soluciones en su frontera.

Si $z_1, \cdots, z_r$ son las soluciones de $f(z) = c$ en el interior del paralelogramo especial $(\mathring{P})$ con multiplicidades $k_1, \cdots, k_r$ respectivamente y si $N_c = k_1 + \cdots + k_r$, entonces se dice que "*existen* N_c *soluciones de la ecuación* $f(z) = c$".

Como $z_1, \cdots, z_r$ son representantes de las clases de congruencias de soluciones de $f(z) = c$, para $z \in \mathbb{C}$, se puede pensar a N como la suma de las multiplicidades de las soluciones de $f([z]) = c$, donde $[z] \in \mathbb{T} = \mathbb{C}/\Omega$.

3.2. Propiedades generales de las funciones elípticas

Teorema 3.2.1. *La suma de los residuos de una función elíptica, en el interior de un paralelogramo especial es cero.*

Demostración. Sea f una función elíptica y P un paralelogramo especial para el lattice $\Omega_{\{\omega_1,\omega_2\}}$. Por lo tanto f es meromorfa en el interior del paralelogramo y analítica sobre su frontera ∂P, con polos en $z_j\,, \quad j=1,\cdots,k\,.$

Por el teorema de los residuos se sabe que

$$\sum_{z_j \text{ polos de } f} Res_{z_j\in \mathring{P}} f(z) = \frac{1}{2\pi i}\int_{\partial P} f\,(z)\,dz$$

Para calcular la integral del segundo miembro se considera que $\Gamma_1\,,\,\Gamma_2\,,\,\Gamma_3$ y Γ_4 son lados del paralelogramo P, con vértices t, $t+\omega_1$, $t+\omega_1+\omega_2$, y $t+\omega_2$, donde el sentido de integración a lo largo de cada Γ_j es consistente con la orientación positiva de ∂P como en la Fig.3.1. Luego

$$\int_{\partial P} f(z)dz = \sum_{j=1}^{4}\int_{\Gamma_j} f(z)dz$$

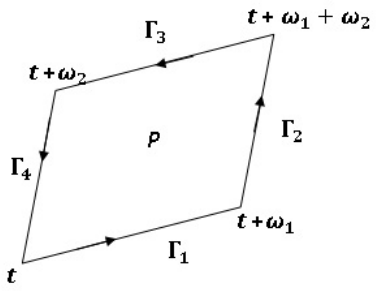


Figura 3.1: Paralelogramo orientado

$$\begin{aligned}\int_{\Gamma_3} f(z)dz &= \int_{\Gamma_3} f(z+\omega_2)dz \quad \text{como } \omega_2 \text{ es período de } f\\ &= -\int_{\Gamma_1+\omega_2} f(z+\omega_2)\,d(z+\omega_2)\end{aligned}$$

donde Γ_3 es $\Gamma_1+\omega_2$ recorrido en sentido contrario y si se sustituye $z-\omega_2$ por z se obtiene:

$$\int_{\Gamma_3} f(z)\,dz = -\int_{\Gamma_1} f(z)\,dz$$

Análogamente

$$\int_{\Gamma_4} f(z)\,dz = -\int_{\Gamma_2} f(z)\,dz$$

Como $f(z+\omega_1) = f(z) = f(z+\omega_2)$ las integrales sobre lados opuestos de ∂P se cancelan

$$\int_{\partial P} f(z)dz = 0$$

por lo tanto

$$\sum_{z_j \, polos \, de \, f} Res_{z_j \in \mathring{P}} f(z) = 0$$

□

Teorema 3.2.2. *Sean $a_1, \cdots, a_r$ y $b_1, \cdots, b_s$ los ceros y polos, con multiplicidades $k_1, \cdots, k_r$ y $l_1, \cdots, l_s$ respectivamente, de una función elíptica f con respecto a $\Omega \subset \mathbb{C}$.*

$$\sum_{h=1}^{r} k_h a_h \sim \sum_{j=1}^{s} l_j b_j \; (mod\, \Omega)$$

Demostración. Sea P un paralelogramo especial para el lattice $\Omega_{\{\omega_1, \omega_2\}}$.

Primero se prueba $\forall\, h = 1, \cdots, r\,,\; j = 1, \cdots, s \,:\, a_h\,,\, b_j \,\in\, \mathring{P}$ que

$$\sum_{h=1}^{r} k_h a_h - \sum_{j=1}^{s} l_j b_j = \frac{1}{2\pi i} \int_{\partial P} \frac{z\, f'(z)}{f(z)}\, dz.$$

Si f tiene un cero de multiplicidad k en $z = a$, entonces $f(z) = (z-a)^k\, g(z)$, en un entorno de a, con g analítica y $g(a) \neq 0$. Entonces

$$\begin{aligned}
\frac{z\, f'(z)}{f(z)} &= \frac{z}{(z-a)^k g(z)} \left(k\,(z-a)^{k-1}\, g(z) + (z-a)^k g'(z)\right) \\
&= \frac{kz}{z-a} + \frac{z g'(z)}{g(z)} \qquad \text{(se reemplaza } z = z + a - a) \\
&= \frac{ka}{z-a} + k + \frac{(z-a+a) g'(z)}{g(z)} \\
&= \frac{ka}{z-a} + k + \frac{a g'(z)}{g(z)} + \frac{(z-a) g'(z)}{g(z)}
\end{aligned}$$

válido en un entorno de $z = a$. Luego $\dfrac{z\, f'}{f}$ tiene un polo simple en $z = a$ con residuo ka.

Si f tiene un polo de orden l en $z = b$, se trabaja de manera análoga y se obtiene que $z = b$ es un polo simple de $\dfrac{z\, f'}{f}$ con residuo $-lb$.

Cuando los ceros y polos de f en el interior del paralelogramo especial P son $a_1, \cdots, a_r$ y $b_1, \cdots, b_s$ con multiplicidades $k_1, \cdots, k_r$ y $l_1, \cdots, l_s$ respectivamente, entonces por el teorema del residuo

$$\frac{1}{2\pi i} \int_{\partial P} \frac{z\, f'(z)}{f(z)}\, dz = \sum_{h=1}^{r} k_h a_h - \sum_{j=1}^{s} l_j b_j$$

Por otra parte, si se parametriza ∂P en forma análoga a la utilizada en el Teorema 3.2.1 y se recorre el contorno en sentido positivo, entonces

$$\begin{aligned}\int_{\Gamma_2} \frac{z\, f'(z)}{f(z)}\, dz &= \int_{\Gamma_2} \frac{(z-\omega_1)\, f'(z)}{f(z)}\, dz + \int_{\Gamma_2} \frac{\omega_1\, f'(z)}{f(z)}\, dz \\ &= -\int_{\Gamma_4} \frac{(z)\, f'(z+\omega_1)}{f(z+\omega_1)}\, dz + \omega_1[\ln f(z)]_{\Gamma_2} \\ &= -\int_{\Gamma_4} \frac{z\, f'(z)}{f(z)}\, dz + 2\pi i\, n_1\, \omega_1\end{aligned}$$

para algún $n_1 \in \mathbb{Z}$.

Esto se obtiene de considerar que Γ_4 es exactamente el arco $\Gamma_2 - \omega$ recorrido en sentido negativo. Además f y f' son funciones periódicas y $\ln f(z)$ cambia su valor en un múltiplo entero de $2\pi i$ cuando z recorre Γ_2 como en la Fig. 3.1.

Análogamente, se tiene que

$$\int_{\Gamma_1} \frac{z\, f'(z)}{f(z)}\, dz = -\int_{\Gamma_3} \frac{z\, f'(z)}{f(z)}\, dz + 2\pi i\, n_2\, \omega_2$$

para algún $n_2 \in \mathbb{Z}$, entonces

$$\begin{aligned}\sum_{h=1}^{r} k_h a_h - \sum_{j=1}^{s} l_j b_j &= \frac{1}{2\pi i} \int_{\partial P} \frac{z\, f'(z)}{f(z)}\, dz \\ &= \frac{1}{2\pi i} \sum_{j=1}^{4} \int_{\Gamma_j} \frac{z\, f'(z)}{f(z)}\, dz \\ &= \frac{1}{2\pi i}(2\pi i\, n_1\, \omega_1 + 2\pi i\, n_2\, \omega_2) \\ &= n_1\, \omega_1 + n_2\, \omega_2\end{aligned}$$

Luego, existen $n_1\,, n_2 \in \mathbb{Z}$, tal que

$$\sum_{h=1}^{r} k_h a_h - \sum_{j=1}^{s} l_j b_j = n_1\, \omega_1 + n_2\, \omega_2$$

y esto es un elemento de Ω, lo que completa la demostración. □

3.3. Orden de una función elíptica

Definición 3.3.1. *El* ***orden*** *de una función elíptica f es el número de soluciones de la ecuación $f(z) = \infty$. Se denota con* ***ord*** (f).

Teorema 3.3.2. *Si una función elíptica f tiene orden $N > 0$ entonces f toma cada valor $c \in \mathbb{C}^*$, donde $\mathbb{C}^* = \mathbb{C} \cup \{\infty\}$, en el interior de un paralelogramo especial, exactamente N veces.*

Demostración. Sea f función elíptica, por definición de orden, N es el número de soluciones de la ecuación $f(z) = \infty$. Luego sólo falta considerar para valores de c en el plano complejo finito, es decir $c \in \mathbb{C}$.

Sea $f(z) = c \quad$ con $c \in \mathbb{C}$. Ya que f y $f - c$, tienen el mismo orden $\forall\ c \in \mathbb{C}$, basta considerar el caso en que $c = 0$.

La función $\dfrac{f'}{f}$ resulta meromorfa y si P es un paralelogramo especial para f, la función $\dfrac{f'}{f}$ es analítica sobre ∂P, por lo tanto se puede integrar $\dfrac{f'}{f}$ sobre ∂P.
Como f es elíptica, también lo son f' y $\dfrac{f'}{f}$ luego, por el Teorema de Residuos

$$\int_{\partial P} \frac{f'(z)}{f(z)}\, dz = 2\pi i \sum_{z_j \text{ polos en } \mathring{P}} Res\left(\frac{f'(z)}{f(z)}\right)$$

Se sabe que en los ceros y polos de orden k de f pertenecientes al $\mathring{P}$, $\dfrac{f'}{f}$ tiene polos simples con residuo k y $(-k)$ respectivamente.

Sean $z_1, \cdots, z_r$ los ceros de f con multiplicidad k_h , $h = 1, 2, \cdots, r$ y $z'_1, \cdots, z'_s$ los polos de f de orden k'_j , $j = 1, 2, \cdots, s$. Por el Teorema 3.2.1, la suma de los residuos de $\dfrac{f'}{f}$ es cero y al aplicar el Principio del Argumento a la integral del primer miembro, se tiene

$$\begin{aligned}\int_{\partial P} \frac{f'(z)}{f(z)} dz &= 2\pi i\left(\sum_{h=1}^{r} k_h - \sum_{j=1}^{s} k'_j\right)\\ &= 0\end{aligned}$$

Luego

$$\sum_{h=1}^{r} k_h = \sum_{j=1}^{s} k'_j$$

es decir, el número de ceros de f es igual al número de polos en el interior de P, contando multiplicidades. Entonces la ecuación $f(z) = 0$ tiene N soluciones en el interior del paralelogramo especial P. □

Teorema 3.3.3. *Una función elíptica f es constante si y sólo si su orden N es nulo.*

Demostración. Si la función f es constante y analítica, entonces no tiene polos en $\mathbb{C}$, luego tiene orden $N = 0$.

Recíprocamente, suponga que $N = 0$, es decir la función f no tiene polos, luego f es analítica sobre $\mathbb{C}$. Sea P un paralelogramo especial para f, luego P es compacto y f continua, entonces $f(P)$ es subconjunto compacto de $\mathbb{C}$ y por lo tanto es acotado.

Como $f(\mathbb{C}) = f(P)$ se sigue que f es acotada en $\mathbb{C}$ y por el Teorema de Liouville, como f es analítica y acotada, luego debe ser constante. □

Teorema 3.3.4. *No existen funciones elípticas de orden $N = 1$.*

Demostración. Suponga por el contrario que f sea una función elíptica de orden $N = 1$. Ésta debería tener un polo de orden 1 en el interior de P, es decir $\exists\, a \in \mathring{P} : z = a$ es un polo simple de f en $\mathring{P}$, luego

$$f(z) = \sum_{j=-1}^{\infty} a_j\,(z-a)^j\ ; \qquad 0 <\mid z-a \mid < r$$

con $a_{-1} \neq 0$. Así la suma de los residuos de f en el interior de P es a_{-1} distinto de cero. Esto es una contradiccción, por el Teorema 3.2.1. □

3.4. Ceros y Polos de funciones elípticas

Proposición 3.4.1. *Sean f y g dos funciones elípticas con respecto al lattice Ω.*

(i) Si f y g tienen polos en los mismos puntos de $\mathbb{C}$ y con la misma parte principal en esos puntos, entonces $f(z) = g(z) + c$ para alguna constante compleja c.

(ii) Si ambas funciones tienen ceros y polos en los mismos puntos de $\mathbb{C}$ y del mismo orden, entonces $f(z) = cg(z)$ para alguna constante compleja $c \neq 0$.

Demostración. Las funciones $f - g$ y $\dfrac{f}{g}$ son elípticas y no tienen polos, luego su orden es cero. Por el Teorema 3.3.3 estas funciones son constantes en $\mathbb{C}$. □

Proposición 3.4.2. *Toda función racional $f : \mathbb{C}^* \longrightarrow \mathbb{C}^*$, no idénticamente nula, tiene un número finito de ceros en $a_1, \cdots, a_r$ y de polos en $b_1, \cdots, b_s$ con multiplicidades $k_1, \cdots, k_r$ y $l_1, \cdots, l_s$, respectivamente.*
Y recíprocamente, dados los conjuntos disjuntos $\{a_1, \cdots, a_r\}, \{b_1, \cdots, b_s\} \subset \mathbb{C}^*$ y los números $k_1, \cdots, k_r\,; l_1, \cdots, l_s \in \mathbb{N}$, tales que

$$k_1 + \cdots + k_r \;=\; l_1 + \cdots + l_s$$

entonces existe una función racional f con ceros en los a_h y polos en los b_j y con multiplicidades k_h, l_j respectivamente.

Demostración. En un sentido la demostración es inmediata, en el otro la función racional es:

$$f(z) = \frac{\prod_h (z-a_h)^{k_h}}{\prod_j (z-b_j)^{l_j}}$$

con $a_h,\ b_j \in \mathbb{C}$ para $h = 1, 2, \cdots, r\ ;\ j = 1, 2, \cdots, s$, donde se excluyen los factores cuando $a_h = \infty$ ó $b_j = \infty$. □

Para las **funciones elípticas** existen propiedades análogas que se resumen en el siguiente resultado

Proposición 3.4.3. *Sean* k_h, l_j *con* $h = 1, 2, \cdots, r$; $j = 1, 2, \cdots, s$, *enteros no negativos y* a_h, b_j *números complejos.*

Las condiciones:

(i) $k_1 + \cdots + k_r = l_1 + \cdots + l_s = N_c = \sharp\{$ *soluciones de* $f(z) = c\}, \forall c \in \mathbb{C}$.

(ii) *los conjuntos* $\{a_1, \cdots, a_r\}$ *y* $\{b_1, \cdots, b_s\}$ *son disjuntos.*

(iii) $\sum k_j\, a_j \sim \sum l_j b_j \,(mod \Omega)$.

son suficientes para la existencia de una función elíptica f *con ceros y polos determinados.*

Por lo antes probado, *si* f *es elíptica con ceros en* a_h *con multiplicidad* k_h *con* $h = 1, 2, \cdots, r$ *y polos en* b_j *con multiplicidad* l_j ; $j = 1, 2, \cdots, s$, *entonces se cumplen* (i), (ii) *y* (iii).

Falta probar que *si valen* (i), (ii) *y* (iii), *entonces existe una función elíptica con esos ceros y polos y con esas multiplicidades.* Esto se desarrolla en una sección posterior.

.

4. Funciones de Weierstrass

4.1. Conceptos Previos

Sea $\Omega = \Omega_{\{\omega_1\,,\omega_2\}}$ un lattice, con $\{\omega_1\,,\,\omega_2\} \subset \mathbb{C}$ una base de Ω y sea P un paralelogramo fundamental para Ω. Se quieren construir funciones f, no constantes, elípticas respecto del lattice Ω y donde P resulte un paralelogramo especial para f. Se sabe por el Teorema 3.3.3, que tal función debe ser meromorfa y con sus polos en el interior de P. Además, como se demostró en el Teorema 3.3.4, f no puede tener un único polo simple en el paralelogramo P. Por lo tanto las funciones elípticas no constantes más sencillas tienen, al menos, orden 2. Luego deben tener o bien, dos polos simples con residuos opuestos, ó un polo de orden 2 con residuo cero, en $\mathring{P}$.

Para las funciones que nos interesa construir, es necesario el siguiente lema:

Lema 4.1.1. *Sean Ω un lattice en $\mathbb{C}$ y λ un número real, entonces la serie*

$$\sum_{\omega\,\in\,\Omega}{}' \frac{1}{|\omega|^{\lambda}} \qquad \textit{converge si y sólo si } \lambda > 2 \tag{4.1}$$

donde $\sum'_{\omega\,\in\,\Omega}$ indica $\omega \neq 0$

Demostración. Todos los períodos $\omega \in \Omega_{\{\omega_1\,,\omega_2\}}$, distintos de cero, están situados en los contornos de paralelogramos semejantes entre sí, todos con centro en el origen de coordenadas. En la Fig.4.1 se representan tres de ellos. El primer paralelogramo contiene en

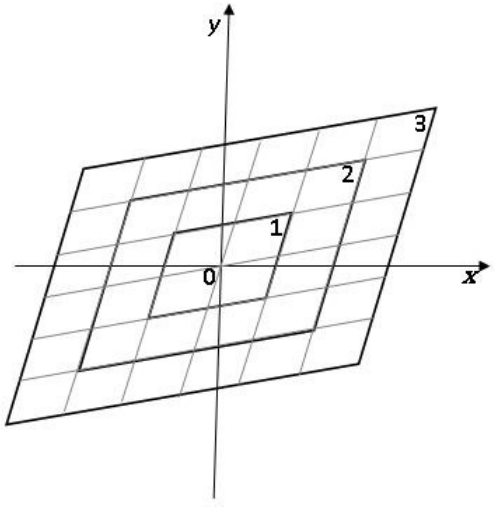


Figura 4.1: Paralelogramos concéntricos

su contorno ocho períodos distintos, el segundo contiene dieciseis.

Se supone que el contorno del k-ésimo paralelogramo contiene $8k$ períodos, entonces, proyectándolos en el $(k+1)$-ésimo paralelogramo, en direcciones paralelas a ω_1 y ω_2 se obtiene que, a cada período situado en el contorno del k-ésimo paralelogramo, distinto de

los vértices, le corresponde en el contorno del $(k+1)$-ésimo paralelogramo un período. A cada uno de los cuatro vértices le corresponden dos períodos.

Si a todo esto se le agregan los cuatro vértices del $(k+1)$-ésimo paralelogramo, se obtiene en su contorno ocho períodos más que en el contorno del precedente, en total, $8(k+1)$ períodos. La cantidad de períodos crece en progresión aritmética de razón 8.

Si d es la distancia del origen de coordenadas al primer paralelogramo, entonces kd es la distancia desde el origen al k-ésimo paralelogramo.

El módulo de cualquier período ω situado en el último circuito, verifica:

$$|\omega| \geqslant kd$$

de donde

$$\frac{1}{|\omega|^{\lambda}} \leqslant \frac{1}{k^{\lambda}\, d^{\lambda}}\,, \qquad \forall\, \lambda > 0$$

luego, la suma de los términos de la serie (4.1) que corresponden a los $8k$ períodos, situados en el contorno del k-ésimo paralelogramo no es superior a

$$\frac{8k}{k^{\lambda}\, d^{\lambda}} = \frac{8}{k^{\lambda-1}\, d^{\lambda}}$$

se deduce entonces, que la suma parcial de los términos de la serie (4.1) que corresponde a los períodos que están situados en el interior y en los lados del k-ésimo paralelogramo no es superior a:

$$\frac{8}{d^{\lambda}} \sum_{1}^{k} \frac{1}{j^{\lambda-1}}$$

pero la serie

$$\sum_{1}^{\infty} \frac{1}{j^{\lambda-1}}$$

converge para $\lambda > 2$; luego la serie (4.1) es convergente para $\lambda > 2$.

Si D es el mayor de los módulos de los períodos situados en el contorno del primer paralelogramo, se encuentra que la suma parcial de la serie (4.1) que corresponde a todos los períodos situados en el interior y en los lados del k-ésimo paralelogramo no es inferior a

$$\frac{8}{D^{\lambda}} \sum_{1}^{k} \frac{1}{j^{\lambda-1}}$$

Se deduce que la serie (4.1) es divergente si $\lambda \leq 2$. Luego

$$\frac{8}{D^{\lambda}} \sum_{1}^{k} \frac{1}{j^{\lambda-1}} \leq \sum_{\omega \in \Omega}{}' \frac{1}{|\omega|^{\lambda}} \leq \frac{8}{d^{\lambda}} \sum_{1}^{k} \frac{1}{j^{\lambda-1}}$$

□

4.2. La función $\wp$ de Weierstrass

En la búsqueda de una función elíptica de orden dos, se propone una función que sólo tenga un polo doble en el origen y en sus puntos congruentes respecto del lattice $\Omega \subset \mathbb{C}$. Además que sea analítica en todo otro punto y que la parte principal del desarrollo en serie de Laurent, alrededor del origen, sea:

$$\frac{1}{z^2}$$

No es posible definir la función buscada a partir de $\frac{1}{z^2}$ ya que $\sum_{\omega \in \Omega} \frac{1}{(z+\omega)^2}$ no converge en forma normal.

Existe una función que cumple con lo requerido, es la *función $\wp(z)$ de Weierstrass.*

Definición 4.2.1. *Se llama **función $\wp(z)$ de Weierstrass** a:*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega}{}' \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] \tag{4.2}$$

y también

$$\wp'(z) = \sum_{\omega \in \Omega} \frac{-2}{(z-\omega)^3} \tag{4.3}$$

Se demostrará que ambas funciones son elípticas en $\mathbb{C}$.

Proposición 4.2.2. *Las series anteriores (4.2) y (4.3) convergen absoluta y uniformemente sobre subconjuntos compactos de $\mathbb{C}$. Además $\wp(z)$ y $\wp'(z)$ son funciones meromorfas en $\mathbb{C}$ donde $\wp' = \dfrac{d\wp}{dz}$*

Demostración. Se prueba primero que la serie que define a $\wp'(z)$ es absoluta y uniformemente convergente en cada recinto acotado del plano complejo.

Es suficiente suponer que z pertenece a un círculo fijado arbitrariamente $|z| < R$ y considerar los términos de la serie que corresponden a los períodos ω que están situados fuera de un círculo de radio $2R$.

Para estos términos $\left|\dfrac{z}{\omega}\right| < \dfrac{1}{2}$ y se obtiene la acotación siguiente:

$$\begin{aligned} \left| \frac{1}{(z-\omega)^3} \right| &\leq \frac{1}{(|\omega| - |z|)^3} \\ &\leq \frac{1}{\left(1 - \frac{|z|}{|\omega|}\right)^3} \frac{1}{|\omega|^3} \\ &< \frac{8}{|\omega|^3} \end{aligned} \tag{4.4}$$

donde, en virtud del Lema 4.1.1, se deduce la convergencia absoluta y uniforme de la serie (4.3).

Si se designa la suma de la serie mediante $\wp'(z)$, se puede escribir, en el círculo $|z| < R$

$$\wp'(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3} = -2 \sum_{|\omega| \leqq R} \frac{1}{(z-\omega)^3} - 2 \sum_{|\omega| > R} \frac{1}{(z-\omega)^3} \quad ; \quad |z| < R$$

La primera suma del último miembro es el desarrollo de una función racional con un polo de tercer orden en cada período perteneciente al círculo $|z| < R$. La parte principal correspondiente tiene la forma $\dfrac{-2}{(z-\omega)^3}$

La segunda suma es una serie que difiere sólo en un número finito de términos de

$$\sum_{|\omega| > 2\,R} \frac{-2}{(z-\omega)^3}$$

cuya convergencia uniforme en el círculo $|z| < R$ se acaba de establecer. Luego la serie (4.3) converge uniformemente en subconjuntos compactos de $\mathbb{C}$.

Entonces la función $\wp'(z)$ es meromorfa en cualquier círculo $|z| < R$ con polos de tercer orden, ubicados en los períodos, pertenecientes al círculo indicado. Luego la función $\wp'(z)$ es meromorfa en todo el plano finito.

De manera análoga, si se considera el disco compacto $|z| \leq r$, se sabe que existe un número finito de elementos $\omega \in \Omega$ que verifican que $|\omega| < 2r$.

Sea $\omega \in \Omega$ tal que $|\omega| > 2\,r$, se encuentra que $\dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}$ es analítica en $|z| \leq r$. Es claro que

$$\begin{aligned} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| &= \left| \frac{(2\omega - z)z}{\omega^2 (z-\omega)^2} \right| \\ &\leq \frac{2|\omega| \left(1 + \frac{|z|}{2|\omega|}\right) |z|}{\left(1 - \frac{|z|}{|\omega|}\right)^2} \frac{1}{|\omega|^4} \\ &\leq \frac{10\,|z|}{|\omega|^3} \end{aligned}$$

Pero $|\omega| > 2r \geq 2|z|$, luego $\left| \dfrac{z}{\omega} \right| < \dfrac{1}{2}$, por lo tanto

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

de donde, por el Lema 4.1.1 se deduce la convergencia absoluta y uniforme de la serie (4.2) en cada disco compacto $|z| \leq r$. Por lo tanto $\wp(z)$ es meromorfa en $\mathbb{C}$.

Es sencillo ver que, a partir de la convergencia uniforme de la serie que define $\wp(z)$, derivando término a término, se encuentra $\wp'(z)$. □

Proposición 4.2.3. *$\wp'(z)$ es una función elíptica de orden 3, impar y con períodos fundamentales ω_1 y ω_2; donde $\{\omega_1\,,\,\omega_2\}$ es una base de Ω.*

Demostración. Si $\omega_0 \in \Omega$ se tiene que

$$\wp'(z+\omega_0) = \sum_{\omega\in\Omega} \frac{-2}{(z+\omega_0-\omega)^3} = \sum_{\omega\in\Omega} \frac{-2}{(z-(\omega-\omega_0))^3} = \sum_{\omega\in\Omega} \frac{-2}{(z-\omega)^3} = \wp'(z)$$

esto es así ya que la serie converge uniforme y absolutamente. Además si ω recorre todo el lattice Ω, entonces $\omega-\omega_0$ también recorre todo Ω. Esto dice que $\wp'(z)$ es doblemente periódica con períodos fundamentales ω_1 y ω_2 ya que todo período de f es combinación lineal de $\omega_1\,,\,\omega_2$ con coeficientes enteros. Por la forma de su desarrollo es claro que $\wp'$ tiene orden 3.

Además, si $z \in \mathbb{C}$

$$\begin{aligned} \wp'(-z) &= -2\sum_{\omega\in\Omega} \frac{1}{(-z-\omega)^3} \\ &= 2\sum_{\omega\in\Omega} \frac{1}{(z-(-\omega))^3} \\ &= -\wp'(z) \end{aligned} \tag{4.5}$$

si $\omega \in \Omega$, entonces $-\omega \in \Omega$, luego las series $\sum_{\omega\in\Omega} \frac{1}{(z-(-\omega))^3}$ y $\sum_{\omega\in\Omega} \frac{1}{(z-\omega)^3}$ sólo difieren en el orden de sus términos y su suma es la misma.

Luego $\wp'(-z) = -\wp'(z) \quad \forall\, z \in \mathbb{C}$ es decir $\wp'$ es función impar. □

Teorema 4.2.4. .

(i) *$\wp(z)$ es una función par*

(ii) *$\wp$ es una función elíptica con períodos fundamentales ω_1 y ω_2 .*

(iii) *$\wp\,(z)$ tiene orden 2.*

Demostración. .

(i) Si se calcula la derivada de $\wp(-z)$

$$\begin{aligned} (\wp(-z))' &= (\wp'(-z))(-1) \\ &= -(\wp'(-z)) \\ &= \wp'(z) \end{aligned} \tag{4.6}$$

esto vale $\forall\, z \in \mathbb{C}$ ya que $\wp'$ es función impar, integrando

$$\wp(-z) - \wp(z) = c \qquad \forall\, z \in \mathbb{C}$$

con c constante compleja. Si se considera $z = 0$, se obtiene que

$$\wp(0) - \wp(0) = c \quad \Rightarrow c = 0 \quad \Rightarrow \wp(-z) = \wp(z) \qquad \forall\, z \in \mathbb{C}$$

luego la función $\wp(z)$ es par.

(*ii*) Se sabe que $\wp'(z)$ es doblemente periódica, es decir

$$\wp'(z + \omega) = \wp'(z) \quad \forall\, \omega \in \Omega; \quad \forall\, z \in \mathbb{C}$$

Se define la función

$$g(z) := \wp(z + \omega) - \wp(z) \quad \forall\, \omega \in \Omega; \quad \forall\, z \in \mathbb{C}$$

al derivar se encuentra

$$g'(z) = \wp'(z + \omega) - \wp'(z) \equiv 0$$

luego

$$g'(z) = 0 \qquad \Rightarrow \quad g(z) = n \qquad \forall\, z \in \mathbb{C} \quad n \text{ cte. compleja}$$

Si se considera $z = -\dfrac{\omega}{2}$, resulta:

$$\wp\left(\frac{\omega}{2}\right) - \wp\left(-\frac{\omega}{2}\right) = n$$

y como $\wp$ es función par:

$$n = 0$$

luego

$$\wp(z + \omega) = \wp(z) \qquad \forall\, \omega \in \Omega, \quad \forall\, z \in \mathbb{C}$$

es decir $\wp$ es una función doblemente periódica. Al ser periódica repecto de Ω, sus períodos fundamentales son ω_1 y ω_2.

(*iii*) La parte principal correspondiente a cada polo $\omega \in \Omega$ tiene la forma $\dfrac{1}{(z-\omega)^2}$.
Luego $\wp(z)$ tiene sólo clases de congruencias de polos en el lattice de puntos $\omega \in \Omega$, cada uno de orden 2, por lo tanto $\wp(z)$ tiene orden 2.

□

Observación. *Estas dos funciones $\wp$ y $\wp'$ son fundamentales en la teoría de las funciones elípticas y se las llaman* ***funciones elípticas de Weierstrass****.*

Es importante notar que las funciones de Weierstrass dependen del particular lattice $\Omega \subset \mathbb{C}$, por ello en general se escribe $\wp(z, \Omega)$. Sin embargo en muchos casos el lattice Ω está automáticamente determinado, por lo que esa notación no es imprescindible.

4.3. La ecuación diferencial para $\wp$

Teorema 4.3.1. *Sea Ω un lattice en $\mathbb{C}$ y sea $(\wp(z), \Omega)$ la función de Weierstrass. Entonces $\wp(z)$ satisface la ecuación diferencial*

$$(y\prime)^2 = 4\,y^3 - g_2\,y - g_3 \tag{4.7}$$

donde

$$g_2 = 60\sum_{\omega\in\Omega}{}' \frac{1}{\omega^4}\,, \qquad g_3 = 140\sum_{\omega\in\Omega}{}' \frac{1}{\omega^6} \tag{4.8}$$

Además $g_2\,,\, g_3$ verifican que

$$g_2^3 - 27\,g_3^2 \neq 0 \tag{4.9}$$

Para demostrar este teorema son necesarios los dos lemas siguientes:

Lema 4.3.2. *Sea Ω un lattice en $\mathbb{C}$. Si n es impar entonces $\sum'_{\omega\in\Omega} \frac{1}{\omega^n} = 0$*

Demostración. La función $\rho : \Omega \to \Omega$ definida por $\rho(\omega) = -\omega$ es de orden 2 y su único punto fijo es el 0. Luego la órbita para $\omega \neq 0$ es $[\omega]_\rho = \{\omega\,,\, -\omega\}$, por lo tanto $\Omega \setminus \{0\}$ es unión disjunta de estas órbitas. Por ello si n es impar se cumple $\sum'_{\omega\in\Omega} \frac{1}{\omega^n} = 0$ □

Lema 4.3.3. *Sea Ω un lattice en $\mathbb{C}$ y $k \geq 2$. Entonces la serie*

$$G_{2k} = G_{2k}(\Omega) = \sum_{\omega\in\Omega}{}' \omega^{-2k} \qquad \textit{converge} \tag{4.10}$$

Demostración. Sea $\omega \in \Omega$ tal que $|\omega| > 1$. Entonces $|\omega|^{2k} \geq |\omega|^3$ para $k \geq 2$. Luego

$$\left| \sum_{\omega\in\Omega,|\omega|>1} \frac{1}{\omega^{2k}} \right| \leq \sum_{\omega\in\Omega,|\omega|>1} \frac{1}{|\omega|^{2k}} \leq \sum_{\omega\in\Omega,|\omega|>1} \frac{1}{|\omega|^3}$$

Por el Lema 4.1.1 se tiene que $\sum_{\omega\in\Omega,|\omega|>1} \frac{1}{|\omega|^3}$ converge, luego $\sum_{\omega\in\Omega,|\omega|>1} \frac{1}{\omega^{2k}}$ converge.

Se sabe que existe una cantidad finita de $\omega \in \Omega$ tales que $|\omega| \leq 1$. Luego

$$\sum_{\omega\in\Omega}{}' \frac{1}{\omega^{2k}} = \underbrace{\sum_{\omega\in\Omega,\,0<|\omega|\leq 1} \frac{1}{\omega^{2k}}}_{suma\,finita} + \sum_{\omega\in\Omega,|\omega|>1} \frac{1}{\omega^{2k}}$$

donde $\sum_{\omega\in\Omega,|\omega|>1} \frac{1}{\omega^{2k}}$ es convergente. Por lo tanto $\sum'_{\omega\in\Omega} \frac{1}{\omega^{2k}}$ converge. □

Observación 4.3.4. *Sea Ω un lattice en $\mathbb{C}$. Para cada natural $k \geq 2$, por la definición dada en la ec. (4.10) para*

$$G_{2k} = G_{2k}(\Omega) = \sum_{\omega\in\Omega}{}' \omega^{-2k}$$

la ecuación (4.7) toma la forma:

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - 60\,G_4\,\wp(z) - 140\,G_6 \tag{4.11}$$

donde G_4 y G_6 se definen como en (4.10).

Se demuestra el Teorema 4.3.1.

Demostración. A partir del desarrollo de Taylor

$$\frac{1}{1-t} = \sum_{n=0}^{\infty} t^n\,, \quad |t| < 1$$

se obtiene

$$\frac{1}{(1-t)^2} = \sum_{n=1}^{\infty} n\,t^{n-1} = \sum_{n=0}^{\infty}(n+1)\,t^n\,, \quad |t| < 1$$

Si se considera que $|z| < |\omega|$, con $\omega \in \Omega$, $\omega \neq 0$, así $\left|\frac{z}{\omega}\right| < 1$, entonces

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left[\left(1-\frac{z}{\omega}\right)^{-2} - 1\right] = \sum_{1}^{\infty}\frac{n+1}{\omega^{n+2}}\,z^n$$

converge en $|z| < |\omega|$ con $\omega \in \Omega \setminus \{0\}$. Por lo tanto, se encuentra

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Omega}{}'\sum_{n=1}^{\infty}\frac{n+1}{\omega^{n+2}}\,z^n \tag{4.12}$$

intercambiando el orden de las sumas, se obtiene

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{n=1}^{\infty}\sum_{\omega\in\Omega}{}'(n+1)\frac{z^n}{\omega^{n+2}} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}\left((n+1)\,z^n\sum_{\omega\in\Omega}{}'\frac{1}{\omega^{n+2}}\right)\end{aligned}$$

pero se sabe que si n es impar, $\sum'_{\omega\in\Omega}\frac{1}{\omega^{n+2}} = 0$. Luego el desarrollo de Laurent alrededor de $z = 0$

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}\left((2k+1)\,z^{2k}\sum_{\omega\in\Omega}{}'\frac{1}{\omega^{2k+2}}\right) \tag{4.13}$$

Por el Lema 4.3.3 se tiene que para $k \geq 1$,

$$\sum_{\omega\in\Omega}{}'\frac{1}{\omega^{2k+2}} \quad \text{converge.}$$

Entonces

$$\wp(z) = \frac{1}{z^2} + 3\left[\sum_{\omega\in\Omega}{}' \frac{1}{\omega^4}\right] z^2 + 5\left[\sum_{\omega\in\Omega}{}' \frac{1}{\omega^6}\right] z^4 + 7\left[\sum_{\omega\in\Omega}{}' \frac{1}{\omega^8}\right] z^6 + \cdots$$

$$\wp(z) = \frac{1}{z^2} + 3\,G_4\,z^2 + 5\,G_6\,z^4 + 7\,G_8\,z^6 + \cdots \quad \text{luego se deriva}$$

$$\wp'(z) = \frac{-2}{z^3} + 6\,G_4\,z + 20\,G_6\,z^3 + 42\,G_8\,z^5 + \cdots \quad \text{se eleva al cuadrado}$$

$$(\wp'(z))^2 = \frac{4}{z^6} - 24\,G_4\,\frac{1}{z^2} - 80\,G_6 + \cdots \quad \text{el cubo de } \wp(z)$$

$$(\wp(z))^3 = \frac{1}{z^6} + 9\,G_4\,\frac{1}{z^2} + 15\,G_6 + \cdots$$

luego se encuentra

$$\left(\wp'(z)\right)^2 - 4\left(\wp(z)\right)^3 + 60\,G_4\,\wp(z) + 140\,G_6 = h(z)$$

donde el segundo miembro es una función analítica en 0. Si tal función se denomina h, resulta $h(0) = 0$. El primer miembro es una función elíptica ya que $\wp$ y $\wp'$ lo son, luego h es elíptica y no tiene polos en una región fundamental que contiene a 0 entonces, por el teorema de Liouville, es constante. Pero $h(0) = 0$, luego se tiene que

$$\left(\wp'(z)\right)^2 - 4\left(\wp(z)\right)^3 + 60\,G_4\,\wp(z) + 140\,G_6 = 0$$

de donde

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - 60\,G_4\,\wp(z) - 140\,G_6$$

Se ha encontrado una ecuación diferencial de primer orden, que la función $\wp(z)$ satisface. □

Los coeficientes $60\,G_4$ y $140\,G_6$ se designan con g_2 y g_3 respectivamente, son **invariantes** de la función $\wp(z)$ y no dependen de los períodos fundamentales considerados.

Observación 4.3.5. *Se ha probado que la función elíptica $\wp$ de Weierstrass satisface la ecuación diferencial $(\wp')^2 = p(\wp)$, siendo p un polinomio cúbico de la forma*

$$p(z) = 4\,z^3 - g_2\,z - g_3 \tag{4.14}$$

donde $g_2 = g_2(\Omega)$ y $g_3 = g_3(\Omega)$ se determinan por las ecuaciones (4.8).

Todo polinomio que se exprese en la forma (4.14) se dice que está en la ***forma normal de Weierstrass****.*

Mediante la sustitución $\Psi : z \mapsto a\,z + b \quad (a\,,\,b \in \mathbb{C}\,,\,a \neq 0)$, cualquier polinomio cúbico se puede expresar en la forma (4.14) preservando la multiplicidad de sus ceros ya que $\Psi : \mathbb{C} \to \mathbb{C}$ es una biyección. Por lo tanto, sin pérdida de generalidad, se puede restringir el estudio a polinomios cúbicos que se encuentren en la forma normal de Weierstrass.

Teorema 4.3.6. *Si Ω es un lattice en $\mathbb{C}$, entonces*

$$4\,z^3 - g_2\,z - g_3 = 4\,(z-e_1)\,(z-e_2)(z-e_3) \tag{4.15}$$

con $e_i \neq e_j\,;\,\forall\, i \neq j$

Para demostrar este teorema se revisan las tres proposiciones siguientes:

Proposición 4.3.7. *Sea Ω un lattice con base $\{\,\omega_1\,,\,\omega_2\,\}$ y sea $\omega_3 = \omega_1 + \omega_2$. Si P es el paralelogramo especial con $0\,,\ \frac{1}{2}\,\omega_1\,,\ \frac{1}{2}\,\omega_2$ y $\frac{1}{2}\,\omega_3$ en su interior, entonces $\frac{1}{2}\,\omega_1\,,\ \frac{1}{2}\,\omega_2$ y $\frac{1}{2}\,\omega_3$ son los ceros de $\wp'$ en P, donde $\wp$ es la función de Weierstrass asociada al lattice.*

Demostración. Como la función $\wp'$ es de orden 3, tiene tres ceros en P.

Si $\omega \in \Omega$ entonces $\frac{1}{2}\,\omega \sim -\frac{1}{2}\,\omega\,(mod\,\Omega)$.

Se tiene $\wp'(\frac{1}{2}\,\omega) = \wp'(-\frac{1}{2}\,\omega)$ pero $\wp'$ es una función impar, por lo que

$$\wp'\left(\frac{1}{2}\,\omega\right) = \wp'\left(-\frac{1}{2}\,\omega\right) = -\wp'\left(\frac{1}{2}\,\omega\right)$$

luego $\wp'(\,\frac{1}{2}\,\omega)$ es 0 ó ∞.

Como el único polo de $\wp'$ en el interior de P es el polo triple 0, se tiene que $\wp'(\frac{1}{2}\,\omega_j) = 0$ para $j = 1,\,2,\,3$. □

Definición 4.3.8. *Sea el lattice $\Omega = \Omega_{\{\,\omega_1\,,\omega_2\,\}}$ y $\wp$ su correspondiente función de Weierstrass, se define*

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), \quad e_2 = \wp\left(\frac{\omega_2}{2}\right), \quad e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$$

Observación 4.3.9. *Si se llama $S = \left[\frac{1}{2}\omega_1\right] \cup \left[\frac{1}{2}\,\omega_2\right] \cup \left[\frac{1}{2}\,\omega_3\right]$ al conjunto de todos los ceros de $\wp'$ sobre $\mathbb{C}$, se observa que*

$$\{e_1\,,\,e_2\,,\,e_3\} = \wp(S)$$

es independiente de la particular base $\{\,\omega_1\,,\,\omega_2\,\}$ elegida para Ω.

Estos valores no dependen, salvo el orden, de la elección de la base del lattice Ω. Es usual denotar a los **valores críticos de** $\wp$ con $e_1\,,\,e_2\,,\,e_3$ y llamar **medios períodos** a

$$\frac{\omega_1}{2}\,,\ \frac{\omega_2}{2}\,,\ \frac{\omega_1+\omega_2}{2}$$

Proposición 4.3.10. *Para cada $c \in \mathbb{C}^* \setminus \{e_1\,,\,e_2\,,\,e_3\,,\,\infty\}$ la ecuación $\wp(z) = c$ tiene dos soluciones simples y para $c = e_1\,,\,e_2\,,\,e_3$ ó ∞ la ecuación tiene una solución doble.*

Demostración. Como $\wp$ es elíptica de orden 2, toma cada valor $c \in \mathbb{C}^*$ dos veces, según el Teorema 3.3.2, se tiene entonces dos soluciones simples, en z y $-z$, ó una solución doble, ya que $\wp$ es par.

Si $c \in \mathbb{C}$ entonces $\wp(z) = c$ tiene una solución doble si y sólo si $\wp'(z) = 0$, luego se encuentra que

$$z \sim \frac{1}{2}\omega_j \qquad (j = 1\,,\,2\,,\,3)$$

y por lo tanto $c = e_j\,;\ (j = 1,\,2,\,3)$.

El polo de orden 2 en $z = 0$ muestra que $\wp(z) = \infty$ tiene una solución doble en $z = 0$ y en todos sus puntos congruentes, luego en todos los puntos del lattice Ω.

Para todo otro valor de c, la ecuación $\wp(z) = c$ tiene dos soluciones simples. □

Proposición 4.3.11. *Los tres valores $e_1\,,\ e_2$ y e_3 son distintos dos a dos.*

Demostración. Sea $f_j(z) = \wp(z) - e_j$ para $j = 1,\,2,\,3\,.$

Para cada $j = 1,\,2,\,3\,,$ los polos de f_j son los mismos que los de $\wp\,,$ luego f_j es una función elíptica de orden 2 y por lo tanto tiene sólo dos ceros, contando multiplicidades.

Para cada $j = 1,\,2,\,3\,,$

$$f_j(z) = 0 \quad \Longleftrightarrow \quad \wp(z) = e_j \quad \Longleftrightarrow \quad z = \frac{1}{2}\omega_j$$

Y para los ceros dobles se cumple que: para cada $j = 1,\,2,\,3\,,$

$$f_j'(z) = 0 \quad \Longleftrightarrow \quad \wp'(z) = 0 \quad \Longleftrightarrow \quad z = \frac{1}{2}\omega_j$$

Luego, para cada $j = 1,\,2,\,3\,,$

$$f_j\left(\frac{1}{2}\omega_j\right) = f_j'\left(\frac{1}{2}\omega_j\right) = 0$$

Para cada $j = 1,\,2,\,3\,,$ f_j tiene ceros dobles en $\frac{1}{2}\omega_j$ y en sus puntos congruentes, por lo tanto no tiene otros ceros.

Para $j \neq k$ se verifica que $f_j\big(\frac{1}{2}\omega_k\big) \neq 0$ y como

$$\begin{aligned} f_j\left(\frac{1}{2}\omega_k\right) &= \wp\left(\frac{1}{2}\omega_k\right) - e_j \\ &= e_k - e_j \end{aligned} \tag{4.16}$$

se sigue que $e_j \neq e_k$ para $j \neq k$. □

Se demuestra el Teorema 4.3.6.

Demostración. Se demostró que la función elíptica $\wp$ de *Weierstrass* satisface la ecuación diferencial

$$(\wp')^2 = p(\wp); \qquad p(t) = 4\,t^3 - g_2\,t - g_3$$

Si se sustituye $\wp(t) = z$, se obtiene:

$$\left(\frac{dz}{dt}\right)^2 = 4\,z^3 - g_2\,z - g_3 \tag{4.17}$$

Se sabe que $\wp'(z)$ se anula para $z_1 = \dfrac{\omega_1}{2}$, $z_2 = \dfrac{\omega_2}{2}$ y $z_3 = \dfrac{\omega_1 + \omega_2}{2}$, luego el polinomio

$$4\,z^3 - g_2\,z - g_3 \tag{4.18}$$

debe anularse para $\wp(z_j) = e_j, \quad (j = 1,\, 2,\, 3)$.

Por lo tanto, se puede escribir

$$\left[\wp'(t)\right]^2 = 4\,[\wp(t) - e_1]\,[\wp(t) - e_2]\,[\wp(t) - e_3] \tag{4.19}$$

Como e_1 , e_2 y e_3 son números distintos entre sí, la ecuación cúbica

$$4\,\omega^3 - g_2\,\omega - g_3 = 0$$

tiene discriminante distinto de cero, luego

$$16\,\Delta = \left[\, g_2^3 - 27\,g_3^2 \,\right] = 16\,[e_2 - e_3\,]^2\,[e_3 - e_1\,]^2\,[e_1 - e_2\,]^2 \;\neq\; 0 \tag{4.20}$$

Por relación entre raíces y coeficientes de una ecuación algebraica, se obtiene:

$$e_1 + e_2 + e_3 = 0$$

$$g_2 = -\,4(e_1\,e_2 + e_2\,e_3 + e_3\,e_1) = 2(e_1^2 + e_2^2 + e_3^2)$$

$$g_3 = 4\,e_1\,e_2\,e_3$$

Luego, se demostró el teorema. □

La ecuación (4.19) proporciona para cada $\wp\,(z)$ dos valores de $\wp'\,(z)$ que se distinguen entre sí sólo por el signo. Esto concuerda con el hecho de que $\wp\,(z)$ no varía al sustituir z por $-z$, ya que es función par, mientras que $\wp'\,(z)$ cambia de signo por ser función impar.

4.4. La función ζ de Weierstrass

Si se comparan las funciones doblemente periódicas con las simplemente periódicas, entonces, como correspondiente de la función $\wp(z)$, que tiene un polo doble en cada uno de los períodos $\omega = m\omega_1 + n\omega_2$, con parte principal $\dfrac{1}{(z-\omega)^2}$, se puede considerar a la función $\operatorname{cosec}^2 z$, ya que también posee un polo doble en cada uno de sus períodos $\alpha = n\pi$ con parte principal $\dfrac{1}{(z-\alpha)^2}$, sin embargo no pueden ser tratadas de manera similar.

Existen funciones trigonométricas más simples que $\operatorname{cosec}^2 z$ que están estrechamente relacionadas con esta función, por ejemplo $\operatorname{cotg} z$ tiene polos simples en cada uno de los períodos α con parte principal $\dfrac{1}{z-\alpha}$ y $\operatorname{sen} z$ con ceros simples en cada uno de los períodos. Estas funciones se relacionan a través de:

$$(\operatorname{cotg} z)' = -\operatorname{cosec}^2 z \quad ; \quad (\ln \operatorname{sen} z)' = \operatorname{cotg} z.$$

Entre las funciones elípticas no pueden existir funciones con polos simples en los períodos (y que no tengan otros polos) ni funciones enteras. Sin embargo, sin exigir que sean elípticas, se pueden construir funciones vinculadas a $\wp(z)$ del mismo modo que las funciones $\operatorname{cotg} z$ y $\operatorname{sen} z$ estan vinculadas a $\operatorname{cosec}^2 z$.

Se define y se analiza la **función ζ de Weierstrass** que desempeña un papel importante en los cálculos con funciones elípticas.

Definición 4.4.1. *Sea Ω un lattice de $\mathbb{C}$ y $\wp$ la función de Weierstrass asociada, se llama función ζ de Weierstrass a la función definida por las siguientes condiciones:*

$$\big[\zeta(z)\big]' = -\wp(z) \qquad y \qquad \lim_{z\to 0}\left[\zeta(z) - \frac{1}{z}\right] = 0 \tag{4.21}$$

Esta función se puede expresar en la forma:

$$\zeta(z) - \frac{1}{z} = -\int_0^z \left[\wp(\psi) - \frac{1}{\psi^2}\right] d\psi$$

donde la integración se efectúa a lo largo de cualquier curva rectificable que no pase por los puntos $\omega \in \Omega$.

Como $\wp$ tiene residuos cero, es la derivada de una función analítica $\forall\, z \in \mathbb{C} \setminus \Omega$; luego la función ζ está bien definida.

Si se reemplaza $\wp(z)$ por su desarrollo en fracciones simples y se integra término a término, se obtiene:

$$\zeta(z) = \frac{1}{z} + \sum_{\omega\in\Omega\,,\,\omega\neq 0}\left[\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right] \quad , \quad |z| < |\omega| \tag{4.22}$$

La convergencia es clara, salvo por el término $\dfrac{1}{z}$. La nueva serie se obtiene al integrar término

a término una serie uniformemente convergente, a lo largo de cualquier contorno que no pase por los polos.

Luego la función $\zeta(z)$ es meromorfa y tiene polos simples en los puntos $z = \omega$ con parte principal $\dfrac{1}{z-\omega}$.

Se observa que $\zeta(z)$ es una función impar, en efecto,

$$\begin{aligned}\big[\zeta(z)+\zeta(-z)\big]' &= \zeta'(z)-\zeta'(-z)\\ &= -\wp(z)-(-\wp(-z)) \qquad \text{por definicion de } \zeta\\ &= -\wp(z)+\wp(-z) \qquad \wp \text{ es par}\\ &= 0\end{aligned}$$

y por lo tanto

$$\zeta(z)+\zeta(-z) \equiv C,$$

Luego se puede escribir

$$\big[\zeta(z)-\frac{1}{z}\big]+\big[\zeta(-z)-\frac{1}{-z}\big] \equiv C$$

Para $z \to 0$, cada término del primer miembro tiende a 0 (por la segunda condición de la definición); por lo tanto $C = 0$ y

$$\zeta(z) = -\zeta(-z)$$

Observación. *La función $\zeta(z)$ no es elíptica, ni es invariante por traslaciones, sin embargo su comportamiento bajo traslaciones facilita la construcción de funciones elípticas.*

Por definicion $\big[\zeta(z)\big]' = -\wp(z)$. Se observa entonces que

$$\big[\zeta(z+\omega_j)\big]' = -\wp(z+\omega_j) = -\wp(z) = \big[\zeta(z)\big]', \quad (j = 1,\, 2).$$

Por lo tanto se tiene

$$\big[\zeta(z+\omega_j)-\zeta(z)\big]' = 0$$

luego

$$\zeta(z+\omega_j)-\zeta(z) = \eta_j, \quad (j = 1,\, 2),$$

donde η_1 , η_2 son constantes independientes de z.

Si $\omega \in \Omega$ entonces $\omega = m\,\omega_1 + n\,\omega_2$, donde $m, n \in \mathbb{Z}$ y luego

$$\zeta(z+\omega) = \zeta(z)+\eta \tag{4.23}$$

donde

$$\eta = m\,\eta_1 + n\,\eta_2$$

Entre las cantidades ω_j y η_j existe una relación muy simple. Para deducirla se integra

la función $\zeta(z)$ a lo largo del contorno ∂P del paralelogramo para Ω, que contiene al 0 en su interior, con vértices $t\,,\, t+\omega_1\,,\, t+\omega_1\,+\,\omega_2\,,\, t+\omega_2$ y lados $\Gamma_1\,,\,\Gamma_2\,,\,\Gamma_3\,,\,\Gamma_4$, orientado positivamente, como muestra la Fig.4.2.

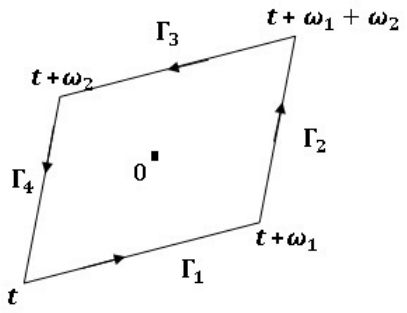


Figura 4.2: Paralelogramo especial

La función $\zeta(z)$ es meromorfa y tiene un único polo en el interior de P, en el punto 0 y con residuo igual a 1. Por el teorema de Residuos se tiene que

$$\begin{aligned} 2\pi i \;&= \int_{\partial P} \zeta\,(z\,)\,dz \\ &= \sum_{j=1}^{4} \int_{\Gamma_j} \zeta\,(z\,)\,dz \end{aligned}$$

Como

$$\begin{aligned} \int_{\Gamma_3} \zeta\,(z\,)\,dz &= -\int_{\Gamma_1} \zeta\,(z\,+\omega_2)\,dz \\ &= -\int_{\Gamma_1} (\zeta\,(z)\,+\eta_2)\,dz, \end{aligned}$$

entonces

$$\begin{aligned} \int_{\Gamma_1} \zeta\,(z\,)\,dz + \int_{\Gamma_3} \zeta\,(z\,)\,dz &= -\int_{\Gamma_1} \eta_2\,dz \\ &= \;-\eta_2\,\omega_1 \end{aligned}$$

Análogamente

$$\int_{\Gamma_2} \zeta\,(z\,)\,dz + \int_{\Gamma_4} \zeta\,(z\,)\,dz = \;\eta_1\,\omega_2$$

Luego

$$\eta_1\,\omega_2 - \eta_2\,\omega_1 = 2\pi i \tag{4.24}$$

A ésta ecuación se la llama ***relación de Legendre***. De lo anterior se deduce que al menos una de las constantes $\eta_1\,,\eta_2$ es no nula y por lo tanto $\zeta(z)$ *no es elíptica.*

.

5. El cuerpo de las funciones elípticas

5.1. Estructura de las funciones elípticas

En esta sección se muestra que toda *función elíptica con respecto a* Ω, un lattice de $\mathbb{C}$, es una función racional de $\wp$ y su derivada $\wp'$.

Sean f y g funciones elípticas, entonces también lo son $f+g$, $f-g$ y $f\,g$; además si g no es idénticamente nula, también $\dfrac{1}{g}$ es elíptica.

De este modo, el conjunto de las funciones elípticas tiene estructura de cuerpo y se lo denota con $E(\Omega)$.

Este cuerpo contiene un sub-cuerpo $E_1(\Omega)$ formado por las funciones elípticas pares. Las funciones constantes forman, a su vez, un sub-cuerpo de $E_1(\Omega)$, isomorfo a $\mathbb{C}$, por lo tanto se puede considerar a $E(\Omega)$ y a $E_1(\Omega)$ como extensiones del cuerpo $\mathbb{C}$.

Como $E_1(\Omega)$ contiene a $\wp(z) = \wp(z\,,\,\Omega)$, éste contiene a todas las funciones racionales de $\wp$ con coeficientes complejos. Estas funciones racionales forman el cuerpo $\mathbb{C}(\wp)$, que es el más pequeño cuerpo que contiene a $\wp$ y a las funciones constantes de $\mathbb{C}$.

Análogamente $E(\Omega)$ contiene a $\wp$ y a $\wp'$ y por lo tanto contiene al cuerpo $\mathbb{C}(\wp,\wp')$ de las funciones racionales de $\wp$ y $\wp'$; éste es el más pequeño cuerpo que contiene a $\wp$, $\wp'$ y $\mathbb{C}$.

Teorema 5.1.1.

(i) Si f es una función elíptica par, entonces $f = R_1(\wp)$ para alguna función racional R_1 y vale que $E_1(\Omega) = \mathbb{C}(\wp)$.

(ii) Si f es una función elíptica, entonces

$$f = R_1(\wp) + \wp' R_2(\wp)$$

donde R_1 y R_2 son funciones racionales y vale que $E(\Omega) = \mathbb{C}(\wp,\wp')$

Demostración. (i) Sea f una función elíptica. Como el resultado es obvio para funciones constantes, se supone que f tiene orden $N > 0$.

Si $k \in \mathbb{C}$, entonces $f(z) = k$ tiene soluciones múltiples sólo donde $f'(z) = 0$ y esto ocurre sólo en un número finito de clases de congruencias de puntos z, todos múltiples.

Cuando $f'(z) \neq 0$, $f(z) = k$ tiene soluciones simples para los valores de k no nulos del plano finito.

Se eligen dos números complejos c y d tal que las soluciones de $f(z) = c$ y $f(z) = d$ sean todas simples y por lo tanto no son congruentes a 0 ni a $\dfrac{1}{2}\omega_j$ $(j = 1, 2, 3)$.

Como f es par, el conjunto de todas las soluciones de

$$f(z) = c$$

en el paralelogramo fundamental, tendrá como elementos a: a_1 , $-a_1$, a_2 , $-a_2$, $\cdots$, a_n , $-a_n$, cada una simple y mutuamente no congruentes.

Análogamente $b_1\,,\ -b_1\,,\ b_2\,,\ -b_2\,,\ \cdots\,,\ b_n\,,\ -b_n$ son las soluciones de

$$f(z) = d$$

entonces la función elíptica

$$g(z) = \frac{f(z) - c}{f(z) - d}$$

tiene ceros simples en

$$\{a_1\,,\ -a_1\,,\ a_2\,,\ -a_2\,,\ \cdots\,,\ a_n\,,\ -a_n\}$$

y polos simples en

$$\{b_1\,,\ -b_1\,,\ b_2\,,\ -b_2\,,\ \cdots\,,\ b_n\,,\ -b_n\}.$$

Por la Proposición 4.3.10, las ecuaciones $\wp(z) = \wp(a_i)$ y $\wp(z) = \wp(b_i)$ tienen soluciones simples $z = \pm\, a_i,\ z = \pm\, b_i \quad (1 \leq i \leq n)$ respectivamente, por eso la función elíptica

$$h(z) = \frac{[\wp(z) - \wp(a_1)]\,[\wp(z) - \wp(a_2)]\,\cdots[\wp(z) - \wp(a_n)]}{[\wp(z) - \wp(b_1)]\,[\wp(z) - \wp(b_2)]\,\cdots[\wp(z) - \wp(b_n)]}$$

tiene los mismos ceros y polos que g, con las mismas multiplicidades, todas simples.

Luego por la Proposición 3.4.1 se deduce que $g = \mu h$ para alguna constante $\mu \neq 0$.

$$\frac{f(z) - c}{f(z) - d} = \mu \frac{[\wp(z) - \wp(a_1)][\wp(z) - \wp(a_2)]\cdots[\wp(z) - \wp(a_n)]}{[\wp(z) - \wp(b_1)][\wp(z) - \wp(b_2)]\cdots[\wp(z) - \wp(b_n)]}$$

Despejando $f(z)$, es claro que f es una función racional $R_1(\wp)$, con coeficientes complejos.

Así el cuerpo de las funciones elípticas pares $E_1(\Omega)$ es el cuerpo $\mathbb{C}(\wp)$ de las funciones racionales de $\mathbb{C}$ generadas por $\wp$.

(ii) Si f es una función elíptica impar, entonces el cociente $\dfrac{f}{\wp'}$ es par, luego por (i) se tiene que $f = \wp' R_2(\wp)$ para alguna función racional R_2.

En general, si f *es una función elíptica cualquiera*, entonces

$$f(z) = \frac{1}{2}[f(z) + f(-z)] + \frac{1}{2}[f(z) - f(-z)]$$

donde $\frac{1}{2}[f(z) + f(-z)]$ es una función elíptica par y $\frac{1}{2}[f(z) - f(-z)]$ es función elíptica impar.

Así se tiene que

$$f = R_1(\wp) + \wp' R_2(\wp)$$

donde R_1 y R_2 son funciones racionales.

Luego, el cuerpo de las funciones elípticas $E(\Omega)$ es el cuerpo $\mathbb{C}\,(\wp\,,\ \wp')$. □

Ejemplo. *Sea la función F:*

$$F = \frac{\wp\wp'}{\wp' + 1} \tag{5.1}$$

Se quiere expresar F en la forma $R_1(\wp) + \wp' R_2(\wp)$ donde R_1 y R_2 son funciones racionales de $\mathbb{C}$.
Se utiliza la ecuación diferencial que vincula a $\wp$ con $\wp'$

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2\,\wp(z) - g_3$$

donde $g_2 = 60\,G_4$ y $g_3 = 140\,G_6$
Si se realizan artificios convenientes y se eliminan potencias de $\wp'$, se obtiene

$$\begin{aligned}
\frac{\wp\wp'}{\wp' + 1} &= \frac{\wp\wp'}{\wp' + 1} . \frac{\wp' - 1}{\wp' - 1} \\
&= \frac{\wp\wp'(\wp' - 1)}{(\wp')^2 - 1} \\
&= \frac{\wp(\wp')^2 - \wp\wp'}{(\wp')^2 - 1} \\
&= \frac{(4\wp^4 - g_2\,\wp^2 - g_3\,\wp) - \wp\wp'}{4\wp^3 - g_2\,\wp - g_3\ - 1} \\
&= \frac{4\wp^4 - g_2\,\wp^2 - g_3\,\wp}{4\wp^3 - g_2\,\wp - g_3\ - 1} \ - \ \wp' \frac{\wp}{4\wp^3 - g_2\,\wp - g_3\ - 1}
\end{aligned}$$

luego las funciones racionales buscadas son

$$R_1(\wp) = \frac{4\wp^4 - g_2\,\wp^2 - g_3\,\wp}{4\wp^3 - g_2\,\wp - g_3 - 1}$$

y

$$R_2(\wp) = \frac{\wp}{4\wp^3 - g_2\,\wp - g_3 - 1}$$

5.2. Construcción de funciones elípticas con ceros y polos dados

Se aborda el problema específico de encontrar funciones elípticas f con polos y ceros dados. En la sección 3, se mostró que si $f \in E(\Omega)$ tiene en $a_1, \cdots, a_r$ y en $b_1, \cdots, b_s$ sus ceros y polos, con multiplicidades $k_1, \cdots, k_r$ y $l_1, \cdots, l_s$ respectivamente, entonces:

(i) $k_1 + \cdots + k_r = l_1 + \cdots + l_s$ (ambos miembros deben ser igual al orden de f)

(ii) los conjuntos $\{a_1, \cdots, a_r\}$ y $\{b_1, \cdots, b_s\}$ son disjuntos

(iii) $\sum_{h=1}^{r} k_h\, a_h \ \sim \ \sum_{j=1}^{s} l_j b_j \ (mod\ \Omega)$

Estas **tres** condiciones no son sólo necesarias, sino también son *suficientes para la existencia de una función elíptica f* respecto de un lattice fijo. Esto muestra que la situación es diferente al caso de funciones racionales, sobre la esfera, que sólo necesitan dos condiciones, las correspondientes a (i) y (ii).

Teorema 5.2.1. *Sean* $[a_1], \cdots, [a_r]$ *y* $[b_1], \cdots, [b_s]$ *elementos de* $\mathbb{C}/\Omega$ *para un lattice* Ω *y sean* $k_1, \cdots, k_r$; $l_1, \cdots, l_s$ *números enteros positivos. Si valen las condiciones* (i), (ii) *y* (iii), *entonces existe una función* $f \in E(\Omega)$ *con ceros de multiplicidad* k_h *en* $[a_h]$ *y polos de multiplicidad* l_j *en* $[b_j]$, *si* f *no tiene otros ceros ni polos.*

Demostración. Sea $u_h \in [a_h]$, $h = 1, \cdots, r$ y considere k_h su multiplicidad; si n es el orden de f entonces por (i)

$$n = \sum_{h=1}^{r} k_h$$

Análogamente, sean $v_j \in [b_j]$, $j = 1, \cdots, s$ y l_j su multiplicidad, entonces

$$n = \sum_{j=1}^{s} l_j$$

Por hipótesis los conjuntos $\{u_1, \cdots, u_r\}$ y $\{v_1, \cdots, v_s\}$ son disjuntos y la correspondiente condición (iii) toma la forma:

$$\sum_{h=1}^{r} k_h\, u_h - \sum_{j=1}^{s} l_j\, v_j = \omega \in \Omega$$

y esta relación no pierde generalidad si se reemplaza u_1 por su elemento congruente $u_1 - \omega$, luego (iii) se escribe

$$\underbrace{u_1 + \cdots + u_1}_{k_1} + \underbrace{u_2 + \cdots + u_2}_{k_2} + \cdots + u_r = v_1 + \cdots + v_1 + v_2 + \cdots + v_2 + \underbrace{\cdots + v_s}_{l_s}$$

renombrando los ceros y los polos, se puede escribir

$$\sum_{h=1}^{n} u_h^* = \sum_{j=1}^{n} v_j^*$$

Por el Teorema 3.3.2 es claro que se puede definir:

$$f(z) = \frac{[\wp(z) - \wp(u_1^*)] \cdots [\wp(z) - \wp(u_n^*)]}{[\wp(z) - \wp(v_1^*)] \cdots [\wp(z) - \wp(v_n^*)]}$$

Luego existe una función f que tiene ceros de multiplicidad k_h en $[a_h]$, con $h = 1, \cdots, r$, polos de multiplicidad l_j en $[b_j]$, para $j = 1, \cdots, s$ y tal que no tiene otros ceros ni polos. Es claro que $f \in E(\Omega)$, por el Teorema 5.1.1. □

Si g es cualquier otra función elíptica con los mismos ceros y polos que f, entonces por la Proposición 3.4.1 $g(z) = cf(z)$ para alguna constante $c \neq 0$.

5.3. Construcción de funciones elípticas con parte principal dada

Dados un conjunto finito arbitrario de polos y sus correspondientes partes principales, como el Teorema 3.2.1 impone condiciones sobre los residuos en esos polos, no resulta sencillo construir funciones elípticas sobre el toro $\mathbb{T} = \mathbb{C}/\Omega$.

Si una función elíptica f en $\mathbb{C}/\Omega$ tiene s polos diferentes en $b_1\,, \cdots, b_s$ y en sus puntos congruentes, con parte principal:

$$\sum_{k=1}^{l_j} \frac{a_{k,\,j}}{(z-b_j)^k} \tag{5.2}$$

en cada b_j $(1 \leqq j \leqq s)$, entonces la suma de los residuos es

$$\sum_{j=1}^{s} a_{1\,,\,j} = 0 \tag{5.3}$$

Se muestra que la ecuación (5.3) es una condición necesaria y suficiente para la existencia de una función elíptica $f(z)$ con parte principal dada por la expresión (5.2). Para ello es necesario el siguiente lema.

Lema 5.3.1. *Sean $c_1\,, \cdots, c_s$ números complejos y sea ζ la función de Weierstrass definida en (4.22). Entonces*

$$g\,(z) := \sum_{j=1}^{s} c_j\,\zeta(z-b_j)$$

es una función elíptica si y sólo si $\sum_{j=1}^{s} c_j = 0$

Demostración. Como la función $\zeta(z)$ es meromorfa, también lo es $g\,(z)$. Si $\omega \in \Omega$ entonces por (4.23)

$$\begin{aligned} g\,(z+\omega) &= \sum_{j=1}^{s} c_j\,\zeta(z+\omega-b_j) \\ &= \sum_{j=1}^{s} c_j\,\left[\zeta(z-b_j)+\eta\right] \end{aligned}$$

donde $\eta = m\,\eta_1 + n\,\eta_2$ para $\omega = m\,\omega_1 + n\,\omega_2$, luego

$$\begin{aligned} g\,(z+\omega) &= \sum_{j=1}^{s} c_j\,\zeta(z-b_j) + \sum_{j=1}^{s} c_j\,\eta \\ &= g(z) + \eta \sum_{j=1}^{s} c_j \end{aligned}$$

Por la relación de Legendre (4.24) al menos una de las constantes $\eta_1\,, \eta_2$ es no nula, luego $\eta \neq 0$ para algún $\omega \neq 0$ y por lo tanto $g(z)$ es elíptica con respecto a Ω si y sólo si $\sum_{j=1}^{s} c_j = 0$ □

Teorema 5.3.2. *Sean $b_1, \cdots, b_s$ números complejos, mutuamente no congruentes con respecto al lattice Ω y sean $l_1, \cdots, l_s$ números enteros no negativos. Si $a_{k,j}$ son números complejos $(1 \leqq k \leq l_j \ ; \ 1 \leqq j \leq s)$ tal que se verifica la ecuación (5.3) y $a_{l_j,j} \neq 0$ para cada j, entonces existe una función elíptica $f \in E(\Omega)$ con polos en $b_1, \cdots, b_s$ y parte principal, respecto de b_j, dada por la expresión (5.2) es decir:*

$$\sum_{k=1}^{l_j} \frac{a_{k,j}}{(z-b_j)^k} \quad (1 \leqq k \leq l_j \ ; \ 1 \leqq j \leq s)$$

Demostración. Se define:

$$f(z) := \sum_{j=1}^{s} \sum_{k=1}^{l_j} a_{k,j} F_k(z-b_j) \tag{5.4}$$

donde $F_1 = \zeta$, $F_2 = \wp$ y para $k \geq 3$, $F_k(z)$ es la función elíptica $\sum_{\omega \in \Omega} (z-\omega)^{-k}$

Para $k = 1$, por el lema anterior,

$$\sum_{j=1}^{s} a_{1,j} F_1(z-b_j)$$

es una función elíptica ya que $\sum_{j=1}^{s} a_{1,j} = 0$

La función F_k es elíptica $\forall\, k \geq 2$, luego f resulta una función elíptica.

Cada F_k tiene una única clase de polos de orden k, en puntos del lattice $\omega \in \Omega$, con parte principal respecto de 0 dada por z^{-k}, luego se sigue que los polos de f se encuentran en $[b_1], \cdots, [b_j]$, con parte principal respecto de b_j dada por (5.2) con la condición $a_{l_j,j} \neq 0 \quad \forall\, j$. □

Si g es otra función elíptica de la forma (5.4), con los mismos polos e igual parte principal que f, entonces por la Proposición 3.4.1, g y f difieren en una constante aditiva.

Observación. *Sea Ω un lattice de $\mathbb{C}$. Se denota con $V = V(l_1, b_1; l_2, b_2; \cdots; l_s, b_s)$ al conjunto de todas las funciones elípticas (respecto de Ω) que sean analíticas sobre $\mathbb{C} \setminus ([b_1] \cup \cdots \cup [b_j])$ y que además sean analíticas o tengan polos de orden l_j, a lo sumo, sobre cada clase $[b_j]$, con $1 \leq j \leq s$*

Si $f, g \in V$ entonces $f+g \in V$ y $cf \in V$, $\forall\, c \in \mathbb{C}$ constante, luego V tiene estructura de espacio vectorial sobre $\mathbb{C}$.

Teorema 5.3.3. *El espacio vectorial $V = V(l_1, b_1; l_2, b_2; \cdots; l_s, b_s)$ tiene dimensión $l_1 + \cdots + l_s$ sobre $\mathbb{C}$.*

Demostración. Por la demostración del Teorema 5.3.2 y las observaciones correspondientes, es claro que la forma más general de un elemento $g \in V$ está dada por $g = f + c$, donde

$c \in \mathbb{C}$ y f tiene la forma (5.4), es decir

$$f(z) = \sum_{j=1}^{s} \sum_{k=1}^{l_j} a_{k\,,j} F_k(z - b_j)$$

donde las constantes $a_{k,j}$ son arbitrarias, pero verifican la relación $\sum_{j=1}^{s} a_{1,\,j} = 0$.

Luego V está generado por:

- las $l_1 + \cdots + l_s - s$ funciones $F_k(z - b_j), \quad (2 \leq k \leq l_j \,;\, 1 \leq j \leq s)$;
- las $s - 1$ funciones $F_1(z - b_j) - F_1(z - b_1), \quad (2 \leq j \leq s)$
- la función constante 1.

Luego V tiene, a lo sumo, dimensión $(l_1 + \cdots + l_s - s) + (s - 1) + 1$.

Si se considera la parte principal de cada función, es fácil ver que las funciones son linealmente independientes sobre $\mathbb{C}$, por lo que forman una base para V. El espacio vectorial tiene la dimensión requerida. □

Este teorema es un caso particular del importante Teorema de Riemann-Roch, el cual da la dimensión de ciertos espacios de funciones meromorfas definidas sobre superficies de Riemann compactas.

Ejemplo. *Una base para el espacio vectorial* $V = V(2\,,\,0)$ *es* $\{\wp\,,\,1\}$*, ya que tiene un polo doble en cero. Luego la dimensión del espacio es dos,* $\dim V = 2$.

Por lo tanto la función elíptica más general, con polos de orden a lo sumo 2 *en* Ω *y analítica en* $\mathbb{C} \setminus \Omega$*, tiene la forma*

$$a\,\wp(z) + c \qquad a,\, c \in \mathbb{C}$$

.

6. Propiedades topológicas de las funciones elípticas

Se sabe que las funciones racionales $f : \Sigma \to \Sigma$ de grado $d > 0$ se pueden considerar como un cubrimiento con d-ramas de la esfera de Riemann Σ por sí misma.

Se recuerda que el *grado (u orden) de una función racional* $f = \frac{p}{q}$ es el máximo de los grados de los polinomios p y q, siendo p y q polinomios co-primos. Si $q = 1$, entonces f es un polinomio y $gr(f) = gr(p)$. Y f es constante si y sólo si $gr(f) = 0$.

Se supone ahora que la función $f : \mathbb{C} \to \Sigma$ es elíptica con respecto al lattice $\Omega \subset \mathbb{C}$ y que f tiene orden $N > 0$. Luego f induce una función

$$\widehat{f} : \mathbb{C}/\Omega \to \Sigma \text{ definida por } \widehat{f}([z]) = f(z), \quad \forall\, [z] \in \mathbb{C}/\Omega,$$

donde $[z]$ denota la clase de z.

Si se considera que $a \in \mathbb{C}$ y $f(a) = c$, $c \in \Sigma$ con multiplicidad k y si U es un entorno de a, suficientemente pequeño de manera que no existan en U pares de puntos congruentes, módulo Ω entonces, como se ve en Fig. 6.1, la proyección

$$p : \mathbb{C} \to \mathbb{C}/\Omega \text{ definida por } \quad z \mapsto [z]$$

mapea homeomórficamente U sobre un entorno $\widehat{U}$ de $[a]$ en $\mathbb{C}/\Omega$. Tal entorno U existe ya que Ω es discreto.

La función f resulta un mapeo abierto, localmente k-uno a uno en a y si se analiza el homeomorfismo de $U \to \widehat{U}$ es claro que $\widehat{f}$ es un mapeo abierto localmente k-uno a uno en $[a]$. *Los puntos de ramificación* de la función $\widehat{f}$ son los puntos de multiplicidad $k > 1$, es decir, los ceros de su derivada $\widehat{f}\,'$ y los polos múltiples de $\widehat{f}$ (si los tuviera).

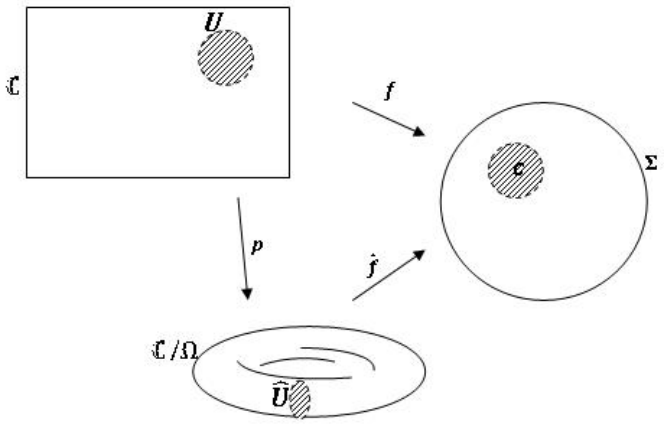


Figura 6.1: *El plano complejo, el toro y la esfera*

En el caso que se analiza, f y f' son funciones meromorfas, estos conjuntos, por la compacidad del toro $\mathbb{C}/\Omega$, son discretos y por lo tanto finitos. *El número de ramas* está

determinado por $|\widehat{f}^{-1}([a])| = N$, según el Teorema 3.3.2, es decir la cantidad de pre-imagenes de $\widehat{f}$.

Por lo tanto $\widehat{f}$ es un cubrimiento ramificado con N-láminas, *de la esfera* Σ *por el toro* $\mathbb{C}/\Omega$.

Si por **ejemplo** f fuera la función elíptica $\wp$ **de Weierstrass**, entonces $N = 2$, por lo tanto $\widehat{\wp}$ es un cubrimiento ramificado de 2-ramas de la esfera Σ por el toro $\mathbb{C}/\Omega$.

Por la Proposición 4.3.7 se sabe que la función $\wp'$ tiene ceros en las clases de congruencias $\left[\frac{1}{2}\,\omega_1\right]$, $\left[\frac{1}{2}\,\omega_2\right]$, $\left[\frac{1}{2}\,\omega_3\right]$, donde $\{\omega_1\,,\,\omega_2\}$ es una base de Ω y $\omega_3 = \omega_1 + \omega_2$. La multiplicidad k, de cada cero en $\wp$, debe satisfacer $1 < k \leq N = 2$, luego $k = 2$.

Además, existe una única clase de congruencia de polos de $\wp$, que es $[0] = \Omega$. Por lo tanto la función

$$\widehat{\wp} : \mathbb{C}/\Omega \to \Sigma$$

tiene cuatro puntos de ramificación de orden $k-1 = 1$; que son las clases $\left[\frac{1}{2}\,\omega\right]$ para $\omega \in \Omega$.

Se puede visualizar a la función $\widehat{\wp}$ de la siguiente manera:
Sea P un paralelogramo fundamental para Ω con vértices $\frac{1}{2}(\pm\omega_1 \pm \omega_2)$, entonces el 0 es el centro del paralelogramo. Como la función $\wp$ es par y tiene orden $N = 2$ vale que:

si $z_1\,,\, z_2 \in \mathring{P}$ entonces $(\,\wp(z_1) = \wp(z_2) \iff z_2 = \pm\, z_1\,)$

si $z_1\,,\, z_2 \in \partial P$ entonces $(\,\wp(z_1) = \wp(z_2) \iff z_2 \sim \pm\, z_1\,)$

Por lo tanto

$$\widehat{\wp}(\mathbb{C}/\Omega) = \wp(\mathbb{C}) = \wp(P)$$

La imagen del toro se puede obtener de la imagen de P, identificando cada punto del interior del paralelogramo con su opuesto y cada punto de su frontera con puntos en $[\pm\, z] \cap \partial P$.

La transformación

$$\rho : z \mapsto -z$$

produce una rotación, según un ángulo π, del paralelogramo P alrededor del origen 0. Fig.6.2.

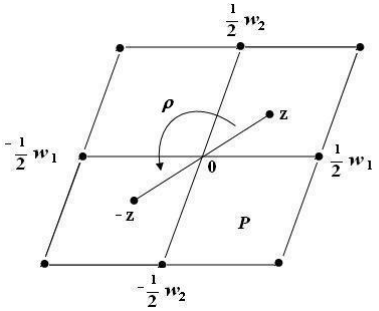


Figura 6.2: *Rotación alrededor del origen de coordenadas*

Además ρ mapea pares de puntos congruentes de la frontera de P, en pares de puntos congruentes, luego ρ induce un mapeo $\widehat{\rho}$ del toro $\mathbb{C}/\Omega$ en sí mismo, definido por

$$\widehat{\rho}([z]) = [\rho(z)] = [-z].$$

Los puntos fijos de $\widehat{\rho}$

$$[z] = [-z],$$

son las clases que satisfacen:

$$[2z] = [0] = \Omega$$

por lo tanto $\left[\frac{1}{2}\,\omega\right]$ son los cuatro puntos de ramificación de $\widehat{\wp}$.

Entonces se puede visualizar a $\mathbb{C}/\Omega$ como un toro de $\mathbb{R}^3$. La función $\widehat{\rho}$ representa una rotación de un ángulo π, alrededor de un eje que atraviesa al toro en estos cuatro puntos de ramificación, Fig.6.3.

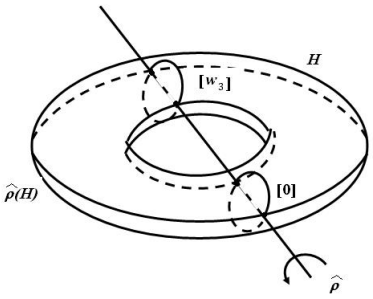


Figura 6.3: *Partición del toro*

En las Fig. 6.3 y Fig. 6.4 se muestra como se puede dividir al toro $\mathbb{C}/\Omega$ en dos mitades, H y $\widehat{\rho}(H)$, las cuales se intercambian por la función $\widehat{\rho}$ y se *"pegan"* a través de las dos *componentes circulares acotadas* C_1 *y* C_2 de H.

Cada punto en $\mathbb{C}/\Omega$ es equivalente, bajo la acción de $\widehat{\rho}$, a un único punto en H, excepto para los puntos sobre C_1 y C_2, que son equivalentes de a pares.
Por lo tanto se obtiene el espacio cociente $\widehat{\wp}(\mathbb{C}/\Omega)$ a partir de H, al identificar pares de puntos de $C_1 \cup C_2$ como se indica por las flechas, Fig.6.4.

El espacio resultante, Fig.6.5, es homeomorfo a la esfera, ya que $\widehat{\wp}(\mathbb{C}/\Omega)$ es la Esfera de Riemann Σ, como se ve, Fig.6.1.

En resumen, el efecto de $\widehat{\wp}$ sobre $\mathbb{C}/\Omega$ es tal que identifica cada clase $[z]$ con $[-z]$. Como la rotación $\widehat{\rho}$ tiene el mismo efecto, la imagen $\widehat{\wp}(\mathbb{C}/\Omega)$ es justo el espacio cociente bajo la acción de $\widehat{\rho}$ y éste es homeomorfo a la esfera.

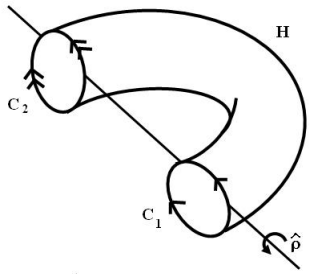


Figura 6.4: *Arcos congruentes del toro*

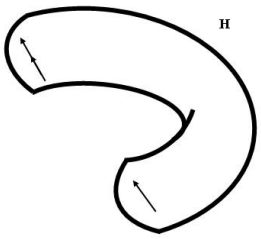


Figura 6.5: *Superficie homeomorfa a la Esfera*

6.1. Toros conformemente equivalentes

Un toro complejo es una variedad compleja sobre $\mathbb{R}$ de dimensión compleja 1 de la forma $T_\Omega = \mathbb{C}/\Omega$, donde Ω es un lattice en $\mathbb{C}$, o sea $\Omega = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$ donde ω_1 , ω_2 son linealmente independientes sobre $\mathbb{R}$.

El espacio T_Ω tiene una estructura compleja inducida por la proyección natural

$$\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Omega \text{ definida por } z \mapsto [z] \ , \quad \pi \text{ es holomorfa.}$$

Es claro que si

$$f : \mathbb{C}/\Omega \longrightarrow \mathbb{C}$$

Para todo abierto $V \subset \mathbb{C}$, su imagen $\pi(V)$ es abierta en $\mathbb{C}/\Omega$.

La restricción $f\,|_{\pi\,(V)}$ es holomorfa si y sólo si $f \circ \pi : V \longrightarrow \mathbb{C}$ es holomorfa.

Lo que interesa estudiar ahora, es el espacio $\boldsymbol{M} = \{\text{toros complejos} \,/\sim\}$, donde la relación de equivalencia $\sim$ se define:

$$\mathbb{C}/\Omega_1 \sim \mathbb{C}/\Omega_2 \Longleftrightarrow \exists\, \phi : \mathbb{C}/\Omega_1 \to \mathbb{C}/\Omega_2 \ \textit{biholomorfa.}$$

Luego, dos toros se dicen **conformemente equivalentes** si existe un homomorfismo analítico entre ellos.

Definición 6.1.1. *Un homomorfismo analítico es un homomorfismo de grupos que además es una aplicación holomorfa entre dos superficies de Riemann.*

Proposición 6.1.2. *Sean Ω_1, Ω_2 dos lattices de $\mathbb{C}$.*
Si $\phi : \mathbb{C}/\Omega_1 \to \mathbb{C}/\Omega_2$ es una aplicación holomorfa entre los toros complejos tal que cumple que $\phi(0) = 0$, entonces ϕ es el homomorfismo analítico inducido por la multiplicación, de un cierto número complejo a.

Es decir dados Ω_1, Ω_2 , lattices de $\mathbb{C}$, $\quad \mathbb{C}/\Omega_1 \sim \mathbb{C}/\Omega_2 \iff \exists\, a \in \mathbb{C} : a\,\Omega_1 = \Omega_2$

Demostración. Se define la función ϕ mediante el diagrama:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\widetilde{\phi}} & \mathbb{C} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Omega_1 & \xrightarrow[\phi]{} & \mathbb{C}/\Omega_2 \end{array}$$

Se puede suponer que $\phi([0]) = [0]$. Si no fuera así, se corrige con la traslación $z \to z - b \in Aut\,(\mathbb{C}/\Omega_2)$. Luego existe, por un resultado de topología algebraica, un *levantamiento* $\widetilde{\phi} : \widetilde{\phi}(0) = 0 \Rightarrow \widetilde{\phi}(z) = a\,z$ y entonces es claro que $a\,\Omega_1 \subset \Omega_2$

Si se usa $\phi^{-1} : \mathbb{C}/\Omega_2 \to \mathbb{C}/\Omega_1$, tal que $[0] \mapsto [0]$ y como ϕ biholomorfa, se *levanta* a

$$\widetilde{\phi^{-1}} : \mathbb{C} \to \mathbb{C};\ \text{tal que } 0 \mapsto 0$$

$$\widetilde{\phi^{-1}}(z) = \widetilde{\phi}^{-1}(z) = a^{-1}\,z \ \text{ y de esto } \ a^{-1}\,\Omega_2 \subset \Omega_1$$

Luego $a\,\Omega_1 = \Omega_2$ □

Definición 6.1.3. *Se dice que dos lattices en $\mathbb{C}$, Ω_1 y Ω_2 son $\mathbb{C}$-equivalentes si y sólo si $\exists\,\mu \in \mathbb{C}^{\mathrm{x}} = \mathbb{C} \setminus \{0\}$ tal que $\Omega_2 = \mu\,\Omega_1$*

Es decir dos lattices complejas se dicen $\mathbb{C}$-equivalentes si se relacionan mediante una homotecia y rotación.

Y dos toros $\mathbb{C}/\Omega_1$ y $\mathbb{C}/\Omega_2$ son isomorfos si y sólo si, los retículos Ω_1 y Ω_2 son $\mathbb{C}$-equivalentes.

Teorema 6.1.4. *El espacio cociente de los toros complejos en la relación de equivalencia de lattices ($\sim$), es isomorfo al espacio $SL_2(\mathbb{Z})/H$, donde H es el semiplano superior de $\mathbb{C}$.*

Demostración. Sea $\{\omega_1\,,\,\omega_2\,\}$ base ordenada del lattice Ω y el número complejo

$$\tau = \frac{\omega_2}{\omega_1}$$

tal que $Im(\tau) > 0$, si no se cambia por $\dfrac{\omega_1}{\omega_2}$. Luego $\mathbb{T}_{\langle \omega_1\,,\,\omega_2 \rangle} = \mathbb{T}_{\left\langle 1\,,\,\frac{\omega_2}{\omega_1} \right\rangle}$

Si se considera $\tau\,,\,\tau' \in H$

$$\mathbb{T}_\tau = \mathbb{T}_{\langle 1,\tau\rangle}\,,\,\mathbb{T}_{\tau'} = \mathbb{T}_{\langle 1,\tau'\rangle}$$

$$\begin{aligned}\mathbb{T}_\tau \sim \mathbb{T}_{\tau'} &\Leftrightarrow \exists\,\mu \in \mathbb{C}^x : \langle 1,\tau'\rangle = \mu\,\langle 1,\tau\rangle \\ &\Leftrightarrow \exists\,\mu \in \mathbb{C}^x : \tau' = \mu(a\,\tau + b\,) \quad \wedge \quad 1 = \mu(c\,\tau + d);\; a,\, b,\, c,\, d \in \mathbb{Z}\end{aligned}$$

entonces

$$\tau' = \frac{a\,\tau + b}{c\,\tau + d} \tag{6.1}$$

donde $a\,,\,b\,,\,c$ y $d \in \mathbb{Z}$ y $ad - bc = \pm 1$ ya que la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ es inversible.
Si ocurre que $ad - bc = -1$, la transformación

$$T : \tau \mapsto \frac{a\,\tau + b}{c\,\tau + d}$$

mapea H sobre el semiplano inferior, por lo tanto *la única posibilidad* es $ad - bc = 1$ ya que τ y τ' deben pertenecer al semiplano superior $H = \{\tau \in \mathbb{C}\,|\,Im(\tau) > 0\}$.

Recíprocamente si $a\,,\,b\,,\,c\,,\,d \in \mathbb{Z}$ y $ad - bc = 1$, entonces

$$\tau' = \left(\frac{1}{c\,\tau + d}\right)(a\,\tau + b) \quad \wedge \quad 1 = \left(\frac{1}{c\,\tau + d}\right)(c\,\tau + d) \tag{6.2}$$

luego $\mathbb{T}_\tau \sim \mathbb{T}_{\tau'} \Leftrightarrow \exists\gamma \in SL_2(\mathbb{Z}) : \tau' = \gamma\,\tau$
donde $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, inversible y $\gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ □

Observación 6.1.5. *Sean* $\Omega = \Omega_{\{\omega_1,\,\omega_2\}}$; $\Omega' = \Omega'_{\{\omega'_1,\,\omega'_2\}}$ *lattices en* $\mathbb{C}$ *tal que* $\tau = \dfrac{\omega_2}{\omega_1}$ *y* $\tau' = \dfrac{\omega'_2}{\omega'_1}$ *de* H*, entonces los siguientes enunciados son equivalentes:*

* *Los Toros* $\mathbb{C}/\Omega$ *y* $\mathbb{C}/\Omega'$ *son biholomorfos;*
* *Los lattices* Ω *y* Ω' *son* $\mathbb{C}$*-equivalentes;*
* $\tau' = \gamma(\tau)$ *para algún* $\gamma \in \Gamma = SL_2(\mathbb{Z})$

Esto sugiere que se puede obtener información del lattice y del toro, al estudiar la acción de Γ *sobre el semiplano superior* H*.*

Con esto en mente se analiza, más adelante en el trabajo, la función $j : H \to \mathbb{C}$ con la *propiedad*:

$$j(\tau') = j(\tau) \iff \tau' = \gamma(\tau)\,\text{para toda}\,\gamma \in \Gamma \quad \wedge \quad \tau \in H \tag{6.3}$$

7. Curvas elípticas

7.1. Definición

Inicialmente se puede pensar a una **curva elíptica** como el conjunto de soluciones $(x, y) \in \mathbb{C}^2$ de una ecuación de la forma:

$$y^2 = 4x^3 + ax + b, \text{ con } a, b \in \mathbb{C} \tag{7.1}$$

Si se toma un sistema de referencia adecuado y se realizan sustituciones convenientes, cualquier curva elíptica se puede expresar en la forma de la ecuación (7.1) llamada **forma de Weierstrass**.

Sea Ω un lattice en $\mathbb{C}$, se sabe que la función $\wp$, asociada al lattice, satisface la ecuación diferencial $(\wp')^2 = p(\wp)$, donde $p(x)$ es el polinomio cúbico $p(x) = 4x^3 - g_2x - g_3$, con

$$g_2 = 60 \sum_{\omega \in \Omega}{}' \frac{1}{\omega^4}\,, \qquad g_3 = 140 \sum_{\omega \in \Omega}{}' \frac{1}{\omega^6}$$

entonces todo punto $t \in \mathbb{C}/\Omega$ determina un punto $(\wp(t), \wp'(t))$ sobre la *curva elíptica*

$$E = \{(x, y) \in \widehat{\mathbb{C}} \times \widehat{\mathbb{C}} \,|\, y^2 = p\,(x)\} \quad \textit{donde } \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

Por lo tanto se puede considerar al conjunto E como la representación gráfica de la ecuación $y^2 = p(x)$, para $x, y \in \widehat{\mathbb{C}}$. Por ser subconjunto de $\widehat{\mathbb{C}} \times \widehat{\mathbb{C}}$, E tiene una topología natural.

Teorema 7.1.1. *El mapeo $\theta : \mathbb{C}/\Omega \to E$ definido por $t \mapsto (\wp(t), \wp'(t))$ es un homeomorfismo.*

Demostración. Los puntos $t = [0]\,; t = [\frac{1}{2}\,\omega_j]$ se mapean por θ, respectivamente sobre $(\infty\,,\,\infty)$ y $(e_j\,,\,0)$, para $j = 1, 2, 3$.

Para todo otro punto $(x, y) \in E$, como $\wp$ es par y tiene orden 2, la ecuación $\wp(t) = x$ tiene dos soluciones diferentes $t = \pm\, t_1$ siempre que $x \neq \{\infty\,,\, e_j\}$, $j = 1, 2, 3$. Por lo tanto

$$\begin{aligned} \wp'(t_1) &= -\,\wp'(-\,t_1) \quad \wp' \text{ función impar} \\ &\neq \wp'(-\,t_1) \quad \text{por ser soluciones simples} \end{aligned}$$

Entonces $\wp'(t_1)$ y $\wp'(-\,t_1)$ son los dos valores de la raíz cuadrada

$$\wp'(t) = \sqrt{p(\,\wp(t))} = \sqrt{p(x)}$$

y uno de estos valores es el que toma y, el que pertenece a la rama considerada. Luego, existe un único $t \in \mathbb{C}/\Omega$ con $t = t_1$ ó $t = -t_1$ que verifica $\theta\,(t) = (x,\, y)$, entonces θ es una biyección.

Las funciones $\wp$ y $\wp'$ son no constantes, meromorfas, abiertas y continuas. Por lo tanto θ también lo es, luego θ es un homeomorfismo. □

7.2. Curva elíptica real

Este embedding del toro $\mathbb{C}/\Omega$, como subconjunto E del producto cartesiano de dos esferas, es bastante difícil de visualizar. Por el momento nos concentramos en los *puntos reales* de E, es decir aquellos para los cuales $x\,,\, y \in \mathbb{R}$.

Se *define* como ***curva elíptica real*** al conjunto:

$$E_{\mathbb{R}} = \{(x,y) \in \mathbb{R}^2 \,|\, y^2 = p(x) = x^3 - g_2\, x - g_3\}$$

La gráfica de $y^2 = p(x)$ es la de una ecuación de dos variables reales. Luego es una curva plana no singular de grado 3.

Es claro que la curva $E_{\mathbb{R}}$ es simétrica respecto del eje x de $\mathbb{R}^2$, las otras propiedades de $E_{\mathbb{R}}$ se encuentran fácilmente bosquejando la gráfica de $p(x)$ y luego tomando las raíces cuadradas, siempre que $p(x) \geq 0$.

Por *ejemplo*, al ser un polinomio cúbico real sin raíces repetidas, $p(x)$ tiene una o tres raíces reales, según que el discriminante:

$$\Delta = g_2^3 - 27\, g_3^2$$

sea negativo o positivo, esto se puede ver fácilmente al considerar los puntos reales de $p(x)$. La curva $E_{\mathbb{R}}$ tiene entonces *una o dos componentes* respectivamente, como se muestra más adelante.

Definición 7.2.1. *Sea Ω un lattice de $\mathbb{C}$,*

- *La función meromorfa $f : \mathbb{C} \to \Sigma$ se dice* ***real*** *si $f(\overline{z}) = \overline{f(z)}, \quad \forall\, z \in \mathbb{C}$ ($\overline{\infty}$ se interpreta como ∞).*
- *El lattice Ω se dice* ***real*** *si $\overline{\Omega} = \Omega$ donde $\overline{\Omega} = \{\overline{\omega} \,|\, \omega \in \Omega\}$.*

Teorema 7.2.2. *Sean Ω un lattice de $\mathbb{C}$ y $\wp$ la función de Weierstrass asociada a Ω;*

$$g_2 = 60\, G_4\,, \quad g_3 = 140\, G_6; \quad G_k = \sum_{\omega \in \Omega}{}' \omega^{-k}\,, \quad k > 2$$

Entonces los siguientes enunciados son equivalentes:

(i) $g_2\,,\, g_3 \in \mathbb{R}$;

(ii) $G_k \in \mathbb{R} \qquad \forall\, k \geq 3$;

(iii) $\wp$ *es una función real;*

(iv) Ω *es un lattice real.*

Demostración. Primero se demuestra $(i) \Rightarrow (ii)$

Si se deriva $(\wp')^2 = 4\wp^3 - g_2\,\wp - g_3$ y se divide por $2\,\wp'$, ya que $\wp'$ no es idénticamente nula, se tiene que

$$\wp'' = 6\,\wp^2 - \frac{g_2}{2}$$

En la Sección 4 se encontró que la función $\wp(z)$ tiene un desarrollo de Laurent, válido alrededor de $z = 0$ dado por:

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} a_n\, z^{2n}$$

donde

$$a_n = (2n+1)G_{2n+2} = (2n+1)\sum_{\omega}{}' \omega^{-2n-2}$$

El coeficiente de z^{2n} en el desarrollo de $\wp''(z)$ es por lo tanto

$$(2n+2)(2n+1)a_{n+1}$$

mientras que el coeficiente de z^{2n} en el desarrollo de $(\wp(z))^2$ es

$$2a_{n+1} + \sum_{r+s=n} a_r\, a_s$$

Al igualar los coeficientes en la derivada segunda de $\wp$, para cada $n \geq 1$ se tiene:

$$(2n+2)(2n+1)\,a_{n+1} = 12\,a_{n+1} + 6\sum_{r+s=n} a_r\, a_s$$

y luego

$$(2n+5)(n-1)\,a_{n+1} = 3\sum_{r+s=n} a_r\, a_s$$

Para $n \geq 2$ se tiene:

$$a_{n+1} = \frac{3}{(2n+5)(n-1)}\sum_{r+s=n} a_r\, a_s$$

que expresa a_{n+1} en términos de $a_1 \cdots a_n$ así

$$\begin{aligned} a_3 &= \frac{1}{3}\,a_1^2 \\ a_4 &= \frac{3}{11}\,a_1 a_2 \\ a_5 &= \frac{1}{13}\,(2\,a_1\,a_3 + a_2^2) = \frac{1}{39}\,(2\,a_1^2 + 3a_2^2), \quad etc. \end{aligned}$$

Por recurrencia, se encuentra que cada coeficiente a_n es un polinomio en a_1 y a_2, con coeficientes racionales.

Si se reemplaza

$$a_n = (2n+1)\,G_{2n+2} \quad , \quad g_2 = 60\,G_4 \quad y \quad g_3 = 140\,G_6\,,$$

por inducción se muestra que cada G_k (para k par; $k \geq 4$) es un polinomio en g_2 y g_3 con coeficientes racionales, entonces si g_2 y g_3 fueran reales, G_k también lo será. Según el Lema 4.3.2, para todo k impar $G_k = 0$, luego se demostró (ii).

$(ii) \Rightarrow (iii)$

Si $G_k \in \mathbb{R} \quad \forall\, k \geq 3$, entonces los coeficientes del desarrollo en serie de Laurent de la función $\wp$ son reales, luego $\wp(z) = \overline{\wp(\,\overline{z}\,)}$ alrededor de $z = 0$. Las funciones $\wp(z)$ y $\overline{\wp(\,\overline{z}\,)}$ son funciones meromorfas, que coinciden en un entorno de cero, luego son iguales en todo el conjunto de los complejos. Entonces $\wp$ es una función real.

$(iii) \Rightarrow (iv)$

Sea $\omega \in \Omega$, entonces $\wp(z+\overline{\omega}) = \overline{\wp(\,\overline{z}+\omega)} = \overline{\wp(\,\overline{z}\,)} = \wp(\,z\,)$ ya que $\wp$ es real y ω es uno de sus períodos. Por lo tanto $\overline{\omega} \in \Omega$, luego $\overline{\Omega} \subseteq \Omega$.

Si se consideran los conjugados, se tiene que $\overline{\overline{\Omega}} = \Omega \subseteq \overline{\Omega}$, luego por igualdad de conjuntos $\Omega = \overline{\Omega}$ y entonces Ω es real.

$(iv) \Rightarrow (i)$

Esto es inmediato si se considera que por hipótesis Ω es real y que

$$g_2 = 60 \sum_{\omega \in \Omega}{}' \omega^{-4} \qquad y \qquad g_3 = 140 \sum_{\omega \in \Omega}{}' \omega^{-6}$$

□

Este teorema muestra que es suficiente caracterizar los lattices reales.

Definición 7.2.3. *Si Ω es un lattice de $\mathbb{C}$,*

- *Se dice que Ω es **real rectangular** si $\Omega = \Omega_{(\omega_1,\omega_2)}$ donde ω_1 es real y ω_2 es imaginario puro.*
- *Se dice que Ω es **real rómbico** si $\Omega = \Omega_{(\omega_1,\omega_2)}$ donde ω_1 no es real y $\omega_2 = \overline{\omega_1}$.*

El nombre del lattice Ω está determinado por el paralelogramo fundamental, con vértices $\{0,\, \omega_1\,,\, \omega_1+\omega_2\,, \omega_2\,\}$, según sea un rectángulo o un rombo respectivamente. Fig.7.1.

Teorema 7.2.4. *Un lattice Ω es real si y solamente si es real rectangular ó real rómbico.*

Demostración. Si $\Omega = \Omega_{(\omega_1,\omega_2)}$ es real rectangular, con $\omega_1 \in \mathbb{R}$ y $\omega_2 \in i\,\mathbb{R}$ entonces

$$\overline{\Omega} = \Omega_{(\overline{\omega_1},\overline{\omega_2})} = \Omega_{(\omega_1,\,-\omega_2)} = \Omega_{(\omega_1,\,\omega_2)} = \Omega$$

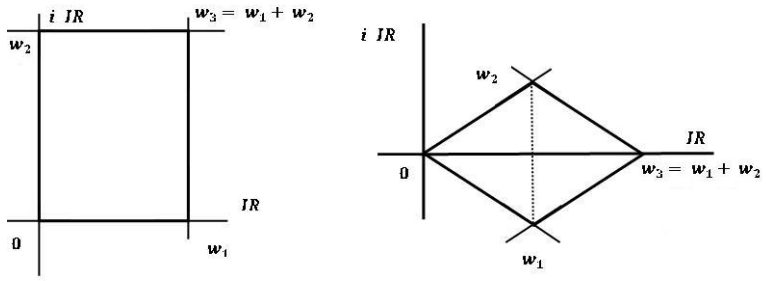


Figura 7.1: Lattices reales

luego Ω es real. Un argumento similar se aplica para el caso de lattices rómbicos:

$$\overline{\Omega} = \Omega_{(\overline{\omega_1}, \overline{\omega_2})} = \Omega_{(\omega_2, \omega_1)} = \Omega$$

Recíprocamente, se supone que Ω es real. Si $\omega \in \Omega$ entonces $\omega + \overline{\omega}$, $\omega - \overline{\omega} \in \Omega$, luego Ω contiene a ambos elementos real e imaginario puro y éstos forman los subgrupos discretos $\Omega \cap \mathbb{R} = \lambda\mathbb{Z}$ y $\Omega \cap i\mathbb{R} = \mu i\mathbb{Z}$ para ciertos λ, $\mu \in \mathbb{R}$; λ, $\mu > 0$.

Es claro que $\Omega \supseteq \lambda\mathbb{Z} + \mu i\mathbb{Z}$ y si se tiene la igualdad entonces Ω es real rectangular ya que $\{\lambda, \mu i\}$ es una de sus bases.

Si se supone que existe $\omega \in \Omega \setminus (\lambda\mathbb{Z} + \mu i\mathbb{Z})$ y se considera que $0 \leq Re(\omega) < \lambda$ y $0 \leq Im(\omega) < \mu$. Se obtiene

$$2\omega = (\omega + \overline{\omega}) + (\omega - \overline{\omega}),$$

con $(\omega + \overline{\omega}) \in \Omega \cap \mathbb{R} = \lambda\mathbb{Z}$ y $\omega - \overline{\omega} \in \Omega \cap i\mathbb{R} = \mu i\mathbb{Z}$, luego se tiene

$$2\omega = m\lambda + n\mu i \qquad m, n \in \mathbb{Z}$$

Las condiciones requeridas sobre $Re(\omega)$ e $Im(\omega)$ exigen que m y n tomen los valores 0 ó 1. Como ω no es ni real ni imaginario puro, se debe exigir que $m = n = 1$ y entonces $\omega = \dfrac{1}{2}(\lambda + \mu i)$.

Así todo elemento de $\Omega \setminus (\lambda\mathbb{Z} + \mu i\mathbb{Z})$ tiene la forma:

$$\frac{1}{2}(\lambda + \mu i) + a\lambda + b\mu i = (a + b + 1)\left(\frac{\lambda + \mu i}{2}\right) + (a - b)\left(\frac{\lambda - \mu i}{2}\right)$$

para los enteros a, b, mientras que todo elemento de $\lambda\mathbb{Z} + \mu i\mathbb{Z}$ tiene la forma:

$$a\lambda + b\mu i = (a + b)\left(\frac{\lambda + \mu i}{2}\right) + (a - b)\left(\frac{\lambda - \mu i}{2}\right).$$

Luego $\{\frac{1}{2}(\lambda + \mu i), \frac{1}{2}(\lambda - \mu i)\}$ es una base de Ω y éste es real rómbico. □

Teorema 7.2.5. *Sea Ω un lattice real. Entonces la curva elíptica real $E_{\mathbb{R}}$ tiene una o dos componentes según sea Ω un lattice real rómbico o real rectangular, respectivamente.*

Demostración. Como $E_{\mathbb{R}}$ es el gráfico de $y^2 = p(x)$, se puede contar sus componentes contando las raíces de $p(x)$, es decir, los puntos $(x, y) \in \mathbb{R}^2$ para los cuales $y = \wp'(z) = 0$ y $x = \wp(z) \in \mathbb{R}$ para algún $z \in \mathbb{C}$. Como $p(x)$ es un polinomio cúbico con raíces diferentes, existe uno o tres de tales puntos y $E_{\mathbb{R}}$ tiene una o dos componentes respectivamente.

Como las únicas soluciones de $\wp'(z) = 0$ son de la forma $z \sim \frac{1}{2}\omega_j$, $(j = 1, 2, 3)$ es suficiente determinar cuáles de los $e_j = \wp(\frac{1}{2}\omega_j)$ son reales.

Se propone $\Omega = \Omega_{(\omega_1,\omega_2)}$ real rectangular, con $\omega_1 \in \mathbb{R}$ y $\omega_2 \in i\mathbb{R}$. Fig.7.2.

Por Teorema 7.2.2 para un lattice real, la función $\wp$ es real, $\wp(\mathbb{R}) \subseteq \mathbb{R} \cup \{\infty\}$, luego $e_1 = \wp(\frac{1}{2}\omega_1) \in \mathbb{R}$.

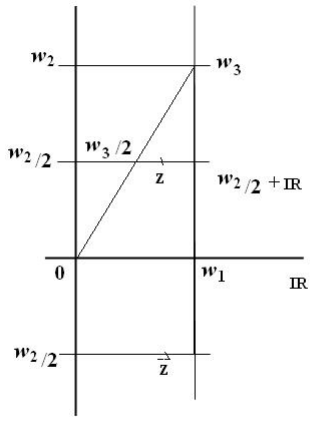


Figura 7.2:

Si $z \in \frac{1}{2}\omega_2 + \mathbb{R}$ entonces $\overline{z} = z - \omega_2$ y por lo tanto

$$\overline{\wp(z)} = \wp(\overline{z}) = \wp(z - \omega_2) = \wp(z)$$

luego $\wp(z) \in \mathbb{R}$.

Si se calcula $\wp(\frac{1}{2}\omega_2)$ y $\wp(\frac{1}{2}\omega_3)$ se encuentra que los respectivos valores e_2 y $e_3 \in \mathbb{R}$.

Entonces $p(x)$ tiene tres raíces reales, por lo que $E_{\mathbb{R}}$ intersecta al eje real x en tres puntos e_1, e_2, e_3, por lo tanto tiene dos componentes, una infinita que contiene a $(e_1, 0)$ y que corresponde a $Re(z) > e_1$, la otra acotada, que contiene a $(e_2, 0)$ y $(e_3, 0)$ que corresponde a $z \in \frac{1}{2}\omega_2 + \mathbb{R}$. Fig. 7.3.

Si $\Omega = \Omega_{(\omega_1,\omega_2)}$ es real rómbico, con $\overline{\omega_1} = \omega_2$, entonces de nuevo se tiene que $\wp(\mathbb{R}) \subseteq \mathbb{R} \cup \{\infty\}$ y por lo tanto $e_3 \in \mathbb{R}$. Ahora $\frac{1}{2}\overline{\omega_1} = \frac{1}{2}\omega_2$, luego

$$e_2 = \wp\left(\frac{1}{2}\omega_2\right) = \wp\left(\frac{1}{2}\overline{\omega_1}\right) = \overline{\wp\left(\frac{1}{2}\omega_1\right)} = \overline{e_1}$$

como $e_1 \neq e_2$, ninguno puede ser real, por lo tanto $p(x)$ tiene una única raíz real, luego $E_{\mathbb{R}}$ sólo tiene una componente que intersecta al eje x en $(e_3, 0)$ que corresponde a $z \in \mathbb{R}$.

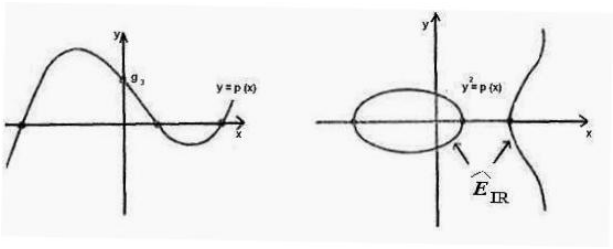
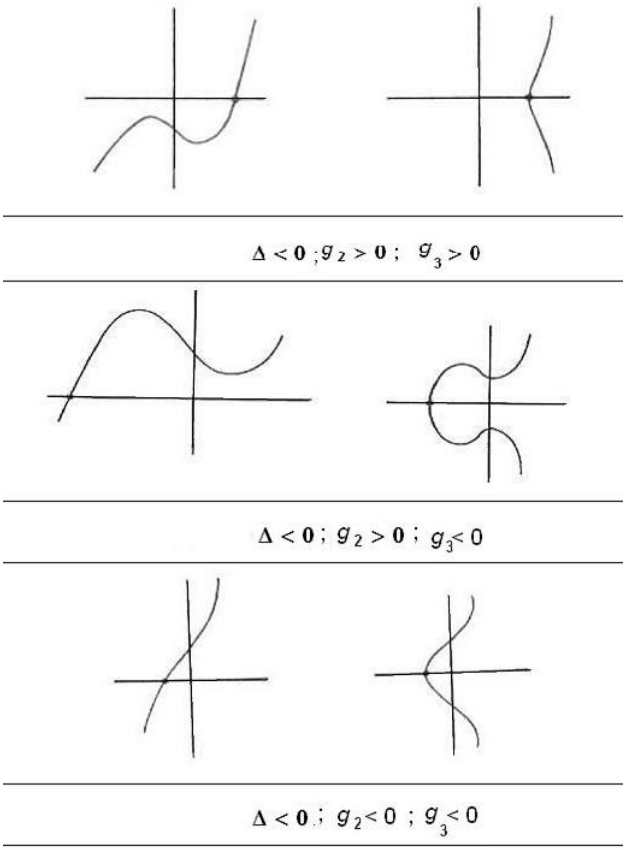


Figura 7.3: $\Delta > 0\,;\, g_2 > 0;\, g_3 < 0$

□



Nota: En los gráficos, la curva de la izquierda representa a $y = p\,(x)$ y sobre la derecha se representa $y^2 = p\,(x)$. Los puntos fijos son las intersecciones con el eje x. Cuando $\Delta > 0$ la curva de la derecha tiene dos componentes y si $\Delta < 0$ sólo una.

.

8. El teorema de Adición

Se dice que una función f posee un *Teorema de Adición* si existe una relación entre $f(z_1)$, $f(z_2)$ y $f(z_1+z_2)$ de la forma

$$R\big(f(z_1)\,,\,f(z_2)\,,\,f(z_1+z_2)\big)=0 \tag{8.1}$$

para todo $z_1\,,\,z_2\,\in\mathbb{C}$ donde R es una función racional no nula, con coeficientes complejos en sus componentes.

Si se multiplica (8.1) por el denominador de la función R se puede considerar que el primer miembro es un polinomio.

Observación. *La función R es una expresión racional de $f(z_1)$, $f(z_2)$ y $f(z_1+z_2)$. No se exige que f sea una función racional.*

Ejemplos conocidos del Teorema de Adición son aquellos que involucran a las funciones exponenciales y trigonométricas, tales como:

$$\exp(z_1+z_2)=\exp(z_1)\,.\,\exp(z_2) \tag{8.2}$$

y

$$\tan(z_1+z_2)=\frac{\tan(z_1)+\tan(z_2)}{1-\tan(z_1)\,\cdot\,\tan(z_2)} \tag{8.3}$$

ambas son equivalentes a identidades de la forma (8.1).

El teorema de adición para la función seno se obtiene de:

$$\operatorname{sen}(z_1+z_2)=\operatorname{sen}(z_1)\cos(z_2)+\operatorname{sen}(z_2)\cos(z_1)$$

si se reemplaza $\cos(z_j)=\sqrt{1-\operatorname{sen}^2(z_j)}$ para $j=1\,,\,2$ y se eleva al cuadrado dos veces para eliminar la raíz cuadrada.

Técnicas similares se aplican para las otras funciones trigonométricas.

Las *funciones racionales* poseen un Teorema de Adición, aunque la expresión correspondiente a (8.1) en general, no es ni obvia ni particularmente conveniente.

Para encontrar la expresión cuando f es una función racional, se sugiere el procedimiento siguiente:
Sea $f=\dfrac{p}{q}$ una función racional de z , con p y q polinomios; se define

$$\begin{aligned} g(u) &= p(u)-f(z_1)\,q(u)\\ h(v) &= p(v)-f(z_2)\,q(v)\\ k(u\,,\,v) &= p(u+v)-f(z_1+z_2)\,q(u+v) \end{aligned}$$

g, h y k son polinomios en las variables u, v o ambas. Sus coeficientes tienen la forma

$$a + bf(z_1)\,; \quad a + bf(z_2)\,; \quad a + bf(z_1 + z_2)$$

donde las constantes $a\,,\ b$ se obtienen de los coeficientes de p y q.

Más aún, las ecuaciones:

$$\left.\begin{aligned} g(u) &= 0 \\ h(v) &= 0 \\ k(u\,,\, v) &= 0 \end{aligned}\right\} \tag{8.4}$$

tienen una solución común[6] en $u = z_1\,,\ v = z_2$

Para obtener el polinomio resultante se puede eliminar u entre $g(u) = 0$ y $k(u\,,\, v) = 0$ y se encuentra $l(v)$. Luego al eliminar v entre $l(v) = 0$ y $h(v) = 0$ se obtiene un teorema de adición de la forma (8.1).

Ejemplo. *Sea* $f(z) = \dfrac{z}{z+1}$ *entonces* $p(u) = u\,;\ q(v) = v + 1\,;\ g(u) = u - f(z_1)(u + 1)$, *luego las ecuaciones (8.4) toman la forma:*

$$\begin{aligned} u(1 - f(z_1)) - f(z_1) &= 0 \\ v(1 - f(z_2)) - f(z_2) &= 0 \\ (u + v)(1 - f(z_1 + z_2)) - f(z_1 + z_2) &= 0 \end{aligned}$$

y eliminando u *y* v *se tiene una expresión para el* ***teorema de adición****;*

$$\frac{f(z_1)}{1 - f(z_1)} + \frac{f(z_2)}{1 - f(z_2)} = \frac{f(z_1 + z_2)}{1 - f(z_1 + z_2)}$$

La eliminación de u *y* v *es, por lo general, mucho más difícil de realizar cuando* f *tiene grado mayor que* 1.

Con un trabajo análogo y utilizando la expresión (8.2) para la función exponencial, se muestra que si $\omega \in \mathbb{C} \setminus \{0\}$ entonces toda composición de una función racional con $\exp(2\pi iz/\omega)$ tiene un teorema de adición.

Si además se considera $\omega = 2\pi$ se encuentran los teoremas de adición para las funciones trigonométricas.

[6] Una condición necesaria y suficiente para que dos ecuaciones polinomiales $s(u) = 0$ y $t(u) = 0$ tengan solución común u es que este valor anule al polinomio *resultante* de s y t.

8.1. El Teorema de Adición para funciones elípticas

El desarrollo de la teoría de las funciones elípticas y en particular del teorema de adición de ciertas integrales elípticas, se remonta a investigaciones de *C.G. Fagano* y *L. Euler* del siglo XVIII.

Un importante resultado de *K. Weierstrass* muestra que una función meromorfa con un teorema de adición debe ser la composición de una función racional con $\exp(2\pi iz/\omega)$ para $\omega \neq 0$, ó una función elíptica con respecto a un lattice.

Esto pone de manifiesto la estrecha relación entre las funciones *racionales*; las *simplemente periódicas* y las *doblemente periódicas*.

Para encontrar un teorema de adición de una función elíptica respecto de un lattice, se hace lo correspondiente para la curva elíptica asociada y para ello se muestra la *estructura de grupo* sobre la curva elíptica E.

En el Teorema 7.1.1 se probó que existe una biyección $\theta : t \mapsto (\wp(t)\,,\,\wp'(t)\,)$ entre el toro $\mathbb{C}/\Omega$ y la curva elíptica $E = \{(x\,,\,y) \in \widehat{\mathbb{C}} \times \widehat{\mathbb{C}} \,|\, y^2 = p(x) = 4x^3 - g_2x - g_3\,\}$

Como $\mathbb{C}/\Omega$ tiene estructura de grupo se puede usar θ para inducir esta estructura sobre la curva E de la siguiente manera:

Sea $P_j \in E$ para $j = 1\,,\,2$; se define $P_1 + P_2 = \theta(t_1 + t_2)$ donde $P_j = \theta(t_j)$; luego la correspondencia $\theta : \mathbb{C}/\Omega \longrightarrow E$ resulta un isomorfismo.

Es claro que el *elemento neutro* de E es $\theta([0]) = (\wp(0)\,,\,\wp'(0)) = (\infty\,,\,\infty)$ y si

$$P = (x\,,\,y) = (\wp(t)\,,\,\wp'(t)) \in E$$

entonces el *inverso* de P es

$$-P = (\wp(-t)\,,\,\wp'(-t)) = (\wp(t)\,,\,-\wp'(t)) = (x\,,\,-y)$$

luego el *inverso* de cada punto de E, es el que le corresponde por *reflexión sobre el eje real* x. Como la curva elíptica es simétrica respecto del eje x, es evidente la estructura de grupo de E.

Algo más difícil es expresar el **teorema de adición de** E, en términos de las coordenadas x e y.

Sea $P_j = (x_j\,,\,y_j) = \theta(t_j) \in E$ para $j = 1\,,\,2$ entonces $P_1 + P_2 = \theta(t_1 + t_2)$
Dejando de lado casos triviales, se puede suponer que $P_1\,,\,P_2$ y $P_1 + P_2$ son no nulos en E, es decir $t_1\,,\,t_2\,,\,t_1 + t_2 \neq [0]$

Se supone ahora que se tiene una función g, elíptica de orden 3, con polo triple en $[0]$ y ceros simples en t_1 y t_2 (ó un cero doble en t_1 si $t_1 = t_2$); entonces g debe tener un tercer

cero en $t_3 \in \mathbb{C}/\Omega$, donde

$$t_1 + t_2 + t_3 = [0] \ ,$$

según el Teorema 3.3.4. Al reemplazar $P_3 = (x_3 \, , \, y_3) = \theta(t_3)$ se obtiene

$$P_1 + P_2 + P_3 = 0$$

y por lo tanto

$$P_1 + P_2 = -\, P_3 = (x_3 \, , \, -\, y_3)$$

Note que las hipótesis acerca de t_1 y t_2 garantizan que ninguno de los ceros t_j coincide con el polo $[0]$ y que $t_3 \neq t_1 \, , \, t_2$

Se verá que tal función g existe. Se considera la función:

$$g(t) := \wp'(t) - \alpha \, \wp(t) - \beta \tag{8.5}$$

con constantes apropiadas $\alpha \, , \, \beta \in \mathbb{C}$; por construcción, cualquier función de esta forma tiene orden 3, con un polo triple en $[0]$.

Se supone primero que $t_1 \neq t_2$. Entonces g tendrá los ceros requeridos si se cumple que:

$$\wp'(t_j) \, = \, \alpha \, \wp(t_j) \, + \, \beta \, , \, j \, = \, 1 \, , \, 2$$

es decir

$$y_j = \alpha \, x_j + \beta \tag{8.6}$$

para $j = 1, 2$; como $t_1 \neq \pm \, t_2$ y $t_1 \, , \, t_2 \neq [0]$, se tiene que x_1 y x_2 son distintos y finitos, luego existen $\alpha \, , \, \beta \in \mathbb{C}$ que verifican (8.6). Como $g(t_3) = 0$, la ecuación (8.6) vale también para $j = 3$ y así los puntos $P_1 \, , \, P_2$ y P_3 están alineados en $\mathbb{C} \times \mathbb{C}$.

Si se reemplaza $P_3 = (\wp(t_1 + t_2) \, , \, -\wp'(t_1 + t_2))$ se deduce que

$$\begin{vmatrix} \wp(t_1) & \wp'(t_1) & 1 \\ \wp(t_2) & \wp'(t_2) & 1 \\ \wp(t_1 + t_2) & -\wp'(t_1 + t_2) & 1 \end{vmatrix} = 0$$

lo cual es válido también cuando $t_1 \, = \, t_2$.

Si se desarrolla este determinante y se tiene ***una forma del teorema de adición*** **para las funciones de Weierstrass** $\wp$ y $\wp'$.

8.2. Teorema de Adición para la función $\wp$ de Weierstrass

Se muestra ahora que la función $\wp$ de Weierstrass tiene un teorema de adición de la forma

$$R\big(\wp(t_1)\,,\,\wp(t_2)\,,\,\wp(t_1+t_2)\big)=0 \tag{8.7}$$

para alguna función racional R.

Para calcular los coeficientes α y β de la función g en la ecuación (8.5) se exigen dos condiciones:

Primero si $t_1 \neq t_2$, entonces de la expresión (8.6) se deduce que:

$$\alpha=\frac{y_1-y_2}{x_1-x_2} \tag{8.8}$$

Si además se considera que $y_j^2=p\,(x_j)$ y que $y_j=\alpha\,x_j+\beta$ para $j=1,2,3$, entonces se obtiene

$$p(x_j)-(\alpha\,x_j+\beta)^2=0\,;\quad j=1,2,3$$

Por lo tanto si x_1 , x_2 , x_3 son las raíces del polinomio cúbico:

$$p(x)-(\alpha\,x+\beta)^2=4\,x^3-\alpha^2\,x^2-(g_2+2\alpha\,\beta)x-(g_3+\beta^2)$$

Por relación entre raíces y coeficientes de una ecuación de tercer grado se tiene que:

$$x_1+x_2+x_3=\frac{\alpha^2}{4} \tag{8.9}$$

y al utilizar (8.8) y $\wp(t_1+t_2)=\wp(-t_3)=\wp(t_3)=x_3$, se obtiene:

$$\wp(t_1+t_2)=\frac{1}{4}\left(\frac{\wp'(t_1)-\wp'(t_2)}{\wp(t_1)-\wp(t_2)}\right)^2-\wp(t_1)-\wp(t_2) \tag{8.10}$$

válido para t_1, t_2, $t_1 \pm t_2 \neq [0]$

Esta expresión (8.10) se conoce como el ***Teorema de Adición*** **para** $\wp$ aunque extrictamente hablando se debería usar $(\wp')^2=p\,(\wp)$ para eliminar las derivadas y encontrar una ecuación de la forma (8.7).

Para cada $t_2 \neq [0]$ fijo, la ecuación (8.7) es válida para todo $t_1 \neq [0]\,,\,\pm t_2$; entonces se puede considerar a

$$R\big(\wp(t_1),\,\wp(t_2),\,\wp(t_1+t_2)\big)=0$$

como una función elíptica de t_1 . Como es función continua del toro en la esfera $\big(\mathbb{C}/\Omega \to \Sigma\big)$, entonces al tomar límite para t_1 tendiendo a cada uno de los valores especiales, se ve que la expresion (8.7) es válida para todo t_1 y para todo $t_2 \neq [0]$.

Si se fija t_1 y se hace tender $t_2 \to [0]$ es claro que la expresion (8.7) es válida para todo t_1, $t_2 \in \mathbb{C}/\Omega$.

Como ejemplo de este proceso límite, se fija $t_2 = t$ y se hace tender $t_1 \to t_2$, entonces se obtiene el *teorema del doble de t*

$$\wp(2t) = \frac{1}{4}\left(\frac{\wp''(t)}{\wp'(t)}\right)^2 - 2\wp(t) \tag{8.11}$$

Alternativamente se puede mostrar esta última expresión de otra manera: cuando $t_1 = t_2 = t$, la función

$$g = \wp' - \alpha\wp - \beta$$

tiene una raíz doble en t, es decir que

$$\wp''(t) - \alpha\wp'(t) = 0$$

luego

$$\alpha = \frac{\wp''(t)}{\wp'(t)}$$

entonces es claro que la expresión (8.11) se sigue de (8.9).

Por otro lado, la estructura de grupo de E y sus coordenadas cartesianas, muestran que

$$P_1 + P_2 \text{ es el punto } (x_3\,,\,-y_3) \in E,$$

y por (8.9)

$$\begin{aligned} x_3 &= \frac{\alpha^2}{4} - x_1 - x_2 \\ &= \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2 \end{aligned}$$

se tiene entonces,

$$y_3 = \alpha\, x_3 + \beta$$

con

$$\beta = \frac{x_1\, y_2 - x_2\, y_1}{x_1 - x_2}$$

y por lo tanto

$$y_3 = \frac{(x_3 - x_2)\, y_1 - (x_3 - x_1)\, y_2}{x_1 - x_2} \tag{8.12}$$

Esto muestra que las coordenadas de $P_1 + P_2$ se pueden expresar como funciones racionales con coeficientes racionales, de las coordenadas de P_1 y P_2.

Análogamente la inversión (reflexión respecto del eje real) $(x\,,\,y) \mapsto (x\,,\,-y)$ es una función racional, luego E es un ejemplo de *grupo algebraico*.

Suponga ahora que Ω **sea un lattice real**. Si se agrega el elemento $(\infty\,,\,\infty)$, neutro de E, a la curva elíptica real $E_{\mathbb{R}} = \{(x,y) \in E \,|\, x,y \in \mathbb{R}\}$, se encuentra:

$$\widehat{E_{\mathbb{R}}} = E_{\mathbb{R}} \cup \{(\infty\,,\,\infty)\}$$

luego $\widehat{E_{\mathbb{R}}}$ es subgrupo de E y por lo tanto es cerrado bajo las operaciones del grupo.

Dados $P_1 \neq P_2$ en $\widehat{E_{\mathbb{R}}}$, se puede encontrar $P_1 + P_2$ usando la colinealidad de $P_1\,,\,P_2$ y P_3; si se toma la recta $y = \alpha\, x + \beta$ que pasa por P_1 y P_2, se encuentra su tercer punto P_3 en la intersección con $\widehat{E_{\mathbb{R}}}$ y por la reflexión de éste, respecto del eje x (), se determina $P_1 + P_2 = -P_3$ Fig.8.1.

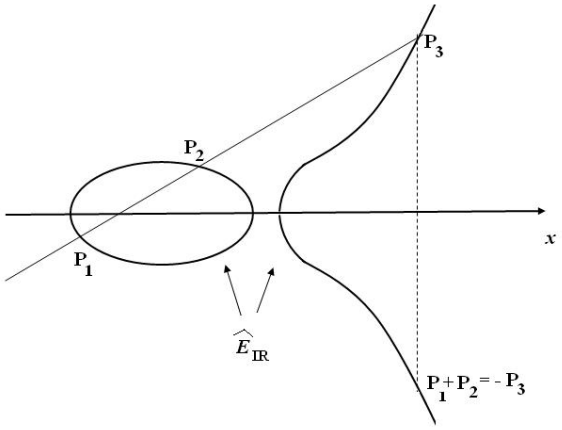


Figura 8.1: *Ley de Grupo en la curva elíptica*

Si $P_1 = P_2$ entonces se toma la recta tangente a $\widehat{E_{\mathbb{R}}}$ en P_1 y se repite el procedimiento anterior.

Un argumento similar muestra que si $g_2\,,\,g_3 \in \mathbb{Q}$ entonces **la curva elíptica racional**

$$\widehat{E_{\mathbb{Q}}} = \{(x,y) \in E \,|\, x,y \in \mathbb{Q}\} \cup \{(\infty,\infty)\}$$

es subgrupo de E.

Estos conceptos tienen gran importancia en la Teoría de Números, particularmente en la búsqueda de soluciones $x,y \in \mathbb{Z} \,|\, y^2 = p\,(x)$ donde p es un polinomio cúbico en una indeterminada.

Teorema 8.2.1. *Si $f\,,\,g \in E(\Omega)$ entonces existe un polinomio Φ en dos variables, no nulo, irreducible, con coeficientes complejos, tal que $\Phi\,(f,g)$ es idénticamente cero.*

Este teorema afirma que **toda función elíptica** f tiene un teorema de adición.

Ejemplo. *Las funciones $\wp$ y f son elípticas respecto del lattice Ω, como se verifican las hipótesis del teorema, entonces existe un polinomio no nulo Φ, irreducible, con coeficientes complejos tal que $\Phi(\wp, f) = 0$.*
Si se elimina $\wp(z_1)$, $\wp(z_2)$ y $\wp(z_1 + z_2)$ de las ecuaciones:

$$\begin{aligned} \Phi(\wp(z_1)\,,\, f(z_1)) &= 0 \\ \Phi(\wp(z_2)\,,\, f(z_2)) &= 0 \\ \Phi(\wp(z_1 + z_2)\,,\, f(z_1 + z_2)) &= 0 \\ R(\wp(z_1)\,,\, \wp(z_2)\,,\, \wp(z_1 + z_2)) &= 0 \end{aligned}$$

se encuentra una expresión polinomial que relaciona a $f(z_1)$, $f(z_2)$ y $f(z_1 + z_2)$.

La expresión que se obtiene es un ***Teorema de Adición para la función elíptica*** *f.*

9. Formas Modulares

9.1. Definiciones

Al semiplano superior se lo denota con $H = \{z \in \mathbb{C} \mid Im(z) > 0\}$ y con $SL_2(\mathbb{R})$ al grupo de las matrices cuadradas de orden 2, con coeficientes reales y determinante 1.

La acción de $SL_2(\mathbb{R})$ sobre $\mathbb{C}^* = \mathbb{C} \cup \{\infty\}$ se determina de la siguiente manera:

Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ es un elemento de $SL_2(\mathbb{R})$ y si $z \in \mathbb{C}^*$, se encuentra que

$$\gamma\, z = \frac{az + b}{cz + d} \tag{9.1}$$

Es claro que

$$Im(\gamma\, z) = \frac{Im(z\,)}{|cz + d|^2}$$

esto muestra que H es invariante bajo la acción de $SL_2(\mathbb{R})$.

El elemento $-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ de $SL_2(\mathbb{R})$ actúa trivialmente sobre H. Se puede considerar al grupo $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})\backslash\{\pm 1\}$ como el grupo de los automorfismos analíticos sobre H.

Se denota con $\Gamma = SL_2(\mathbb{Z})$ al subgrupo de las matrices con coeficientes enteros de $SL_2(\mathbb{R})$ y se puede probar que este subgrupo es discreto.

La imagen de $\Gamma = SL_2(\mathbb{Z})$ en $PSL_2(\mathbb{R})$ es el *grupo modular* $\Gamma\backslash\{\pm 1\}$. Si $\gamma \in \Gamma$, a menudo se utiliza el mismo símbolo para denotar su imagen en el grupo modular.

Sea $\mathcal{L} = \{\Omega \mid \Omega \text{ es un lattice de } \mathbb{C}\}$

En la Sección 4 se definió para $k \geq 2$ y $\Omega \in \mathcal{L}$

$$G_{2k} = G_{2k}(\Omega) = \sum_{\omega \in \Omega}{}' \omega^{-2k}$$

donde $\sum'_{\omega\, \in \Omega}$ indica que la suma se realiza sobre $\omega \in \Omega\,,\, \omega \neq 0$,

$$g_2 = 60\, G_4(\Omega) = 60 \sum_{\omega \in \Omega}{}' \frac{1}{\omega^4}$$

$$g_3 = 140\, G_6(\Omega) = 140 \sum_{\omega \in \Omega}{}' \frac{1}{\omega^6}$$

Proposición 9.1.1. *Sea* $\Omega \in \mathcal{L}$, *para* $\mu \in \mathbb{C} \setminus \{0\}$ *se verifica que*

$$G_{2k}\,(\mu\Omega) = \mu^{-2k}\, G_{2k}(\Omega)$$

Demostración.

$$\begin{aligned} G_{2k}(\mu\,\Omega) &= \sum_{\omega\in\mu\Omega}{}' \omega^{-2k} \\ &= \sum_{\omega\in\Omega}{}' (\mu\omega)^{-2k} \\ &= \mu^{-2k} \sum_{\omega\in\Omega}{}' \omega^{-2k} \\ &= \mu^{-2k}\, G_{2k}(\Omega) \end{aligned}$$

□

Si se considera $\Omega = \langle z\,,\,1\rangle$ y se define

$$g(z) := G_{2k}(\langle z\,,\,1\rangle) = \sum_{(a\,,\,b)\neq(0,0)} (a\,z+b)^{-2k} \quad ;\; z \in H \;\; con \;\; a\,,\,b \in \mathbb{Z}$$

Si $\gamma \in \Gamma$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad con\; a\,,\,b\,,\,c\,,\,d \in \mathbb{Z} \tag{9.2}$$

y se calcula

$$g(\gamma\,z) = G_{2k}(\gamma\,z) = G_{2k}\left(\left\langle \frac{az+b}{cz+d}\,,\,1\right\rangle\right) = (cz+d)^{-1(-2k)}\, G_{2k}\left(\langle az+b\,,\,cz+d\rangle\right)$$

Esta última igualdad vale por la proposición anterior y porque

$$\langle az+b\,,\,cz+d\rangle = \langle z\,,\,1\rangle$$

luego

$$g(\gamma\,z) = (cz+d)^{2k}\, G_{2k}(\langle z\,,\,1\rangle)$$

y por lo tanto

$$g(\gamma\,z) = (cz+d)^{2k}\, g(z)$$

Recíprocamente, si $g : H \to \mathbb{C}$ tal que

$$g(\gamma\,z) = (cz+d)^{2k}\, g(z)$$

donde H es el semiplano superior y γ la transformación bilineal racional con coeficientes enteros, definida por la matriz inversible (9.2), se define la función G para $Im\left(\dfrac{\omega_2}{\omega_1}\right) > 0$, donde $\{\omega_1, \omega_2\}$ es base del lattice Ω

$$G(\langle\omega_1\,,\,\omega_2\rangle) := \omega_1^{-2k}\, g\left(\frac{\omega_2}{\omega_1}\right)$$

además vale que

$$G(\mu\,\Omega) = \mu^{-2k}\,G(\Omega) \qquad \forall\,\mu \in \mathbb{C} \setminus \{0\}$$

Proposición 9.1.2. *Existe una correspondencia biunívoca entre las funciones:*

$$G : \mathcal{L} \to \mathbb{C} \quad ; \quad G(\mu\,\Omega) = \mu^{-2k}\,G(\Omega) \quad , \quad \forall\,\mu \in \mathbb{C} \setminus \{0\}\,,\ \Omega \in \mathcal{L}$$

$$g : H \to \mathbb{C} \quad ; \quad g(\gamma\,z) = (cz+d)^{2k}\,g(z) \quad , \quad \forall\,\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Ambas funciones $G : \mathcal{L} \to \mathbb{C}$ y $g : H \to \mathbb{C}$ son inversas entre sí. Luego $G \leftrightarrow g$ es una biyección.

Definición 9.1.3. *Sea $k \in \mathbb{Z}$. Una* ***función modular de peso*** $2k$ *es una función*

$f : H \to \mathbb{C}$ *meromorfa tal que:*

(i) $f(\gamma\,z) = (cz+d)^{2k}\,f(z) \quad , \quad \forall\,\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

(ii) f *es meromorfa en* ∞

Este concepto se aclara en las proposiciones siguientes:

Proposición 9.1.4. *Sea f una función meromorfa sobre H.*
f es una función modular de peso $2k$ si y sólo si verifica:

(a) $f(z+1) = f(z)$

(b) $f(-1/z) = z^{2k}\,f(z)$

La demostración en un sentido es inmediata si se observa que:

$$z+1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} z \quad , \quad -1/z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z \quad , \quad \textit{por la acción definida en (9.1)}$$

Por lo tanto

$$f(z+1) = 1^{2k} f(z) = f(z) \quad , \quad f(-1/z) = (z+0)^{2k} f(z) = z^{2k} f(z)$$

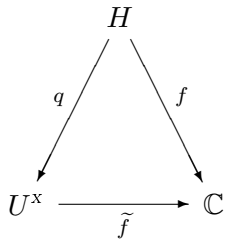
Luego valen las condiciones *(a)* y *(b)*.

Para la demostración en el otro sentido, se tiene en cuenta que las matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generan $SL_2(\mathbb{Z})$.

Además, para estudiar el comportamiento de la función en el infinito y debido a que $f(z+1) = f(z)$, basta estudiarla en el disco unidad U, centrado en cero. Entonces en las proximidades de $z = 0$, $\exists\, \widetilde{f} : U^x \to \mathbb{C}$, holomorfa, ($U^x$ indica al disco unidad sin el cero), entonces se puede expresar a f como composición de $q(z) = e^{2\pi i z}$ y $\widetilde{f}$, es decir

$$f(z) = \widetilde{f}(e^{2\pi i z}) \quad \text{con } \widetilde{f} \text{ meromorfa en } \; 0 < |q| < 1 \tag{9.3}$$

Esto se visualiza en el diagrama siguiente:



Luego

$$\widetilde{f}(q) = \sum_{-\infty}^{\infty} a_n\, q^n \;, \quad 0 < |q| < 1 \tag{9.4}$$

lo que equivale a que f admite un único desarrollo en serie de la forma:

$$f(z) = \sum_{-\infty}^{\infty} a_n\, e^{2\pi i n z} \;, \quad Im(z) > M \tag{9.5}$$

para M suficientemente grande y con los mismos coeficientes a_n de (9.4). Por ser f meromorfa existe $n_0 \in \mathbb{Z}$ y se cumple que $a_n = 0,\ \forall\, n < n_0$. A este desarrollo se lo llama *expansión de Fourier de $f(z)$ en ∞.*

Observación. *Como $\widetilde{f}$ admite el desarrollo (9.4) en un entorno del origen, se considera a $\widetilde{f}$ la prolongación meromorfa en el origen de la función f y por abuso de lenguaje, se dice que f es meromorfa en el infinito.*

Observación. *Cuando f es holomorfa en el infinito, su valor en ese punto está dado por*

$$f(\infty) = \widetilde{f}(0)$$

Definición 9.1.5. *Sea $k \in \mathbb{Z}$. Una **forma modular de peso** $2k$ es una función modular f que es holomorfa en el semiplano superior H y en el ∞. Y si además se cumple que: $f(\infty) = a_0 = 0$, f se llama **forma cuspidal**.*

Definición 9.1.6. *Dada una función meromorfa no idénticamente nula $f : H \to \mathbb{C}$ y un punto $p \in H$, se llama **orden de f en** p al número entero n tal que $f/(z-p)^n$ es holomorfa y no nula en p. Se denota con $v_p(f) = n$*

Si p es un cero de orden k, entonces $v_p(f) = k$

Si p es un polo de orden k, entonces $v_p(f) = -k$

Se define $v_\infty(f) = v_0(\widetilde{f})$, donde $f(z) = \widetilde{f}(e^{2\pi i z})$, como en (9.3)

Observación 9.1.7. *Si f es una función modular de peso $2k$, entonces*

$$v_p(f) = v_{\gamma p}(f)\,,\ \forall p \in H\ ,\ \forall \gamma \in \Gamma$$

Esto es inmediato a partir de la condición *(i)* en la Definición 9.1.3

Serie de Eisenstein de peso $2k$

Un ***ejemplo*** particular de funciones modulares de peso $2k$, son las Series de Eisenstein.

Se llama *serie de Eisenstein de peso* $2k$ a:

$$G_{2k}(z) = \sum_{(c\,,d)\neq(0\,,0)} (cz+d)^{-2k}\,, \qquad z \in H, \quad c\,,\, d\,,\, k \in \mathbb{Z}, \quad k \geq 2 \tag{9.6}$$

Se sabe, por el Lema 4.3.3, que converge para todo punto del semiplano superior y que

$$g(z) = G_{2k}(z) = G_{2k}(\langle 1\,,\, z\rangle)$$

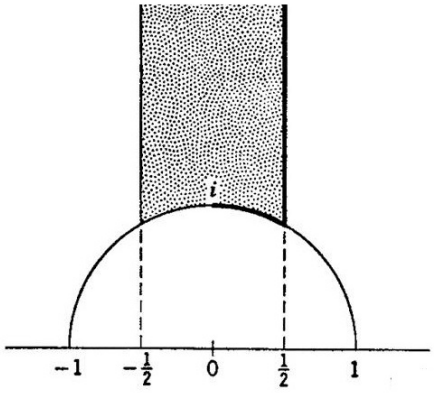


Figura 9.1: *Región Fundamental* ***F***

Las series de Eisenstein convergen en todo el semiplano superior. Ahora se estudia en una región fundamental particular **F**, la franja que se representa en la Fig.9.1. Se calcula

para $z \in \mathbf{F}$

$$\begin{aligned} |c\,z+d|^2 &= (c\,z+d)(c\,\overline{z}+d) \\ &= c^2\,|z|^2 + 2\,c\,d\,Re(z) + d^2 \quad \textit{donde } Re(z) \geq -1 \\ &\geq c^2\,|z|^2 - 2\,c\,d + d^2 \\ &\geq |c\,|z| - d|^2 \end{aligned}$$

Luego

$$\sum_{(c\,,\,d)\neq(0\,,\,0)} \frac{1}{|cz+d|^{2k}} \leq \sum_{(c\,,\,d)\neq(0\,,\,0)} \frac{1}{|c\rho-d|^{2k}} < \infty$$

por lo tanto, por el M-test de Weierstrass la serie $G_{2k}(z)$ converge uniformemente en $\mathbf{F}$. Luego converge uniformemente en $\gamma\,\mathbf{F}$, $\forall\,\gamma \in \Gamma = SL_2(\mathbb{Z})$ y define una función holomorfa en H. Esto ocurre ya que γ es un mapeo conforme y la serie converge uniformemente en $\mathbf{F}$.

En la proposición 9.5.1 se demuestra que:

$$G_{2k}(z) = 2\,\zeta(2k) + \sum_{(c\,,\,d)\neq(0\,,\,0)} (cz+d)^{-2k} \tag{9.7}$$

donde

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,, \qquad \forall\,s \qquad Re(s) > 1\ ,\ \text{es la función } \zeta \textit{ de Riemann.}$$

Por convergencia uniforme en H se puede calcular el límite, término a término, cuando $Im(z) \to \infty$ y resulta

$$\lim_{Im(z)\to\infty} G_{2k}(z) = 2\,\zeta(2k)$$

lo que dice que $G_{2k}(z)$ ***es una forma modular de peso*** $2k$ ***que no es cuspidal***.

Luego G_{2k} no es idénticamente constante. Note que G_4 y G_6 son las series de Eisenstein de peso 4 y 6 respectivamente.

Teorema 9.1.8.

$$\sum_{m=1}^{\infty} m^{-4} = \frac{\pi^4}{90} \qquad y \qquad \sum_{m=1}^{\infty} m^{-6} = \frac{\pi^6}{945}$$

Demostración. Se sabe que

$$\sum_{m=-\infty}^{\infty} (z-m)^{-2} = \pi^2\,\mathrm{cosec}^2\,\pi z \tag{9.8}$$

elevando al cuadrado e invirtiendo el desarrollo en serie de la función seno,

$$\operatorname{sen}\pi z = \pi z - \frac{\pi^3 z^3}{3!} + \frac{\pi^5 z^5}{5!} - \cdots$$

se obtiene la un desarrollo en serie de Laurent

$$\pi^2 \operatorname{cosec}^2 \pi z = \frac{1}{z^2} + \frac{\pi^2}{3} + \frac{\pi^4 z^2}{15} + \frac{2\pi^6 z^4}{189} + \cdots \tag{9.9}$$

válida en $|z| < 1$ ya que $\pi^2 \operatorname{cosec}^2 \pi z = \dfrac{1}{z^2}$ es analítica en el disco unidad.
Al diferenciar dos veces la expresión dada en (9.8) se tiene:

$$6 \sum_{m=-\infty}^{\infty} (z-m)^{-4} = \frac{6}{z^4} + \frac{2\pi^4}{15} + \frac{8\pi^6 z^2}{63} + \cdots$$

válida en $|z| < 1$
Diferenciando dos veces nuevamente, se obtiene

$$120 \sum_{m=-\infty}^{\infty} (z-m)^{-6} = \frac{120}{z^6} + \frac{16\pi^6}{63} + \frac{8\pi^6 z^2}{63} + \cdots$$

válida en $|z| < 1$
Si se cancelan las partes principales, en $z = 0$, con los sumandos correspondientes a $m = 0$ y reemplazando $z = 0$ se tiene

$$6 \sum_{m \in \mathbb{Z} - \{0\}} (-m)^{-4} = \frac{2\pi^4}{15}$$

y

$$120 \sum_{m \in \mathbb{Z} - \{0\}} (-m)^{-6} = \frac{16\pi^6}{63}$$

encontrando lo pedido. □

Nota: Este método permite evaluar la *función zeta de Riemann* $\sum_{m=1}^{\infty} m^{-s}$ en cada número entero par $s \geq 2$, por ejemplo:

$$\sum_{m=1}^{\infty} m^{-2} = \frac{\pi^2}{6}$$

La función discriminante Δ

Definición 9.1.9. *Se llama función discriminante a la función:*

$$\Delta(z) := g_2^3(z) - 27\, g_3^2(z) \tag{9.10}$$

donde $g_2 = 60\, G_4 \qquad y \qquad g_3 = 140\, G_6$

Si se calcula

$$\lim_{z\to\infty} \Delta(z) = (60\, G_4(\infty))^3 - 27\,(140\, G_6(\infty))^2$$
$$60\, G_4(\infty) = 60\, \frac{2\pi^4}{2\, 3^2\, 5} = \frac{4}{3}\pi^4$$
$$140\, G_6(\infty) = 140\, \frac{2\pi^6}{3^3\, 5\, 7} = \frac{2^3}{3^3}\pi^6$$

se obtiene que

$$\Delta(\infty) = \left(\frac{4}{3}\right)^3 \pi^{12} - 27\left(\frac{2^3}{3^3}\right)^6 \pi^{12} \ = 0.$$

La función discriminante $\Delta(z)$ ***es una forma modular cuspidal***. Es así por ser composición de formas modulares además de ser analítica en todo H y en el ∞ ; donde $\Delta(\infty) = 0$.

En el teorema 9.2.4 se demuestra que $\Delta(z) \neq 0 \quad \forall\, z \in H$ y que Δ es una forma modular cuspidal de peso 12.

Nota: El peso *mínimo* de una forma modular cuspidal es 12. Se puede probar que *si* $f(z)$ *es forma modular cuspidal de peso* $k < 12$, *entonces* $f(z) \equiv 0$.

9.2. El espacio de las formas modulares

9.2.1. Ceros y polos de una función modular

Se ha visto que si $f : \mathbb{C}/\Omega \to \mathbb{C}$ es elíptica y no idénticamente nula, entonces

$$\sum_1^r m_i - \sum_1^s m'_j = 0$$

donde $m_1\,, \cdots, m_r$ son los órdenes de ceros de f ; $m'_1\,, \cdots, m'_s$ los órdenes de polos de f y Ω el lattice de f.

Esto es parte de un resultado general, al que se refiere el siguiente teorema

Teorema 9.2.1. *Si* M *es una superficie de Riemann compacta,* $f : M \to \mathbb{C}$ *meromorfa y no idénticamente nula, entonces*

$$\sum_{p\in M} v_p(f) = 0$$

donde

$$v_p(f) = \begin{cases} k & si\ p\ \ es\ cero\ de\ orden\ k\ de\ f \\ -k & si\ p\ \ es\ polo\ de\ orden\ k\ de\ f \\ 0 & si\ f(p) \neq 0\,, \infty \end{cases}$$

La suma de la tesis del teorema es finita por la compacidad de M.

Proposición 9.2.2. *Sea F la región definida en la Fig. 9.1.*

(a) Todo punto del semiplano superior H se mapea sobre $\boldsymbol{F}$, por algún elemento de $SL_2(\mathbb{Z})\backslash\{\pm I\}$, donde $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(b) Los únicos puntos congruentes, por la acción de Γ son los $z \leftrightarrow z+1$ pertenecientes a los lados verticales y los $z \leftrightarrow -\dfrac{1}{z}$ del arco circular de $\boldsymbol{F}$.

(c) Los únicos puntos fijos de $\boldsymbol{F}$ para $\gamma \neq 1$ son
para el subgrupo $\{1, S\}$ la unidad imaginaria i
para el subgrupo $\{1,\ ST,\ (ST)^2\}$ el número complejo $\rho = e^{2\pi i/3}$
para el subgrupo $\{1,\ TS,\ (TS)^2\}$ el número complejo $\rho' = -\overline{\rho} = e^{\pi i/3}$

donde $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ son elementos de Γ.

Teorema 9.2.3. *Si $f(z)$ es una función modular de peso $2k$, no idénticamente nula, entonces*

$$v_\infty(f) + \sum_{p \in H/\Gamma} \frac{v_p(f)}{e_p} = \frac{k}{6}$$

donde $e_p = \sharp\Gamma_p\,, \quad \Gamma_p = \{\gamma\ \in \Gamma : \gamma\, p = p\}$

Un enunciado equivalente de la tesis del teorema, para f función modular de peso $2k$, no identicamente nula es:

$$v_\infty(f) + \frac{v_\rho(f)}{3} + \frac{v_i(f)}{2} + \sum_{p \neq i,\,\rho} v_p(f) = \frac{k}{6} \tag{9.11}$$

Demostración. En primer lugar f tiene un número finito de ceros y de polos $(mod\,\Gamma)$.

Como la función $\tilde{f}$, definida en la ec. (9.3), es meromorfa en 0 entonces $\exists\, r > 0$ tal que $\tilde{f}$ no tiene ceros ni polos en $D^x(0\,,\, r)$, luego f no tiene ningún cero ni polo para $|q| < r$, es decir para $Im(z) > \dfrac{\ln r}{2\pi}$.

Sea $\overline{F_r} = \left\{ z \in \overline{F}\ : Im(z) \leq \dfrac{\ln r}{2\pi} \right\}$, por compacidad y ya que f es meromorfa en H, tiene un número finito de ceros y polos en $\overline{F_r}$.

Se elige como dominio la región fundamental truncada D_r, con r como antes y se integra

$$\frac{1}{2\pi i}\frac{df}{f}$$

Se supone que f no tiene ceros ni polos en la frontera de D_r, excepto tal vez en $z = \rho, -\overline{\rho}, i$. Se modifica ∂D_r cerca de $\rho, -\overline{\rho}, i$ por medio de un arco de círculo como en la Fig.9.2. Existe un contorno ξ en cuyo interior hay un representante de cada cero o polo de f no congruente a $\rho, -\overline{\rho}$, ni a i.

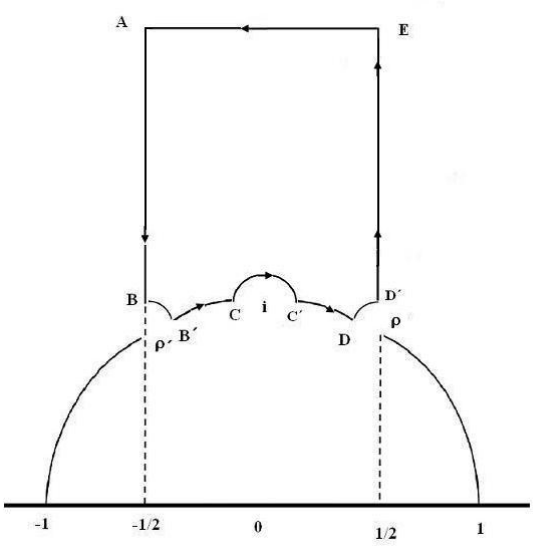


Figura 9.2: Región Fundamental truncada

Se aplica el teorema del residuo para calcular

$$\frac{1}{2\pi i}\int_{\xi}\frac{f'(z)}{f(z)}\,dz =$$

Como

$$v_p(f) = \begin{cases} k & \text{si } p \text{ es cero de orden } k \\ -k & \text{si } p \text{ es polo de orden } k \end{cases}$$

es claro que

$$v_p(f) = Res_{z=p}\frac{f'(z)}{f(z)}$$

Luego

$$\frac{1}{2\pi i}\int_{\xi}\frac{f'(z)}{f(z)}\,dz = \sum_{p\in\mathring{\xi}\subset H} v_p(f)$$

donde p es cero o polo de f en D_r.
En los puntos de la frontera de $\mathbf{F}$, donde $v_p(f)\neq 0$ se marca un semicírculo y se elige puntos A, E tal que $Im(A) = Im(E)$, suficientemente grande de modo que no haya polos ni ceros con $Im(z) > Im(A)$ y $|z| \leq \frac{1}{2}$.

Se calcula la integral del primer miembro, a trozos: primero a lo largo del segmento orientado de E hacia A:

$$\frac{1}{2\pi i}\int_{\overrightarrow{EA}}\frac{f'(z)\,dz}{f(z)} = \frac{1}{2\pi i}\int_{u=r\,e^{2\pi it}}\frac{\tilde{f}'(u)\,du}{\tilde{f}(u)}$$

donde $-\frac{1}{2} \leq t \leq \frac{1}{2}$, $r = e^{-2\pi Im(A)}$, el cambio de variables $q = e^{2\pi iz}$ transforma al segmento $\overline{EA}$ en el círculo $u = r\,e^{2\pi it}$, centrado en 0 y orientado en sentido negativo.

Por lo tanto se encuentra:

$$\frac{1}{2\pi i}\int_{\overrightarrow{EA}} \frac{f'(z)\,dz}{f(z)} = -v_0(\tilde{f}) = -v_\infty(f) \tag{9.12}$$

Ahora se calcula

$$\frac{1}{2\pi i}\int_{\widehat{BB'}} \frac{f'(z)\,dz}{f(z)} =$$

donde $\widehat{BB'}$ es el arco de círculo $\rho' + r\,e^{it}$; $\quad \rho' = -\overline{\rho}$; $\quad \alpha_r \leq t \leq \dfrac{\pi}{2}$ y luego se hace tender r a cero.
Se observa que $v_{\rho'}(f) = v_\rho(f)$, pues $\rho' = S\rho$ y por ello

$$f(z) = (z-\rho)^{v_\rho(f)}\, g(z) \quad ; \qquad g(\rho') \neq 0$$

se deriva

$$f'(z) = v_\rho(f)\,(z-\rho)^{v_\rho(f)-1}\, g(z) + (z-\rho)^{v_\rho(f)}\, g'(z)$$

y se obtiene

$$\frac{f'(z)}{f(z)} = \frac{v_\rho(f)}{z-\rho} + \frac{g'(z)}{g(z)}$$

como $g(\rho') \neq 0$, la función $\dfrac{g'}{g}$ es analítica cerca de ρ', luego si se considera que $r \to 0$,

$$\int_{\widehat{BB'}} \frac{g'}{g} \to 0$$

ya que la longitud del arco $\widehat{BB'}$ tiende a cero cuando $r \to 0$.
Además, $z = \rho' + r\,e^{it}$ donde $\alpha_r \leq t \leq \dfrac{\pi}{2}$, luego la integral

$$\frac{1}{2\pi i}\int_{\widehat{B'B}} \frac{dz}{z-\rho'} = \frac{1}{2\pi}\int_{\alpha_r}^{\frac{\pi}{2}} dt = \frac{1}{2\pi}\left(\frac{\pi}{2} - \alpha_r\right) \to \frac{1}{2\pi}\,\frac{\pi}{3}$$

cuando r tiende a cero. Por lo tanto, si el recorrido se realiza en sentido negativo

$$\lim_{r\to 0} \frac{1}{2\pi i}\int_{\widehat{BB'}} \frac{f'(z)\,dz}{f(z)} = -\frac{v_\rho(f)}{6} \tag{9.13}$$

Si se trabaja de manera análoga se obtiene

$$\lim_{r\to 0} \frac{1}{2\pi i}\int_{\widehat{DD'}} \frac{f'(z)\,dz}{f(z)} = -\frac{v_\rho(f)}{6} \tag{9.14}$$

y

$$\lim_{r\to 0} \frac{1}{2\pi i}\int_{\widehat{CC'}} \frac{f'(z)\,dz}{f(z)} = -\frac{v_i(f)}{2} \tag{9.15}$$

Falta calcular

$$\int_{\widehat{B'C}} \frac{f'(z)\,dz}{f(z)} + \int_{\widehat{C'D}} \frac{f'(z)\,dz}{f(z)} =$$

cuando r tiende a cero.
Los arcos $\widehat{B'C}$ y $\widehat{C'D}$ se corresponden por la función $S(z) = -\dfrac{1}{z}$ pero recorridos en sentidos opuestos. S transforma al arco $\widehat{B'C}$ sobre $\widehat{DC'}$ y como $f(S(z)) = z^{2k}\, f(z)$, se tiene

$$f'(S(z))\,\frac{1}{z^2} = 2kz^{2k-1}\, f(z) + z^{2k}\, f'(z)$$

luego

$$\frac{[f(S(z))]'}{f(S(z))} = \frac{2k}{z} + \frac{f'(z)}{f(z)}$$

por lo tanto

$$\begin{aligned}
\int_{\widehat{C'D}} \frac{f'(z)\,dz}{f(z)} &= \int_{S\circ\xi} \frac{f'(z)\,dz}{f(z)} \\
&= \int_\alpha^\beta \frac{f'(S(\xi(t)))\,\xi'(t)}{f(S(\xi(t)))\,\xi^2(t)}\,dt \\
&= \int_\alpha^\beta \frac{f'(\xi(t))\,\xi'(t)}{f(\xi(t))}\,dt + \int_\alpha^\beta 2k\frac{\xi'(t)}{\xi(t)}\,dt \\
&= -\int_{\widehat{B'C}} \frac{f'(z)\,dz}{f(z)} + 2ki(\beta-\alpha)
\end{aligned}$$

luego,

$$\lim_{r\to 0} \frac{1}{2\pi i}\left(\int_{\widehat{B'C}} \frac{f'(z)\,dz}{f(z)} + \int_{\widehat{C'D}} \frac{f'(z)\,dz}{f(z)}\right) = \frac{k}{\pi}(\beta-\alpha) = \frac{k}{6} \tag{9.16}$$

esto se obtiene al considerar que el ángulo que forman los vectores posición de ρ' e i es $\dfrac{\pi}{6}$.
El gráfico, Fig.9.3, aclara estos cálculos.

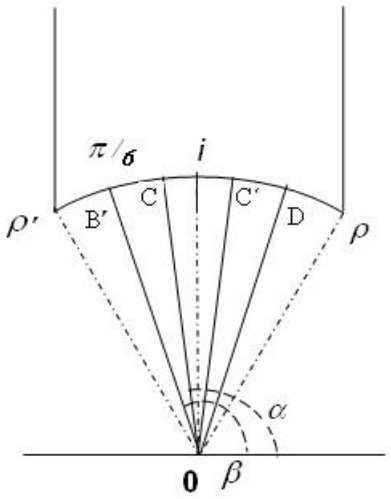


Figura 9.3: Ángulos correspondientes

$T(z) = z + 1$ transforma el segmento $\overline{AB}$ en el $\overline{ED'}$ y como $f(T(z)) = 1^{2k} f(z)$, se tiene que

$$\frac{1}{2\pi i}\int_A^B \frac{df}{f} + \frac{1}{2\pi i}\int_{D'}^E \frac{df}{f} = 0$$

Por lo tanto, al sumar los resultados de cada integral se tiene la expresión del teorema, siempre que no haya ceros ni polos en ∂D_r.

Si f tuviera ceros y polos en la frontera, el contorno se modifica con un semicírculo en cada polo o cero como se muestra en la Fig.9.4 y las integrales correspondientes se cancelan entre sí, cuando los puntos se encuentran sobre las verticales. Cuando los puntos pertenecen al arco que contiene a ρ', i, ρ, los valores que se obtienen respecto de p y de $S(p)$ son ambos, iguales a $-\frac{1}{2}v_p(f)$, aportando $-v_p(f)$ a la suma total. □

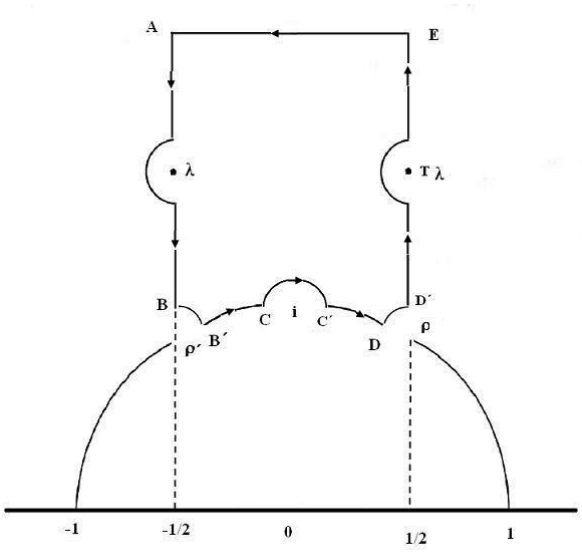


Figura 9.4: Región con ceros y/o polos en la frontera

9.2.2. El álgebra de las formas modulares

Sea k un número entero, se denota con

- $\mathbf{M}_{2k}$ al $\mathbb{C}$-espacio vectorial de formas modulares de peso $2k$.
- $\mathbf{S}_{2k}$ al $\mathbb{C}$-espacio vectorial de formas modulares cuspidales de peso $2k$.

Se consideran sólo subíndices pares porque para los impares, el espacio es $\{\theta\}$ ya que

$$f(z) = f\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} z\right] = (-1)^k f(z)\,, \qquad \forall\, z \in H$$

Para $k \geq 2$, el espacio $\mathbf{S}_{2k}$ es el núcleo de las formas lineales $(f \mapsto f(\infty))$ de $\mathbf{M}_{2k}$ en $\mathbb{C}^*$. Luego la $\dim(\mathbf{M}_{2k}/\mathbf{S}_{2k}) \leq 1$.

Al analizar las series de Eisenstein como ejemplo particular de formas modulares, se probó que para $k \geq 2\,, \quad G_{2k}(z) \in \mathbf{M}_{2k} \setminus \mathbf{S}_{2k}$.
Por lo tanto se tiene

$$\mathbf{M}_{2k} = \mathbf{S}_{2k} \oplus \mathbb{C}G_{2k}\,, \qquad \forall\, k \geq 2$$

Teorema 9.2.4. *Sea $\boldsymbol{M}_{2k}$ el espacio de las formas modulares de peso $2k$*

(i) *Si $k < 0$ ó $k = 1$ entonces $\boldsymbol{M}_{2k} = 0$*

(ii) *Si $k = 0,\, 2,\, 3,\, 4,\, 5$, entonces $\boldsymbol{M}_{2k} = \mathbb{C}G_{2k}$, es un espacio vectorial de dimensión 1 y $\boldsymbol{S}_{2k} = 0$*

(iii) *Si $k \geq 6\,, \quad f \mapsto \Delta f$ define un isomorfismo de $\boldsymbol{M}_{2k-12} \to \boldsymbol{S}_{2k}\,$, donde $\Delta := g_2^3 - 27\, g_3^2$*
Si $k = 6 \qquad \boldsymbol{M}_{12} = \mathbb{C}G_{12} \oplus \mathbb{C}\Delta$

Demostración. Se aplica la expresión (9.11) a $f \in \mathbf{M}_{2k}$, no idénticamente nula.

$$v_\infty(f) + \frac{v_\rho(f)}{3} + \frac{v_i(f)}{2} + \sum_{p \neq i,\, \rho} v_p(f) = \frac{k}{6}$$

Se supone que $\mathbf{M}_{2k} \neq 0$, luego todos los sumandos de la izquierda de la ecuación deben ser mayores o iguales que cero, esto ocurre porque $f \neq 0$ es forma modular, por lo tanto no tiene polos, luego $k \geq 0$. Además $k \neq 1$ ya que $\frac{1}{6}$ no puede ser escrito como $n + \frac{n'}{2} + \frac{n''}{3}$, con $n\,,\, n'\,,\, n'' \in \mathbb{N}_0$. Luego se probó *(i)*.

Si $k = 2,\, 3,\, 4,\, 5$, el lado derecho de la ecuación (9.11) es positivo y menor que 1, luego $v_\infty(f) = 0$ y por lo tanto $f(\infty) \neq 0$.

En cada caso, la ecuación (9.11) tiene una única solución posible:
Para $k = 2$, se encuentra

$\frac{1}{3}v_\rho(f) + \frac{1}{2}v_i(f) + \sum_{p \neq i,\, \rho} v_p(f) = \frac{2}{6}$ cuya única solución es $v_\rho(f) = 1$ y $\forall\, p \neq \rho\,, \quad v_p(f) = 0$

Para $k = 3$, se obtiene $v_i(f) = 1 \quad$ y $\forall\, p \neq i\,, \quad v_p(f) = 0$
Para $k = 4$, se obtiene $v_\rho(f) = 2 \quad$ y $\forall\, p \neq \rho\,, \quad v_p(f) = 0$
Para $k = 5$, se obtiene $v_\rho(f) = 1,\, v_i(f) = 1 \quad$ y $\forall\, p \neq \rho\,,\, i\,, \quad v_p(f) = 0$

Las formas modulares no cuspidales con estas propiedades son G_4, G_6, G_8, G_{10} . Esto es

- $v_\rho(G_4) = 1, \quad v_p(G_4) = 0, \quad \forall\, p \neq \rho\, (mod\, G)$. Luego G_4 genera el subespacio de las formas modulares con esta propiedad. $\mathbf{M}_4 = \mathbb{C}\, G_4$
- $v_i(G_6) = 1, \quad v_p(G_6) = 0, \quad \forall\, p \neq i\, (mod\, G)$. Luego $\mathbf{M}_6 = \mathbb{C}\, G_6$
- $v_\rho(G_8) = 2, \quad v_p(G_8) = 0, \quad \forall\, p \neq \rho\, (mod\, G)$. Luego $\mathbf{M}_8 = \mathbb{C}\, (G_4)^2$
- $v_\rho(G_{10}) = 1, \quad v_i(G_{10}) = 1, \quad v_p(G_{10}) = 0, \quad \forall\, p \neq \rho\, (mod\, G)$.
  Luego $\mathbf{M}_{10} = \mathbb{C}\, G_4\, G_6$

Y como $\mathbf{S}_{2k} = 0$ en estos casos, la afirmación $\mathbf{M}_{2k} = \mathbb{C}G_{2k}$ es clara.

Si $k = 6$, el segundo miembro de la ec.(9.11) es 1 y se puede obtener de tres maneras diferentes:

- $1 = 1$, en este caso $f(z)$ tiene sólo un cero en $z = \infty$. Esto se verifica para la función Δ ó $\mathbb{C}\,\Delta$. En particular $\Delta(z) \neq 0$, $\forall\, z \in H$ y tiene un cero simple en ∞.
  Es decir que $v_\infty(\Delta) = 1$ y $\forall p \in H$, $v_p(\Delta) = 0$.
- $2\,\frac{1}{2} = 1$, en este caso $f(i) = 0$ es solución doble y $f(z) \neq 0$ para todo otro punto. Esto se verifica para la función $(G_6)^2$
- $3\,\frac{1}{3} = 1$ en este caso $f(\rho) = 0$ es solución triple y $f(z) \neq 0$, para todo otro punto. Esto se verifica para la función $(G_4)^3$

Si $k \geq 6$, $\quad f \mapsto \Delta f$ define una función uno a uno de $\mathbf{M}_{2k-12} \to \mathbf{S}_{2k}$
Sea $g \in \mathbf{S}_{2k}$, luego $f(z) = \dfrac{g(z)}{\Delta(z)}$ resulta una función analítica en todas partes, pues Δ tiene sólo un cero simple en ∞, entonces $f \in \mathbf{M}_{2k-12}$ y $\Delta\, f = g$. Luego $f \mapsto \Delta f$ es un isomorfismo, demostrando *(iii)*.

Finalmente si $k < 6$, se tiene que $k - 6 < 0$ y $\mathbf{S}_{2k} = 0$, por *(i)* y *(iii)*; luego $\dim \mathbf{M}_{2k} \leq 1$ y ya que G_4, G_6, G_8, G_{10} son elementos no nulos que generan $\mathbf{M}_{2k}$ para $k = 2, 3, 4, 5$ respectivamente y $M_0 = \mathbb{C}$, se tiene que la $\dim \mathbf{M}_{2k} = 1$ para $k = 0, 2, 3, 4, 5$. Se completa así la prueba de *(ii)* y la demostración del teorema. □

Corolario. *Se deduce que:*

- Δ *tiene sólo un cero simple en* ∞ *y* $\Delta(z) \neq 0, \forall\, z \in H$
- G_4 *sólo tiene un cero simple en* $z = \rho$ *y* $\quad G_4(z) \neq 0 \quad \forall\, z \in (H \setminus \{\rho\}) \cup \{\infty\}$
- G_6 *sólo tiene un cero simple en* $z = i$ *y* $\quad G_6(z) \neq 0 \quad \forall\, z \in (H \setminus \{i\}) \cup \{\infty\}$
- $G_8 = \mathbb{C}(G_4)^2$ *sólo tiene un cero doble en* $z = \rho$ *y* $\quad G_8(z) \neq 0 \quad \forall\, z \in (H \setminus \{\rho\}) \cup \{\infty\}$
- $G_{10} = \mathbb{C}\,G_4\,G_6$ *sólo tiene dos ceros simples en* $z = \rho$, $z = i$
  y $G_{10}(z) \neq 0 \quad \forall\, z \in (H \setminus \{\rho, i\}) \cup \{\infty\}$

Teorema 9.2.5. *Sea* $\boldsymbol{M}_{2k}$ *el espacio de las formas modulares de peso* $2k$

(1)

$$\dim \boldsymbol{M}_{2k} = \begin{cases} \left[\frac{k}{6}\right] & si \quad k \equiv 1 (mod\, 6) \quad k \geq 0 \\ \left[\frac{k}{6}\right] + 1 & si \quad k \neq 1 (mod\, 6) \quad k \geq 0 \end{cases} \tag{9.17}$$

(2) $\boldsymbol{M}_{2k} \simeq \mathbb{C}\,[G_4\,,\, G_6]$, *anillo de polinomios en* G_4 *y* G_6.

Demostración. La expresión (9.17) es verdadera para $k \leq 6$, por $(i), (ii)$ del teorema anterior y ambos miembros aumentan 1 al cambiar k por $k+6$ por (iii) del teorema anterior. Luego se probó *(1)*

Se afirma que $G_4^\alpha\, G_6^\beta$ *generan* $\mathbf{M}_{2k}$ con $2\alpha + 3\beta = k\,;\ \alpha,\ \beta \in \mathbb{N}_0$.
En la demostración del teorema anterior se probó que esto es cierto para $k = 2,\ 3,\ 4,\ 5$ y también para $k = 1$, ya que $\mathbf{M}_2 = 0$. Además

$$\mathbf{M}_{2k} = \mathbb{C}\, G_{2k} + \mathbf{S}_{2k}$$

$$\mathbf{S}_{2k} = \Delta\, \mathbf{M}_{2k-12}\ , \quad k > 6$$

Se sabe que $G_{2k}(\infty) \neq 0$ y $\exists\, \alpha,\ \beta :\quad 2\alpha + 3\beta = k$ con $\alpha,\ \beta \geq 0$, luego

$$\exists\, c \in \mathbb{C} \,:\, G_{2k} = c\, G_4^\alpha\, G_6^\beta + f\,, \quad f \in \mathbf{S}_{2k}\,.$$

Se trata de ver que $\mathbf{S}_{2k}$ está generado por $\{G_4^\alpha\, G_6^\beta \,:\, \alpha,\ \beta \in \mathbb{N}_0\,,\ 2\alpha + 3\beta = k\}$. Esto se prueba por inducción.

Vale para $k \leq 6$ y vale para $\mathbf{M}_{2k-12}$, luego también vale para el producto $\Delta\, \mathbf{M}_{2k-12}$, ya que Δ es combinación lineal de G_4^3 y G_6^2.

Primero se prueba la independencia lineal, para ello se parte de $0 \equiv \sum_{\alpha,\beta} c_{\alpha\,\beta}\, G_4^\alpha\, G_6^\beta$, entonces para cada k fijo:

$$\sum_{2\alpha+3\beta=k} c_{\alpha\,\beta}\, G_4^\alpha\, G_6^\beta \equiv 0$$

Si se evalúa en i se obtiene $c_{\alpha\,0} = 0$, ya que $G_6(i) = 0$ y sólo queda $\sum c_{\alpha\,0}\, G_4^{\frac{k}{2}}\,(i) \equiv 0$, pero $G_4(i) \neq 0$. Si en todos los sumandos aparece el factor G_4, se lo simplifica y se baja el exponente de k a $k-2$, es decir hay una combinación lineal nula de $G_4^{\alpha'}\, G_6^{\beta'}$, con $2\alpha' + 3\beta' = k-2$, por lo tanto los coeficientes son 0, por hipótesis inductiva.

Luego se observa que para $k = 2,\ 3,\ 4,\ 5$ sólo se tiene G_4 , G_6, G_4^2 , $G_4\, G_6$ que generan $\mathbf{M}_4$, $\mathbf{M}_6$, $\mathbf{M}_8$, $\mathbf{M}_{10}$. Y para $k \geq 6$ se utiliza el procedimiento anterior, es decir: para $k = 6$ se baja a $k-2$ y así sucesivamente. □

9.3. Invariante modular

Sea Ω un lattice de $\mathbb{C}$ y sean

$$\Delta = g_2^3 - 27 g_3^2\,; \quad g_2 = 60 G_4\,; \quad g_3 = 140 G_6\,; \quad G_{2k}(\Omega) = \sum_{\omega\in\Omega}{}' \frac{1}{\omega^{2k}}; \quad k \geq 2$$

definidos en la sección 4. Además, por la Proposición 9.1.1, vale que

$$G_{2k}\,(\mu\,\Omega) = \mu^{-2k}\, G_{2k}\,(\Omega)\ , \quad \forall\, \mu \in \mathbb{C} \setminus \{0\}$$

Proposición 9.3.1. *Sea* $j := 1728\,\dfrac{g_2^3}{\Delta}$

(a) La función j es una función modular de peso 0.

(b) La función j es holomorfa en el semiplano superior H y tiene un polo simple en el ∞.

(c) La función j induce una biyección de H/Γ sobre $\mathbb{C}$

Demostración. La función $j(z)$ es analítica en H, por ser cociente de funciones analíticas con $\Delta(z) \neq 0 \quad \forall\, z \in H$, además tiene un polo simple en ∞ ya que $\Delta(z)$ tiene cero simple en ∞ y $G_4(\infty) \neq 0$. Luego se probó *(b)*

La función $j(z)$ es cociente de formas de peso 12, luego es función modular de peso 0. Es decir *j es invariante respecto de la acción de* Γ. Se probó *(a)*.

Se considera la función $j(z) - \alpha, \quad \alpha \in \mathbb{C}$.
Si $\alpha \neq 0$, se tiene entonces una función modular de peso 0 y para ella, la ecuación (9.11), cuando $k = 6$, determina dos soluciones posibles:

- $-1 + 2 \cdot \dfrac{1}{2} = 0$ para $\alpha = j(i) \neq 0$,
- $-1 + 1 = 0$ para $\alpha = j(z); \quad \forall\, z \neq \rho, i$.

Si $\alpha = 0$, como ρ es el único cero de g_2 y no anula a Δ, la función $j(z)$ tiene un único cero en ρ, con orden 3, luego la ecuación (9.11) se verifica para $-1+3.\dfrac{1}{3} = 0$ y no permite otros ceros.

Por lo tanto

$$j \ : H/\Gamma \to \mathbb{C}$$

es una biyección, exceptuando los puntos ρ, i ya que $j(\rho) = 0$ tiene multiplicidad 3 y $j(i) = c \neq 0$ tiene multiplicidad 2. □

Observación. .

- *Si se considera $H_0 = H \setminus \{j(\rho), j(i)\}$ se tiene un abierto y la función $j : H_0 \to \mathbb{C} \setminus \{0, j(i)\}$ resulta un cubrimiento usual.*
- *$\widehat{H/\Gamma} \approx \widehat{\mathbb{C}}$ y $\widehat{j} : \widehat{H/\Gamma} \to \widehat{\mathbb{C}}$ es un cubrimiento con puntos de ramificación en $[\rho], [i]$, con índices de ramificación 3 y 2 respectivamente.*

Proposición 9.3.2. *Sea f una función meromorfa en H. Las siguientes proposiciones son equivalentes*

(i) f es una función modular de peso 0.

(ii) f es cociente de dos formas modulares del mismo peso.

(iii) f es una función racional de j

Demostración. $(ii) \Rightarrow (i)$ es inmediata

$(iii) \Rightarrow (ii)$
Sea f es una función racional de j y sean p, q polinomios, de grado n y m respectivamente, luego $a_n \neq 0$, $b_m \neq 0$.

$$\begin{aligned}\frac{p(j)}{q(j)} &= \frac{p\left(1728\,\frac{g_2^3}{\Delta}\right)}{q\left(1728\,\frac{g_2^3}{\Delta}\right)} \\ &= \frac{a_n\alpha^n\left(\frac{g_2^3}{\Delta}\right)^n + \cdots + a_0}{b_m\alpha^m\left(\frac{g_2^3}{\Delta}\right)^m + \cdots + b_0} \quad , \quad \alpha = 1728 \\ &= \Delta^{m-n}\,\frac{a_n\,(g_2^3)^n + a_{n-1}(g_2^3)^{n-1}\,\Delta + \cdots + a_0\,\Delta^n}{b_m\,(g_2^3)^m + b_{m-1}(g_2^3)^{m-1}\,\Delta + \cdots + b_0\,\Delta^m}\end{aligned}$$

El numerador es producto de un polinomio homogéneo de peso $12n$ por la función Δ^{m-n}, de peso $12(m-n)$, si $m > n$. Resulta entonces que el numerador es una función de peso $12m$, el mismo peso del polinomio denominador. Además la composición de un polinomio y la función j es una foma modular, luego f es cociente de formas modulares de igual peso.
Si $m < n$, se analiza de manera similar, sólo que numerador y denominador tienen peso $12n$ y de nuevo f es cociente de formas modulares de igual peso.
Para el caso $m = n$, la conclusión es inmediata.
$(i) \Rightarrow (iii)$
Sea f una función modular de peso 0, $\exists p$, un polinomio conveniente tal que el producto $p(j(z))\,f(z)$ es una función holomorfa en H.
Como Δ se anula en el ∞ , $\exists\, k \in \mathbb{N}_0 : g = \Delta^k\,p(j)\,f$ es holomorfa en $H \cup \{\infty\}$. Y por el teorema anterior, la función g resulta una forma modular de peso $12k$.

Luego g es combinación lineal de $G_4^\alpha\,G_6^\beta$, con $2\alpha + 3\beta = 6k$. Por lo tanto

$$f = \frac{\sum_{\alpha,\beta} c_{\alpha\,\beta}\,G_4^\alpha\,G_6^\beta}{p(j)\,(g_2^3 - 27g_3^2)^k}$$

Por linealidad se reduce al estudio del caso $g = G_4^\alpha\,G_6^\beta$, es decir :

$$f = \frac{G_4^\alpha\,G_6^\beta}{(g_2^3 - 27g_3^2)^k}\ ,\ \text{con } 2\alpha + 3\beta = 6k$$

pero la relación $2\alpha + 3\beta = 6k$ muestra que, como α, β, k son enteros, $3|\alpha$ y $2|\beta$. Si $\alpha = 3s$, $\quad \beta = 2h$, $\qquad 6k = 6(s+h)$.
Se tiene que

$$f = \frac{G_4^\alpha\,G_6^\beta}{(g_2^3 - 27g_3^2)^{s+h}} = \frac{(G_4^3)^s}{\Delta^s}\,\frac{(G_6^2)^h}{\Delta^h}$$

si se observa que

$$\frac{27\,g_3^2}{\Delta} = \frac{g_2^3 - \Delta}{\Delta} = \frac{g_2^3}{\Delta} - 1$$

es obvio que

$$f = c\,j^s(j-1)^h$$

luego f es función racional de j □

Nota

1. Se ha probado que j determina un isomorfismo biholomorfo $\widehat{H/\Gamma} \longleftrightarrow \widehat{\mathbb{C}}$.
   donde $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ es S_2 la esfera de Riemann.
   Es posible definir una estructura natural sobre $\widehat{H/\Gamma} = \overline{H}/\Gamma$ es:

   $$\mathbf{M}(\widehat{H/\Gamma}) = \mathbb{C}(j) \simeq \mathbb{C}$$

   Como vale la propiedad de invarianza de j, es decir $j(\gamma z) = j(z)\ , \quad \forall z \in H\ ;\ \forall \gamma \in \Gamma$, para cada $c \in \mathbb{C}$, existe una única órbita de Γ en H tal que j toma el valor c.

   Ejemplos sencillos se encuentran al calcular los invariantes de los lattices $\Omega_1 = \langle 1, i\rangle$ y $\Omega_2 = \langle 1, \rho\rangle$, puesto que para Ω_1 se obtiene $G_6(i) = 0$, luego $j(i) = 1728$ y para Ω_2 , $G_4(\rho) = 0$, luego $j(\rho) = 0$.

2. El coeficiente $1728 = 2^6 3^3$ se introdujo para que la función j tenga residuo igual a 1 en el infinito. Luego su desarrollo de Fourier tiene la forma:

   $$j(z) = e^{-2\pi i z} + 744 + \sum_1^\infty c(n)\, e^{2\pi i n z}, \qquad z \in H$$

   donde los $c(n)$ son enteros muy interesantes en teoría de números.

9.4. Relación entre Curva elíptica no singular y lattice en $\mathbb{C}$

Se cuenta, a esta altura, con los conceptos necesarios para probar que **toda curva elíptica no singular proviene de un lattice en** $\mathbb{C}$.

Teorema 9.4.1. *Si* $c_2\,,\ c_3\ \in \mathbb{C}$, *tal que* $c_2^3 - 27\,c_3^2 \neq 0$, *entonces existe* Ω *lattice en* $\mathbb{C}$ *tal que* $c_2 = g_2\,(\Omega), \quad c_3 = g_3\,(\Omega)$.

Demostración. Primero se supone que $c_2 = 0$ entonces, por hipótesis $c_3 \neq 0$.
Para $\rho = e^{2\pi i/3}$ se sabe que $g_2(\rho) = 0$ y que $g_3(\rho) \neq 0$, además $g_2^3(\tau) - 27\,g_3^2(\tau) = \Delta(\tau)$ que no se anula para $\tau \in H$.

Por lo tanto se puede elegir $\mu \in \mathbb{C}^x$: $\mu^{-6}\, g_3(\rho) = c_3$. Luego existe un lattice Ω :

$$\begin{aligned}\Omega &= \mu\, \Omega\,(1, \rho) \\ &= \Omega\,(\mu, \mu\rho)\end{aligned}$$

Se tiene $g_2(\Omega) = \mu^{-4} g_2(\rho) = 0 = c_2$ y $g_3(\Omega) = \mu^{-6} g_3(\rho) = c_3 \neq 0$, como se requería.

Análogamente, si $c_3 = 0$ entonces $c_2 \neq 0$.
Se sabe que $g_3(i) = 0 \neq g_2(i)$. Luego se puede elegir $\mu \in \mathbb{C}^x$: $\mu^{-4}\, g_2(i) = c_2$.
Por lo tanto existe $\Omega = \Omega\,(\mu\,, \mu i)$ que satisface
$g_2(\Omega) = \mu^{-4} g_2(i) = c_2$ y $g_3(\Omega) = 0 = c_3$.

Finalmente se considera $c_2 \neq 0$ y $c_3 \neq 0$ luego existe, $\tau \in H$ tal que, por la propiedad de invarianza de la función j, para cada $c \in \mathbb{C}$ existe una única órbita de Γ en H tal que j toma el valor c. Se considera

$$j(\tau) = 1728\, \frac{c_2^3}{c_2^3 - 27\, c_3^2}$$

Luego $\forall\, \mu \in \mathbb{C}^x$ existe el lattice $\Omega = \Omega\,(\mu\,, \mu\tau)$ que satisface
$g_2(\Omega) = \mu^{-4} g_2(\tau) = c_2$, $g_3(\Omega) = \mu^{-6} g_3(\tau) = \pm c_3$ y $j(\Omega) = 1728\, \dfrac{g_2(\Omega)^3}{g_2^3(\Omega) - 27\, g_3^2(\Omega)} = j(\tau)$.
Si $g_3(\Omega) = c_3$ la conclusión es inmediata.
Si $g_3(\Omega) = -c_3$ se cambia Ω por $i\Omega$ ya que $g_2(i\Omega) = i^{-4}\, g_2(\Omega) = g_2(\Omega) = c_2$,
$g_3(i\Omega) = i^{-6} g_3(\Omega) = -g_3(\Omega) = c_3$ □

Corolario. *Dada una curva elíptica no singular*

$$y^2 = 4\, x^3 - c_2\, x - c_3\,, \qquad c_2\,, c_3 \in \mathbb{C} \qquad {c_2}^3 - 27\, {c_3}^2 \neq 0 \tag{9.18}$$

existe Ω lattice de $\mathbb{C}$ tal que $c_2 = g_2(\Omega)$, $c_3 = g_3(\Omega)$.

En consecuencia $(\wp_\Omega(z)\,,\, \wp'_\Omega(z))$ parametriza la curva no singular dada, para $z \in \mathbb{C}$.

Existe una biyección entre toros complejos $\mathbb{C}/\Omega$ y curvas elípticas no singulares, es decir que verifican (9.18). Luego, toda curva elíptica E se puede parametrizar(uniformizar) con dos funciones elípticas sobre un lattice apropiado.

Observación. .

(a) Se recuerda que:

- *Una curva* $y^2 = a\,x^3 + b\,x^2 + c\,x + d\,, \quad a \neq 0$ *se dice no singular si el polinomio cúbico del segundo miembro tiene todas sus raíces distintas.*

- *Toda curva elíptica no singular se puede expresar en la forma:*

$$y^2 = 4\,(x-a)\,(x-b)\,(x-c) \quad con \quad a\,,\,b\,,\,c \in \mathbb{C} \text{ distintos}$$

Y si se exige que $a+b+c=0$*, mediante un cambio de variables conveniente, la ecuación se expresa en la forma* $y^2 = c\,(x^3 + p\,x + q\,)$*.*

- *La curva* $y^2 = x^3 + p\,x + q\,$*, es no singular si y sólo si* $4\,p^3 + 27\,q^2 \neq 0$*.*
Si la curva es $y^2 = 4\,x^3 - c_2\,x - c_3$ *equivale a exigir que el polinomio*

$$x^3 - \frac{c_2}{4}\,x - \frac{c_3}{4}$$

sea no singular, luego se verifica que:

$$4\,\big(-\frac{c_2}{4}\big)^3 + 27\big(\frac{c_3}{4}\big)^2 \neq 0$$

y por lo tanto

$$\frac{-1}{4^2}(c_2^3 - 27\,c_3^2) \neq 0$$

(b) En la demostración de la ecuación diferencial para $\wp$*, respecto del lattice* Ω*, se encontró que*

$$(\wp')^2 = 4\,\wp^3 - g_2\,\wp - g_3\,, \quad \text{donde } \wp\ ,\ \wp'\ ,\ g_2 \text{ y } g_3 \text{ dependen de } \Omega$$

que se anula para $\frac{\omega_1}{2}\,,\,\frac{\omega_2}{2}\,,\,\frac{\omega_1+\omega_2}{2}$*, todos distintos. Luego la curva*

$$y^2 = 4\,x^3 - g_2(\Omega)\,x - g_3(\Omega)$$

es no singular, lo que implica que $g_2^3 - 27\,g_3^2 \neq 0 \quad \forall\,\Omega$*.*

(c) Para las curvas elípticas no singulares, los coeficientes $g_2\,,\,g_3$ *son invariantes y se determinan por medio de las series de Eisenstein de peso* 4 *y* 6 *respectivamente.*

9.5. Desarrollos de G_{2k} en el infinito

Se sabe que

$$\pi \operatorname{cotg} \pi z = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) \tag{9.19}$$

converge uniformemente sobre compactos en $\mathbb{C} \setminus \mathbb{Z}$.

Si $z \in H$, entonces $|e^{2\pi i z}| < 1$, se puede escribir

$$\begin{aligned} \pi \operatorname{cotg} \pi z &= \pi \frac{\cos \pi z}{\operatorname{sen} \pi z} \\ &= i\pi \frac{e^{2\pi i z} + 1}{e^{2\pi i z} - 1} \\ &= i\pi \frac{q+1}{q-1} \qquad \textit{donde } q = e^{2\pi i z} \\ &= i\pi - 2i\pi \frac{1}{1-q} \end{aligned}$$

$$\pi \operatorname{cotg} \pi z = i\pi - 2i\pi \sum_{d=0}^{\infty} q^d \,, \qquad |q| < 1 \tag{9.20}$$

De (9.19) y (9.20) se encuentra

$$\sum_{m=-\infty}^{\infty} \frac{1}{z+m} = i\pi - 2i\pi \sum_{d=0}^{\infty} q^d \,, \qquad |q| < 1 \,;\, q = e^{2\pi i z}$$

Se deriva término a término $2k-1$ veces y se obtiene

$$\sum_{m=-\infty}^{\infty} \frac{(-1)^{2k-1} 1 \cdot 2 \cdots (2k-1)}{(z+m)^{2k}} = -(2i\pi)^{2k} \sum_{d=1}^{\infty} d^{2k-1} q^d \quad , \quad |q| < 1 \ , \ k \geq 2$$

luego

$$\text{Si } k \geq 2 \ , \ \sum_{m=-\infty}^{\infty} \frac{1}{(z+m)^{2k}} = \frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{d=1}^{\infty} d^{2k-1} e^{2\pi i z d} \,, \qquad z \in H \tag{9.21}$$

Proposición 9.5.1. *Para todo número entero $k \geq 2$ se tiene que:*

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n) \ e^{2\pi i n z} \tag{9.22}$$

donde $\sigma_h(n) = \sum_{d|n} d^h$ es la suma de las potencias h de los divisores positivos de n y la función zeta de Riemann $\zeta(k) = \sum_{m=1}^{\infty} \frac{1}{m^k}$

Demostración. Por definición,

$$\begin{aligned} G_{2k}(z) &= \sum_{(n,m)\neq(0,0)} \frac{1}{(nz+m)^{2k}} \quad \text{para } k \geq 2 \\ &= \sum_{m\neq 0} \frac{1}{m^{2k}} + \sum_{n\neq 0} \sum_{m=-\infty}^{\infty} \frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + 2\sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + 2\sum_{n=1}^{\infty} \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{d=1}^{\infty} d^{2k-1}\,(e^{2\pi i z})^{dn} \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{h=1}^{\infty}\sum_{d=1}^{\infty} d^{2k-1}\, e^{2\pi i z dh} \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)\, e^{2\pi i z n} \end{aligned}$$

Las tres últimas igualdades se obtienen al aplicar la ec (9.21) y la definición de $\sigma_h(n)$. □

Observación. .

1) Se suele normalizar las series de Eisenstein con la función:

$$E_{2k} = (2\zeta(2k))^{-1} G_{2k} \text{ donde } E_{2k}(\infty) = 1\,, \quad \forall\, k \geq 2$$

2) A partir de los números de Bernoulli $B_k \in \mathbb{Q}$, los cuales se definen por la serie

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}$$

se escribe la función $\zeta(2k) = \dfrac{2^{2k-1}}{(2k)!}\, B_k\, \pi^{2k}$

Si se utilizan los primeros *números de Bernoulli*:

$$B_1 = \frac{1}{6} \qquad B_2 = \frac{1}{30} \qquad B_3 = \frac{1}{42} \qquad B_4 = \frac{1}{30} \qquad B_5 = \frac{5}{66}$$

$$B_6 = \frac{691}{2730} \qquad B_7 = \frac{7}{6} \qquad B_8 = \frac{3617}{510} \qquad B_9 = \frac{43867}{798} \qquad B_{10} = \frac{283617}{330}$$

se encuentra para $\zeta(2k)$ que:

$$\zeta(2) = \frac{\pi^2}{2\cdot 3} \qquad \zeta(4) = \frac{\pi^4}{2\cdot 3^2\cdot 5} \qquad \zeta(6) = \frac{\pi^6}{3^3\cdot 5\cdot 7}$$

Corolario. *Para todo número entero $k \geq 2$ se tiene que:*

$$E_{2k}(z) = 1 + \gamma_{2k} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

donde

$$\gamma_{2k} = (-1)^k \frac{4k}{B_k}$$

Ejemplo: Sea $q = e^{2\pi i z}$, $z \in H$

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)\, q^n \quad , \qquad g_2 = 60 \cdot 2\zeta(4) \cdot E_4 = (2\pi)^4 \frac{1}{2^2 \,.\, 3} E_4$$

$$E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)\, q^n \quad , \qquad g_3 = 140 \cdot 2\zeta(6) \cdot E_6 = (2\pi)^6 \frac{1}{2^3 \,.\, 3^3} E_6$$

$$E_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n)\, q^n \quad , \qquad (480 = 2^5 \,.\, 3 \,.\, 5)$$

Se sabe que los espacios de las formas modulares de peso 8 y 10 tienen ambos, dimensión 1. Con estas normalizaciones se tiene que:

$$E_8 = E_4^2 \,, \qquad E_4 \cdot E_6 = E_{10}$$

lo que implica las identidades:

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{n=1}^{\infty} \sigma_3(m)\, \sigma_3(n-m)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{n=1}^{n-1} \sigma_3(n)\, \sigma_5(n-m)$$

Para pesos mayores es algo más complicado. Se tiene que E_{12} , E_6^2 y Δ son linealmente dependientes por ser elementos de M_{12} y ésta tiene dimensión 2.
Una posibilidad es por ejemplo:

$$E_6^2 = E_{12} + \lambda\, \Delta \,, \quad \lambda \in \mathbb{C}$$

En general, todo E_{2k} se puede expresar como un polinomio en E_4 y E_6 de la forma

$$E_{2k} = E_4^{\alpha}\, E_6^{\beta} + f \;\; con \;\; f \in \mathbf{S}_{2k} \,, k = 2\,\alpha + 3\,\beta$$

Las series de Eisenstein G_{2k} muestran que los coeficientes de Fourier de las formas modulares son funciones aritméticas importantes.

A. Aplicaciones en teoría de números

A.1. Estimaciones de los coeficientes de formas modulares

Sea f una forma modular de peso $2k$, $k \geq 2$, cuyo desarrollo es:

$$f(z) = \sum_{n=0}^{\infty} a_n \, (e^{2\pi i z})^n \,, \quad z \in H.$$

Es de interés estudiar **una acotación para los coeficientes de Fourier** a_n cuando $n \to \infty$

Teorema A.1.1. *Si $f = G_{2k}$, el orden de magnitud de a_n es n^{2k-1}. Más aún existen constantes A, $B > 0$ tales que*

$$An^{2k-1} \leq |a_n| \leq Bn^{2k-1}$$

Demostración. La Proposición (9.5.1), muestra que existe una constante $A > 0$ tal que:

$$a_n = (-1)^k A \, \sigma_{2k-1}(n)$$

entonces,

$$\begin{aligned} |a_n| &= A \, \sigma_{2k-1}(n) \\ &\geq A \, n^{2k-1}. \end{aligned}$$

Por otro lado,

$$\begin{aligned} \frac{|a_n|}{n^{2k-1}} &= A \sum_{d|n} \frac{1}{d^{2k-1}} \\ &\leq A \sum_{d=1}^{\infty} \frac{1}{d^{2k-1}} \\ &\leq A \, \zeta(2k-1) < \infty. \end{aligned}$$

Luego,

$$a_n = \mathbf{O}(n^{2k-1}).$$

□

Toda forma modular no cuspidal de peso $2k$, $k \geq 2$ tiene coeficientes de orden n^{2k-1}.

Teorema A.1.2. ***(Hecke)***

Si f es una forma cuspidal de peso $2k$, $k \geq 2$ entonces el cociente $\frac{|a_n|}{n^k}$ permanece acotado cuando $n \to \infty$, es decir el orden de magnitud de a_n es n^k.

Demostración. f es una forma cuspidal, se tiene entonces que $a_0 = 0$, luego

$$f(z) = a_1 e^{2\pi i z} + a_2 e^{2\pi i 2z} + \cdots ,$$

entonces,

$$|f(z)| = \boldsymbol{O}(e^{2\pi i z}) = \boldsymbol{O}(e^{-2\pi y}),$$

donde $y = Im(z) \to \infty$ cuando $q \to 0$.

Sea $\phi(z) = |f(z)|y^k$

$$\phi(\gamma z) = |cz + d|^{2k} \, |f(z)| \, y^k \, |cz + d|^{-2k} = \phi(z) \,, \quad \forall \, \gamma \in SL_2(\mathbb{Z})$$

con γ como en (9.2). Luego ϕ es invariante bajo la acción del grupo modular Γ.

La función ϕ es continua en la región fundamental F y en el semiplano superior H, además $\phi(z) \to 0$ cuando $y \to \infty$, para $y \in F$.

De esto surge que ϕ es acotada, es decir existe una constante positiva M tal que $|\phi(z)| \leq M \,, \quad \forall \, z \in H$, es decir

$$|f(z)| \leq M \, y^{-k} \,, \forall \, z = (x, y) \in H. \tag{A.1}$$

Dado z en la región fundamental, se fija la variable y y la variable x toma valores entre 0 y 1. Luego los puntos $q = e^{2\pi i(x+iy)}$ se mueven sobre el círculo C_y con centro en cero y radio y.

Por el teorema del residuo se tiene

$$a_n = \frac{1}{2\pi i} \int_{C_y} f(z) \, q^{-n-1} \, dq = \int_0^1 f(x + iy) \, e^{-2\pi i n(x+iy)} \, dx$$

y como se cumple (A.1), entonces $|a_n| \leq \frac{M}{2\pi} y^{-k} e^{2\pi n y} \,, \forall \, y > 0$.

Si se considera $y = \frac{1}{n} \Rightarrow |a_n| \leq e^{2\pi} M n^k$.

Luego

$$a_n = \mathbf{O}(n^k).$$

□

El gran matemático **Ramanujan** fue quien estudió los coeficientes del desarrollo de Fourier de la función discriminante $\Delta(z)$. Él denotó con $\tau(n)$ al n-ésimo coeficiente de la forma cuspidal:

$$F(z) = \frac{\Delta(z)}{(2\pi)^{12}} = \sum_{n\geq 1} \tau(n)\, e^{2\pi i n z}$$

llamada *función discriminante normalizada.*

Observación. *A la función $n \mapsto \tau(n)$ se la llama función de Ramanujan.*
Entre sus primeros valores se encuentran:

$$\tau(1) = 1 \qquad \tau(2) = -24 \qquad \tau(3) = 252$$
$$\tau(4) = -1472 \qquad \tau(5) = 4830$$

Alrededor de 1917 Ramanujan enunció dos conjeturas que se enuncian en la siguiente proposición.

Proposición A.1.3. .

(i) $\tau(m\,n) = \tau(m)\,\tau(n)$, *si* $(m\,,\,n) = 1$

(ii) $\tau(n) = \boldsymbol{O}(n^{\frac{11}{2}+\varepsilon}) \quad \forall\, \varepsilon > 0$

Al enunciado (i) lo demostró Mordell[7].

En 1970 Deligne[8] probó (ii), para toda forma cuspidal de peso k que verifique:

$$\begin{aligned} a_n &= \mathbf{O}(n^{k-\frac{1}{2}}\sigma_0(n)) \\ &= \mathbf{O}(n^{k-\frac{1}{2}+\varepsilon}) \quad \forall\, \varepsilon > 0. \end{aligned}$$

Aún continúa vigente la pregunta abierta de Lehmer:

$$\text{¿Es } \tau(n) \neq 0 \quad \forall\, n \geq 1\,?$$

Sólo se sabe que la respuesta es afirmativa para $n \leq 10^{15}$.

[7] L J Mordell (1888 – 1972) realizó importantes aportes al desarrollo de teoría de números y al Álgebra, especialmente por el teorema respecto de las curvas elípticas sobre los racionales (1922). Su extensión a grupos abelianos la enunció André Weil en 1928

[8] Pierre Deligne (nació en 1944) matemático belga conocido por sus importantísimos trabajos sobre las conjeturas de Weil, que demostró en 1973. Medalla Fields 1978 y Premio Abel 2013

.

B. Aplicaciones a Criptografía

La *criptografía* actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. Los avances que se han producido en el mundo de la criptografía, han sido posibles gracias a los grandes avances en el campo de la matemática y la informática.

La *Criptografía simétrica* agrupa las funcionalidades criptográficas que se apoyan en el uso de una sola clave y la *Criptografía de clave pública o Criptografía asimétrica* a protocolos criptográficos que utilizan parejas de claves, una clave pública que sirve para cifrar y una clave privada que sirve para descifrar.

B.1. Criptografía de clave pública

En criptografía de clave pública se hace uso de las funciones unidireccionales. Se trata de funciones matemáticas que resultan sencillas de calcular pero difíciles de invertir. Así, si $f(x)$ es una función unidireccional será rápido calcular la imagen, $f(x) = y$, pero computacionalmente imposible calcular su inversa, $f^{-1}(y) = x$.

La exponencial discreta es una de las funciones unidireccionales más utilizadas. Dado un grupo cíclico G de orden p y uno de sus elementos g, se define la operación exponencial $fg(x) = gx$ *para todo* x.

Existen algoritmos rápidos que pueden hacer este cálculo (dados g *y* x) en tiempos aceptables para grupos de orden p muy grande. Sin embargo, si disponemos del resultado $h = gx$ y la base g, los cálculos necesarios para obtener x requieren de un tiempo exponencial para ejecutarse y resulta imposible en grupos de orden suficientemente grande. Esta operación, $fg^{-1}(h) = x$ se conoce como *logaritmo discreto en base* g *de* h. La principal dificultad surge por la naturaleza cíclica de la operación definida en G y es el soporte de muchos algoritmos criptográficos que se usan hoy en día.

En 1985 Koblitz y Miller propusieron la utilización del grupo de puntos de una curva elíptica definida sobre un cuerpo finito como soporte para criptosistemas y así resolver el problema del logaritmo discreto.

B.2. Criptografía con Curvas Elípticas

La *teoría de curvas elípticas sobre cuerpos finitos* se utiliza en el campo de la criptografía con bastante éxito. Los avances en estos métodos y la utilización de la computadora, exigen números cada vez mas grandes a fin de garantizar la seguridad de los sistemas criptográficos y son los sistemas de cifrado con curvas elípticas los que solucionan el inconveniente, en parte, cuando se implementan procesos de generación y distribución de claves secretas.

La Criptografía de Curva Elíptica (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las curvas elípticas. Koblitz y Miller aseguran que la ECC puede usar claves más cortas, ser más rápida y proporcionar un nivel de seguridad equivalente al de los métodos tradicionales, RSA[9] o ELGamal[10], pero utilizando un número menor de dígitos. Se obtienen claves mas pequeñas, característica que resulta muy útil para la seguridad en aplicaciones basadas en circuitos integrados y tarjetas inteligentes.

Estas apreciaciones y los siguientes conceptos se basan en las notas y bibliografía consultada, ver [7] y [8].

B.2.1. El problema del logaritmo elíptico

Dado un punto P de una curva elíptica E, se quiere calcular $s \in \mathbb{Z}$ tal que $Q = sP$ sea otro punto de la curva E.
Es decir: si E es una curva elíptica sobre un cuerpo finito F_q con $q = pm$, p primo, $m \in \mathbb{N}$ y sea P un punto perteneciente a la curva E de orden n. Se quiere encontrar $s \in \mathbb{Z}$, cuando existe, tal que $Q = sP$, esto es lo que se conoce como *el problema del logaritmo elíptico en* E, respecto de la base P, dado $Q \in E$[11].

Son varios los algoritmos que se pueden utilizar para encontrar la respuesta a este problema.

El método Silverman proyecta r combinaciones lineales en el plano sobre el cuerpo $\mathbb{Q}$ de los racionales y se considera la curva $E(\mathbb{Q})$ que contiene r puntos. Si estos puntos fueran linealmente dependientes se soluciona el problema elíptico. Actualmente se usa este método con $r \leq 9$ pero la probabilidad de que los puntos sean linealmente dependientes es muy pequeña.

Para la **elección de la curva** se debe tener en cuenta los siguientes aspectos

El número r, de puntos de la curva, debe satisfacer las siguientes condiciones:

- ser divisible por un número primo suficientemente grande, $p > 2^{160}$,
- no ser múltiplo de p,
- no ser divisor de $p^{k-1},\ k \in \mathbb{N}$ pequeño,
- no ser igual a $1 (mód\ p)$.

[9] Algoritmo descripto por Rivest, Shamir y Adleman. 1977. Instituto Tecnológico de Massachusetts
[10] Esquema cifrado descripto por el egipcio Taher Elgamal. 1984.
[11] Generación de claves: sea el conjunto $E = \{P, 2P, 3P, ...\}$ de cardinal n. Se elige un valor entero s entre 1 y $n-1$ y se calcula sP. La clave pública es el par (P, sP) y la privada es s.

En cuanto a *cual curva elegir* se puede optar por alguna de las siguientes posibilidades:

- se considera una curva sobre F_2 y luego se la extiende a los racionales,
- se elige una curva sobre los racionales y se la reduce módulo un primo p, o
- de manera aleatoria sobre un cuerpo finito, pero tal que el discriminante de la ecuación cúbica que la define sea distinto de cero, ya que debe ser no singular.

La asignación de mensajes a puntos de la curva no es una tarea sencilla.
Uno de los problemas prácticos que se plantean al usar este tipo de criptografía es el de definir una correspondencia entre los mensajes que se quieren trasmitir y los puntos de la curva. Esto se puede hacer con una tabla o con curvas entrelazadas.

B.2.2. Propiedades

Los métodos que usan criptografía con curvas elípticas aseguran cuatro propiedades básicas de las comunicaciones:

Confidenciabilidad: Garantiza que la información está accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.

Integridad: Garantiza la corrección y completitud de la información. Para conseguirlo se utilizan funciones de dispersión unidireccional (hash).

Autenticidad: Proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.

No Repudio o vinculación: Proporciona protección respecto de alguna de las entidades implicadas en la comunicación, para que no se pueda negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo firma digital.

Como ejemplo, estos métodos permiten que cada usuario opere su cuenta bancaria desde casa sin miedo a que:
otros sujetos sepan el estado de sus cuentas (Confidencialidad),
otros sujetos modifiquen sus órdenes antes de que el banco las reciba (Integridad),
otros sujetos envíen órdenes en su nombre (Autenticidad).

Además el banco agradece que la criptografía le asegure que: El usuario no se retracte de ninguna órden emitida, alegando que fue otro quien se las envió (No Repudio).

Juan G. Tena de la Universidad de Valladolid, en su artículo 25 *años con criptografía de curvas elípticas*, publicado en 2014, reflexiona sobre los progresos realizados en criptografía con curvas elípticas. Asegura que estos métodos han transformado los esquemas de organizaciones y empresas que ya se benefician con el uso criptográfico de las curvas elípticas.

Menciona a la corporación Certicom (*http : //www.certicom.com*) como líder en este tema y afirma que dicha empresa logró realizar aportes importantes de criptografía con curvas elípticas a los estándares de clave pública existentes.

Afirma también que el American National Standards Institute ha sido desde 1999 una de las organizaciones de más peso en adoptar las curvas elípticas dentro de sus estándares de criptografía y asegura que los estándares de esta organización son referencia directa para servicios financieros y la industria en general.

Otra de las principales organizaciones en apostar por la criptografía con curvas elípticas a partir del año 2000 fue la Internacional Organization for Standarizatcion (ISO).

Actualmente se utilizan las nuevas tecnologías basadas en curvas elípticas para:

- Aplicaciones que requieren operaciones de clave pública de tipo intensivo. Por ejemplo, el comercio electrónico basado en Internet.
- Aplicaciones que requieren la utilización de canales con restricciones. Por ejemplo las redes.
- Aplicaciones que requieren el uso de tarjetas inteligentes. Por ejemplo, en 2001 Europay, Mastercard y Visa dieron a conocer un informe técnico sobre curvas elípticas, el EMV40. En él se introdujo el uso de curvas elípticas como sustituto del RSA.

Los autores consultados coinciden en establecer que el análisis de los protocolos criptográficos basados en curvas elípticas y sus aplicaciones resulta bastante interesante y ofrece ventajas incuestionables para la implementación de aplicaciones seguras.

Bibliografía

[1] Ahlfors, L. V. ***"Complex Analysis: an Introduction to the Theory of Analytic Functions of One Complex Variable"***. Capítulo 7 (2^a Edición) 1996. Mc Graw-Hill.

[2] Jones, G. A. and Singerman, D. ***"Complex Funtions an algebraic and geometric viewpoint"***. Capítulo 3: Elliptic functions; Capítulo 6: The modular group. Quinta Edición. 1997. Cambridge University Press.

[3] Serre, J.P. ***"A Course in Arithmetic"***. 1973. Springer-Verlag New York Inc.

[4] Knapp, A. W. ***"Elliptic curves"***. Capítulo VI: Complex Points. 1992. Princeton University Press, New Jersey.

[5] Markushevich, A. ***"Teoría de las Funciones Analíticas"*** **Tomo II**. Capítulo Séptimo: Funciones enteras y meromorfas. 1970. Editorial MIR. Moscú.

[6] Phillips, E. G. ***"Some Topics in Complex Analysis"***. Capítulo 1: Elliptic Functions. 1966. Pergamon Press Ltd. Oxford - London - Edinburgh - New York - Paris - Frankfurt.

[7] Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso. ***Çriptografía con curvas elípticas"***. $PID\_00200952$ Universitat Oberta de Catalunya.

[8] Washington, L. C. ***"Elliptic Curves, Number Theory and Cryptography"***. 2003 - CHAPMAN & HALL/CRC - United States of América.