Infinite Products and Number Theory [1]

Takashi Ichikawa [2]

Abstract

We shall review the following subjects:

- Basic theory of elliptic functions and modular forms;
- Relationship between infinite products and number theory;
- Processes of creation by great mathematicians.

Contents

[1] Available at http://ichikawa.ms.saga-u.ac.jp/

[2] Department of Mathematics, Graduate School of Science and Engineering, Saga University, Saga 840-8502, Japan
e-mail: ichikawn@cc.saga-u.ac.jp

§1. Introduction

1.1. Aim of this lecture. We explain a basic theory of elliptic functions and modular forms based on the infinite products by Euler and Jacobi:

- Euler: $\sin x = x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right)$.
- Euler's pentagonal number theorem:

$$\begin{aligned}\prod_{n=1}^{\infty}(1-q^n) &= \sum_{m=-\infty}^{\infty}(-1)^m q^{m(3m-1)/2} \\ &= 1 + \underbrace{(-q^1+q^5-q^{12}+\cdots)}_{m>0} + \underbrace{(-q^2+q^7-q^{15}+\cdots)}_{m<0} \\ &\quad (1,5,12,\ldots \text{ are pentagon numbers}).\end{aligned}$$

- Jacobi's triple product identity:

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}\zeta)(1+q^{2n-1}\zeta^{-1}) = \sum_{m=-\infty}^{\infty} q^{m^2}\zeta^m.$$

Further, we introduce a recent development called Borcherds products on this theory.

Contribution of elliptic functions and modular forms to number theory.

(1) **A theorem of Jacobi** (1804 – 1851) states that for any positive integer n,

$$\sharp\left\{(m_1,m_2,m_3,m_4)\in\mathbb{Z}^4 \;\middle|\; \sum_{i=1}^{4} m_i^2 = n\right\} = 8\sum_{0<d|n,4\nmid d} d,$$

where $\sharp S$ denotes the number of elements of a finite set S. This theorem is obtained by comparing the coefficients of q^n in the following formula

$$\left(\sum_{m\in\mathbb{Z}} q^{m^2}\right)^4 = 1 - 32\sum_{4|n}\sigma_1(n/4)q^n + 8\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

where $\sigma_1(n)$ denotes the sum of positive divisors of n. This formula was proved by Jacobi using his theory of **elliptic functions**, and later was understood as an equality between **modular forms** of weight 2 and level 2.

(2) **A conjecture of Fermat** (1601 – 1665) or Fermat's last theorem states that if n is an integer ≥ 3, then there is no positive integer a, b, c such that $a^n + b^n = c^n$. This conjecture was finally proved in the paper of Wiles at 1995 as follows. Assume that

there are a prime number $p \geq 5$ and positive integers a, b, c such that $a^p + b^p = c^p$. Then the equation

$$y^2 = x(x - b^p)(x - c^p)$$

defines an elliptic curve E over $\mathbb{Q}$ which is a geometric counterpart of **elliptic functions**. By proving a conjecture of Shimura (and Taniyama) substantially, Wiles showed that the zeta function of E becomes the Mellin transform of a special **modular form**, called a cusp form, of weight 2. By the fact that the discriminant of E is $(abc)^{2p}$ and Frey-Ribet's theorem, the level of this cusp form actually becomes 2 which yields a contradiction since there is no cusp form of weight 2 and level 2. Actually, the proofs of Wiles and Ribet use algebraic geometry of modular curves which are geometric counterparts of **modular forms**.

Two viewpoints of the above formulas.

(1) Identities between functions.

(2) Identities between formal power series.

Recall Riemann's zeta function $\zeta(s)$ is defined as

$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\mathrm{Re}(s) > 1).$$

Applying (2) to the infinite product of $\sin(x)$,

$$\begin{aligned} \sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = \sum_{m=0}^{\infty} (-1)^m \frac{x^{2m+1}}{(2m+1)!}; \text{ Taylor expansion} \\ &= x\left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{2^2\pi^2}\right)\left(1 - \frac{x^2}{3^2\pi^2}\right)\cdots. \end{aligned}$$

Therefore, comparing the coefficients of x^3 in the both sides,

$$-\frac{1}{3!} = -\left(\frac{1}{\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \cdots\right).$$

and hence we can compute the special value of $\zeta(s)$ at $s = 2$ as $\zeta(2) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Exercise 1.1.1. Using $\zeta(2)^2 = \zeta(4) + 2\sum_{n<m} \frac{1}{n^2m^2}$, show $\zeta(4) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$.

Remark. The Bernoulli numbers B_k are defined by the power series expansion

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

Then B_k are seen to be rational numbers, and for any even positive integer $2n$,

$$\zeta(2n) = \frac{2^{2n-1}}{(2n)!} B_{2n} \pi^{2n}.$$

Therefore, $\zeta(2n)/\pi^{2n}$ is a rational number.

Exercise 1.1.2. Using the pentagon number theorem, prove that

$$q^{1/24} \prod_{n=1}^{\infty} (1-q^n) = \sum_{m=1}^{\infty} a(m)\ q^{m^2/24},$$

where

$$a(m) = \begin{cases} 1 & (\text{if } m \equiv 1, 11 \bmod (12)), \\ -1 & (\text{if } m \equiv 5, 7 \bmod (12)), \\ 0 & (\text{otherwise}). \end{cases} \quad \left(= \left(\frac{12}{m} \right) : \text{ Jacobi symbol.} \right)$$

Remark. The followings are important examples of "infinite sum = infinite product".

Rogers-Ramanujan's identity (given by Rogers, Ramanujan and Schur in 1917–1919).

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \frac{q^{n^2}}{(1-q)\cdots(1-q^n)} &= \prod_{n=1}^{\infty} \frac{1}{(1-q^{5n-4})(1-q^{5n-1})}, \\ 1 + \sum_{n=1}^{\infty} \frac{q^{n^2+n}}{(1-q)\cdots(1-q^n)} &= \prod_{n=1}^{\infty} \frac{1}{(1-q^{5n-3})(1-q^{5n-2})}. \end{aligned}$$

This formula is important in combinatorics and representation theory.

Mock theta conjecture by Ramanujan on the 5th order case. Put

$$(a;q)_0 = 1, \quad (a;q)_n = \prod_{k=0}^{n-1} \left(1 - aq^k\right), \quad (a;q)_\infty = \prod_{k=0}^{\infty} \left(1 - aq^k\right).$$

Then

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{q^{n^2}}{(-q;q)_n} &= \frac{(q^5;q^5)_\infty (q^5;q^{10})_\infty}{(q;q^5)_\infty (q^4;q^5)_\infty} - 2\left(-1 + \sum_{m=0}^{\infty} \frac{q^{10m^2}}{(q^2;q^{10})_{m+1} (q^8;q^{10})_m} \right), \\ \sum_{n=0}^{\infty} \frac{q^{n^2+n}}{(-q;q)_n} &= \frac{(q^5;q^5)_\infty (q^5;q^{10})_\infty}{(q^2;q^5)_\infty (q^3;q^5)_\infty} - \frac{2}{q}\left(-1 + \sum_{m=0}^{\infty} \frac{q^{10m^2}}{(q^4;q^{10})_{m+1} (q^6;q^{10})_m} \right). \end{aligned}$$

In 1988, Hickerson proved this conjecture by technical calculation. In 2008, Bringmann, Ono, Rhoades, and Folsom gave this conceptual proof using Zwegers' result in 2002 that mock theta functions become the holomorphic parts of harmonic modular forms.

1.2. Infinite product of $\sin(x)$. We explain Euler's proof of the following formula:

$$\sin(x) = x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right).$$

Since $e^{\sqrt{-1}x} = \cos x + \sqrt{-1}\sin x$,

$$\sin x = \frac{e^{\sqrt{-1}x} - e^{-\sqrt{-1}x}}{2\sqrt{-1}},$$

and hence by $e^z = \lim_{n\to\infty}(1 + z/n)^n$,

$$\sin x = \frac{1}{2\sqrt{-1}} \lim_{n\to\infty} \left\{ \left(1 + \frac{\sqrt{-1}x}{n}\right)^n - \left(1 - \frac{\sqrt{-1}x}{n}\right)^n \right\} \cdots (1).$$

Putting $n = 2m + 1$ and $\zeta = e^{2\pi\sqrt{-1}/n}$,

$$\begin{aligned} X^n - Y^n &= \prod_{k=0}^{n-1} (X - \zeta^k Y) \\ &= (X - Y) \prod_{k=1}^{m} (X - \zeta^k Y)(X - \zeta^{n-k} Y) \\ &= (X - Y) \prod_{k=1}^{m} \left(X^2 - 2XY\cos\left(\frac{2\pi k}{n}\right) + Y^2\right). \end{aligned}$$

Putting $X = 1 + t$ and $Y = 1 - t$,

$$\begin{aligned} (1+t)^n - (1-t)^n &= 2t \prod_{k=1}^{m} \left\{ (1+t)^2 - 2(1-t^2)\cos\left(\frac{2\pi k}{n}\right) + (1-t)^2 \right\} \\ &= 2t \prod_{k=1}^{m} 4\left(\sin^2\left(\frac{\pi k}{n}\right) + t^2 \sin^2\left(\frac{\pi k}{n}\right)\right) \\ &= 2^n t \prod_{k=1}^{m} \sin^2\left(\frac{\pi k}{n}\right) \prod_{k=1}^{m} \left(1 + t^2 \cot^2\left(\frac{\pi k}{n}\right)\right). \end{aligned}$$

Comparing the coefficients of t in this both sides,

$$2n = 2^n \prod_{k=1}^{m} \sin^2\left(\frac{\pi k}{n}\right),$$

and hence

$$(1+t)^n - (1-t)^n = 2nt \prod_{k=1}^{m} \left(1 + t^2 \cot^2\left(\frac{\pi k}{n}\right)\right).$$

Then putting $t = (\sqrt{-1}x)/n$ and letting $n \to \infty$, by (1),

$$\sin x = \lim_{n\to\infty} x \prod_{k=1}^{m} \left(1 - \frac{x^2}{n^2} \cot^2\left(\frac{\pi k}{n}\right)\right).$$

Since

$$\cot^2\left(\frac{\pi k}{n}\right) = \frac{\cos^2\left(\frac{\pi k}{n}\right)}{\sin^2\left(\frac{\pi k}{n}\right)} \sim \frac{n^2}{\pi^2 k^2} \ (n \to \infty),$$

we have

$$\lim_{n\to\infty} \frac{x^2}{n^2} \cot^2\left(\frac{\pi k}{n}\right) = \frac{x^2}{\pi^2 k^2},$$

and more precisely,

$$\frac{x^2}{n^2} \cot^2\left(\frac{\pi k}{n}\right) = \frac{x^2}{\pi^2 k^2} + O\left(\frac{1}{n^2}\right).$$

Furthermore, $\displaystyle\sum_{k=1}^{\infty} \frac{x^2}{\pi^2 k^2}$ is absolutely convergent, and hence by Proposition 1.1 below, the infinite product $\displaystyle\prod_{k=1}^{\infty} \left(1 - \frac{x^2}{\pi^2 k^2}\right)$ is also absolutely convergent. Therefore, we have

$$\begin{aligned} \prod_{k=1}^{m} \left(1 - \frac{x^2}{n^2} \cot^2\left(\frac{\pi k}{n}\right)\right) &= \prod_{k=1}^{m} \left(1 - \frac{x^2}{\pi^2 k^2}\right) + O\left(\frac{m}{n^2}\right) \\ &\to \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{\pi^2 k^2}\right) \ (n \to \infty), \end{aligned}$$

and it follows that

$$\sin x = x \lim_{n\to\infty} \prod_{k=1}^{m} \left(1 - \frac{x^2}{n^2} \cot^2\left(\frac{\pi k}{n}\right)\right) = x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{\pi^2 k^2}\right).$$

This completes the proof. □

Remark.

- This formula inspired the infinite product formula of elliptic functions by Gauss and Abel (cf. 3.1).

1.3. Proof of pentagonal number theorem. The following formula called the pentagon number theorem was found in 1741 and proved in 1750 by Euler.

$$\prod_{n=1}^{\infty}(1-q^n)=\sum_{m=-\infty}^{\infty}(-1)^m q^{m(3m-1)/2}.$$

Euler's proof (cf. [W, Chapter III, §XXI]). Put $P_0=\prod_{n=1}^{\infty}(1-q^n)$ and

$$P_n=\sum_{i=0}^{\infty}q^{in}(1-q^n)(1-q^{n+1})\cdots(1-q^{n+i})\quad(n>0).$$

Then we will show

$$P_n=1-q^{2n+1}-q^{3n+2}P_{n+1}\quad(n\geq 0)\quad\cdots\cdots(*).$$

First,

$$\begin{aligned}
& 1-q-q^2P_1\\
=\ & 1-q-q^2\left\{1-q+q(1-q)(1-q^2)+q^2(1-q)(1-q^2)(1-q^3)+\cdots\right\}\\
=\ & 1-q-q^2(1-q)-q^3(1-q)(1-q^2)-q^4(1-q)(1-q^2)(1-q^3)-\cdots\\
=\ & (1-q)(1-q^2)-q^3(1-q)(1-q^2)-q^4(1-q)(1-q^2)(1-q^3)-\cdots\\
=\ & (1-q)(1-q^2)(1-q^3)-q^4(1-q)(1-q^2)(1-q^3)-\cdots\\
=\ & \cdots\\
=\ & \prod_{n=1}^{\infty}(1-q^n),
\end{aligned}$$

and hence $(*)$ holds when $n=0$. Second, if $n>0$, then

$$\begin{aligned}
P_n &= (1-q^n)+q^n(1-q^n)(1-q^{n+1})+\sum_{i=2}^{\infty}q^{in}(1-q^n)(1-q^{n+1})\cdots(1-q^{n+i})\\
&= 1-q^{2n}-q^{2n+1}+q^{3n+1}+\sum_{i=2}^{\infty}q^{in}(1-q^{n+1})\cdots(1-q^{n+i})\\
&\quad -\sum_{i=2}^{\infty}q^{in+n}(1-q^{n+1})\cdots(1-q^{n+i})\\
&= 1-q^{2n+1}+\underbrace{\sum_{i=2}^{\infty}q^{in}(1-q^{n+1})\cdots(1-q^{n+i})}_{(1)}\\
&\quad \underbrace{-\sum_{i=1}^{\infty}q^{in+n}(1-q^{n+1})\cdots(1-q^{n+i})}_{(2)}
\end{aligned}$$

since $q^{in+n}(1-q^{n+1})\cdots(1-q^{n+i})|_{i=1} = q^{2n} - q^{3n+1}$. Then putting $i = j+2$ in (1), and $i = j+1$ in (2), we have

$$\begin{aligned}
P_n &= 1 - q^{2n+1} + \sum_{j=0}^{\infty} q^{jn+2n}(1-q^{n+1})\cdots(1-q^{n+j+1})(1-q^{n+j+2}) \\
&\quad - \sum_{j=0}^{\infty} q^{jn+2n}(1-q^{n+1})\cdots(1-q^{n+j+1}) \\
&= 1 - q^{2n+1} + \sum_{j=0}^{\infty} q^{jn+2n}(1-q^{n+1})\cdots(1-q^{n+j+1})(-q^{n+j+2}) \\
&= 1 - q^{2n+1} - q^{3n+2}\sum_{j=0}^{\infty} q^{j(n+1)}(1-q^{n+1})\cdots(1-q^{n+1+j}) \\
&= 1 - q^{2n+1} + q^{3n+2}P_{n+1},
\end{aligned}$$

and hence $(*)$ holds when $n > 0$. Therefore,

$$\begin{aligned}
P_0 &= 1 - q - q^2 P_1 \\
&= 1 - q - q^2(1 - q^3 - q^5 P_2) \\
&= 1 - q - q^2 + q^5 + q^{2+5} P_2 \\
&= \cdots \\
&= f_n(q) + (-1)^n q^{2+5+8+\cdots+(3n-1)} P_n \\
&= f_n(q) + (-1)^n q^{a(n)} P_n \\
&= f_n(q) + (-1)^n q^{a(n)}(1 - q^{2n+1} - q^{3n+2} P_{n+1}),
\end{aligned}$$

where $a(n) = 2 + 5 + 8 + \cdots + (3n-1) = \dfrac{3n^2+n}{2}$, and $f_n(q)$ is a polynomial of q with degree $< a(n)$. Hence $A_n(q) = f_n(q) + (-1)^n q^{a(n)}$ satisfies

$$A_{n+1}(q) - A_n(q) = (-1)^n q^{a(n)}\left(-q^{2n+1} - q^{3n+2}\right) = (-1)^{n+1}\left(q^{a(-n-1)} + q^{a(n+1)}\right).$$

Therefore,

$$\prod_{n=1}^{\infty}(1-q^n) = P_0 = \lim_{n\to\infty} A_n(q) = \sum_{n=-\infty}^{\infty}(-1)^n q^{a(n)} = \sum_{n=-\infty}^{\infty}(-1)^n q^{(3n^2-n)/2}. \quad \square$$

Remark.

- We call

$$e^{(\pi\sqrt{-1}\tau)/12}\prod_{n=1}^{\infty}\left(1 - e^{2\pi\sqrt{-1}n\tau}\right) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)\,;\ q = e^{2\pi\sqrt{-1}\tau}$$

  Dedekind's η-function which becomes a modular form of weight $1/2$.

- Using this theorem and function theory, we will show in 3.4 Jacobi's triple product

$$\prod_{n=1}^{\infty}(1-q^n)\left(1-q^{n-1/2}\zeta\right)\left(1-q^{n-1/2}\zeta^{-1}\right)=\sum_{m=-\infty}^{\infty}q^{m^2/2}\zeta^m.$$

Convergence of infinite sums. Recall that for a series $\sum_{n=1}^{\infty}a_n$ of complex numbers is absolutely convergent, namely $\sum_{n=1}^{\infty}|a_n|$ is convergent, then $\sum_{n=1}^{\infty}a_n$ is convergent to the same value independent of the orders of this sum.

Definition of convergence of infinite products. If a sequence $\{a_n\}$ satisfies that each $1+a_n$ is not 0 and that subproducts $\prod_{n=1}^{m}(1+a_n)$ converges to a nonzero number c, then the infinite product $\prod_{n=1}^{\infty}(1+a_n)$ is called to be convergent to c.

Proposition 1.1. *The sum $\sum_{n=1}^{\infty}|a_n|$ is convergent if and only if the infinite product $\prod_{n=1}^{\infty}(1+|a_n|)$ is convergent, and then $\prod_{n=1}^{\infty}(1+a_n)$ is convergent to the same value independent of the orders of this product (In this case, $\prod_{n=1}^{\infty}(1+a_n)$ is called absolutely convergent).*

Proof. The first assertion follows from that

$$\sum_{n=1}^{m}|a_n|\le\prod_{n=1}^{m}(1+|a_n|)\le\prod_{n=1}^{m}\exp(|a_n|)=\exp\left(\sum_{n=1}^{m}|a_n|\right),$$

and that if $|a_n|\le 1/2$, then

$$\left|\prod_{n=1}^{m}(1+a_n)^{-1}\right|\le\prod_{n=1}^{m}\left(1+|a_n|+|a_n|^2+\cdots\right)\le\prod_{n=1}^{m}(1+2|a_n|)\le\exp\left(2\sum_{n=1}^{m}|a_n|\right).$$

The second one follows from the above property of absolute convergent sums. □

Exercise 1.3.1. For any $x\in\mathbb{C}$, using Proposition 1.1 show that the infinite product

$$\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2\pi^2}\right)$$

is absolutely convergent.

Exercise 1.3.2. Using Proposition 1.1 show that the infinite product

$$\prod_{n=1}^{\infty}(1-q^n)$$

is absolutely convergent if $|q|<1$.

§2. Function theory

2.1. Holomorphic functions and Cauchy's theorem.

Definition. A *complex function* is a complex valued function of a complex variable. For $a \in \mathbb{C}$, $f(z)$ is a *holomorphic function* at $z = a$ if there is a neighborhood U of a, i.e., an open subset of $\mathbb{C}$ containing a such that

- $f(z)$ is a complex function defined over U,
- The limit $\lim_{z \in U, z \to a} \dfrac{f(z) - f(a)}{z - a}$ exists and is independent of ways of approaching $z \to a$. This limit is called the derivative of $f(z)$ at $z = a$, and denoted by $f'(a)$.

Remark.

- A holomorphic function at $z = a$ is continuous at $z = a$.
- If $f(z)$, $g(z)$ are holomorphic functions at $z = a$, then $f(z) \pm g(z)$, $f(z)g(z)$ are holomorphic at $z = a$, and $f(z)/g(z)$ is holomorphic at $z = a$ when $g(a) \neq 0$.

Example. The following functions are holomorphic on $\mathbb{C}$, namely holomorphic at any point on $\mathbb{C}$.

- Polynomial function: $a_n z^n + \cdots + a_1 z + a_0$,
- Exponential function: $e^z = e^x(\cos y + \sqrt{-1} \sin y)$; $z = x + \sqrt{-1}y$,
- Trigonometric function: $\cos z = \dfrac{e^{\sqrt{-1}z} + e^{-\sqrt{-1}z}}{2}$, $\sin z = \dfrac{e^{\sqrt{-1}z} - e^{-\sqrt{-1}z}}{2\sqrt{-1}}$.

Cauchy-Riemann's relation. *A differentiable function $f(z)$ is holomorphic at $z = a$ if and only if $f(z)$ satisfies*

$$\sqrt{-1}\frac{\partial f}{\partial x}(a) = \frac{\partial f}{\partial y}(a).$$

Proof. We prove the only if part by considering the two approaches $a + x \to a$ $(x \to +0)$ and $a + \sqrt{-1}y \to a$ $(y \to +0)$. Therefore, by definition

$$\frac{\partial f}{\partial x}(a) = f'(a) = \lim_{y \to 0} \frac{f(a + \sqrt{-1}y) - f(a)}{\sqrt{-1}y} = \frac{1}{\sqrt{-1}}\frac{\partial f}{\partial y}(a).$$

This completes the proof. □

Definition. Let D be a domain, namely connected and open subset of $\mathbb{C}$, and C be an oriented path in D. Then for a holomorphic function on D, its line integral along C is defined as

$$\int_C f(z)dz = \lim_{N \to \infty} \sum_{n=1}^{N} f(z_n)\,(z_n - z_{n-1})\,,$$

where z_0 and z_N are the starting and end points of C respectively.

Cauchy's (integral) theorem (actually founded by Gauss). *Let $D \subset \mathbb{C}$ be a domain, and $C \subset D$ be an counterclockwise oriented closed path such that the interior is contained in D. Then for any holomorphic function on D,*

$$\int_C f(z)dz = 0.$$

Proof. Let U be the interior of C. Then the boundary ∂U is C, and hence by Green's formula,

$$\int_C f(z)dz = \int_U d(f(z)dz).$$

Furthermore,

$$d(f(z)dz) = \left(\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy\right)(dx + \sqrt{-1}dy) = \left(\sqrt{-1}\frac{\partial f}{\partial x} - \frac{\partial f}{\partial y}\right)dx \wedge dy$$

which is equal to 0 by Cauchy-Riemann's relation. Therefore, $\int_C f(z)dz = 0$. $\square$

Application of Cauchy's theorem. *Let the notation be as in Cauchy's theorem.*

(1) **Cauchy's integral formula**. *For a point a in the interior of C,*

$$f(a) = \frac{1}{2\pi\sqrt{-1}}\int_C \frac{f(z)}{z-a}dz.$$

(2) **Taylor expansion**. *For points $a, z \in D$ such that $|z-a| < d(a, \partial D)$,*

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n.$$

Proof. First, we prove (1). Let $C(a;r) \subset \mathbb{C}$ be a circle with center a and radius $r > 0$ which is contained in the interior of C. Then $f(z)/(z-a)$ is holomorphic outside $C(a;r)$, and hence by Cauchy's theorem,

$$\begin{aligned}
\frac{1}{2\pi\sqrt{-1}}\int_C \frac{f(z)}{z-a}dz &= \frac{1}{2\pi\sqrt{-1}}\int_{C(a;r)} \frac{f(z)}{z-a}dz \\
&= \frac{1}{2\pi\sqrt{-1}}\int_0^{2\pi} \frac{f\left(a + re^{\sqrt{-1}\theta}\right)}{re^{\sqrt{-1}\theta}} re^{\sqrt{-1}\theta}\sqrt{-1}d\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} f\left(a + re^{\sqrt{-1}\theta}\right)d\theta.
\end{aligned}$$

This limit under $r \to 0$ is equal to

$$f(a)\frac{1}{2\pi}\int_0^{2\pi} d\theta = f(a)$$

which implies (1).

Second, we prove (2). If $\zeta \in C(a;r)$, then $|(z-a)/(\zeta-a)| < 1$. Hence by (1),

$$\begin{aligned} f(z) &= \frac{1}{2\pi\sqrt{-1}} \int_{C(a;r)} \frac{f(\zeta)}{\zeta - z} d\zeta \\ &= \frac{1}{2\pi\sqrt{-1}} \int_{C(a;r)} \frac{f(\zeta)}{\zeta - a} \left(1 - \frac{z-a}{\zeta-a}\right)^{-1} d\zeta \\ &= \frac{1}{2\pi\sqrt{-1}} \int_{C(a;r)} \sum_{n=0}^{\infty} (z-a)^n \frac{f(\zeta)}{(\zeta-a)^{n+1}} d\zeta. \end{aligned}$$

Therefore, if we put

$$c_n = \frac{1}{2\pi\sqrt{-1}} \int_{C(a;r)} \frac{f(\zeta)}{(\zeta-a)^{n+1}} d\zeta,$$

then

$$f(z) = \sum_{n=0}^{\infty} c_n (z-a)^n,$$

and hence by taking the nth derivative and putting $z = a$ of the both sides, we have

$$c_n = \frac{f^{(n)}(a)}{n!}.$$

This completes the proof. □

Example.

$$\begin{aligned} e^z &= 1 + z + \frac{1}{2!}z^2 + \frac{1}{3!}z^3 + \cdots, \\ \cos z &= 1 - \frac{1}{2!}z^2 + \frac{1}{4!}z^4 - \cdots, \\ \sin z &= z - \frac{1}{3!}z^3 + \frac{1}{5!}z^5 - \cdots. \end{aligned}$$

Meromorphic function. Let $f(z)$ be a complex function.

- For a positive integer m, $f(z)$ is called to have *a zero of order m at $z = a$* if

  $$f(z) = \sum_{n=m}^{\infty} c_n (z-a)^n$$

  around $z = a$, where $c_m \neq 0$.

- For a positive integer m, $f(z)$ is called to have *a pole of order m at $z = a$* if

  $$f(z) = \sum_{n=-m}^{\infty} c_n (z-a)^n; \text{ Laurent expansion of } f(z)$$

  around $z = a$, where $c_{-m} \neq 0$.

- For a domain $D \subset \mathbb{C}$, $f(z)$ is called *meromorphic on* D if $f(z)$ is holomorphic or $f(z)$ has a pole of finite order at each point on D.

Exercise 2.1.1.

- Prove that if $f(z)$ and $g(z)$ have zeros (resp. poles) of order m and n respectively at $z = a$, then $f(z)g(z)$ has a zero (resp. pole) of order $m + n$ at $z = a$.
- Prove that if $f(z)$ has a zero (resp. pole) of order m at $z = a$, then $1/f(z)$ has a pole (resp. zero) of order m at $z = a$.

2.2. Residue theorem and Liouville's theorem.

Residue theorem. *Let $D \subset \mathbb{C}$ be a domain, and $C \subset D$ be a counterclockwise oriented closed path such that the interior of C is contained in D. Then for points $a_1, ..., a_k$ in the interior of C and a holomorphic function on $D - \{a_1, ..., a_k\}$,*

$$\int_C f(z)dz = 2\pi\sqrt{-1}\sum_{j=1}^{k} \mathrm{Res}_{a_j} f(z).$$

Here $\mathrm{Res}_{a_j} f(z) = c_{-1}^{(j)}$ is called the residue of $f(z)$ at $z = a_j$, where

$$f(z) = \sum_{n\in\mathbb{Z}} c_n^{(j)}(z - a_j)^n$$

denotes the Laurent expansion.

Proof. For each $j = 1, ..., k$, let $C_j \subset \mathbb{C}$ be a circle with center a_j and small radius such that C_j and its interior are disjoint to each other and contained in the interior of C. Then $f(z)$ is holomorphic outside C_j, and hence by Cauchy's theorem,

$$\int_C f(z)dz = \sum_{j=1}^{k} \int_{C_j} f(z)dz.$$

Furthermore, by the following exercise,

$$\int_{C_j} f(z)dz = \int_{C_j} \sum_n c_n^{(j)}(z - a_j)^n dz = \sum_n \int_{C_j} c_n^{(j)}(z - a_j)^n dz = 2\pi\sqrt{-1}c_{-1}^{(j)},$$

and hence

$$\int_C f(z)dz = 2\pi\sqrt{-1}\sum_{j=1}^{k} \mathrm{Res}_{a_j} f(z).$$

This completes the proof. □

Exercise 2.2.1. Let r be a positive number and a be a point on $\mathbb{C}$. Then for an integer n, show that

$$\int_{|z-a|=r} (z - a)^n dz = \begin{cases} 0 & (n \neq -1), \\ 2\pi\sqrt{-1} & (n = -1). \end{cases}$$

Liouville's theorem. *A bounded holomorphic function on $\mathbb{C}$ becomes a constant function.*

Proof. Let $f(z)$ be a bounded holomorphic function on $\mathbb{C}$. Then for each $a \in \mathbb{C}$,

$$f(z) = f(a) + f'(a)(z - a) + \frac{f''(a)}{2}(z - a)^2 + \cdots,$$

and hence

$$\frac{f(z)}{(z-a)^2} = \frac{f(a)}{(z-a)^2} + \frac{f'(a)}{z-a} + \frac{f''(a)}{2} + \cdots.$$

Since $f(z)/(z-a)^2$ is holomorphic except $z = a$, for any $R > |a|$, by the residue theorem,

$$\int_{|z|=R} \frac{f(z)}{(z-a)^2} dz = 2\pi\sqrt{-1}\mathrm{Res}_a\left(\frac{f(z)}{(z-a)^2}\right) = 2\pi\sqrt{-1}f'(a).$$

By the assumption on $f(z)$, there is a constant M such that $|f(z)| < M$ for any $z \in \mathbb{C}$, and hence

$$\begin{aligned} |f'(a)| &= \left|\frac{1}{2\pi\sqrt{-1}}\int_{|z|=R} \frac{f(z)}{(z-a)^2} dz\right| \\ &\leq \frac{1}{2\pi}\max_{|z|=R}\left|\frac{f(z)}{(z-a)^2}\right| 2\pi R \\ &\leq \frac{M2\pi R}{2\pi(R-|a|)^2} \to 0 \ (R \to \infty). \end{aligned}$$

Therefore, $f'(a) = 0$ for any $a \in \mathbb{C}$, and hence $f(z)$ is a constant function. □

Fundamental theorem of algebra (first proved by Gauss). *Any polynomial equation over $\mathbb{C}$ of positive degree has at least a solution in $\mathbb{C}$.*

Proof. Assume, on the contrary, that there is a polynomial

$$f(z) = a_n z^n + \cdots + a_1 z + a_0 \ (a_i \in \mathbb{C},\ a_n \neq 0)$$

of degree $n > 0$ such that $f(z) = 0$ has no root in $\mathbb{C}$. Then $g(z) = 1/f(z)$ becomes a holomorphic function on $\mathbb{C}$. If $z \neq 0$, then

$$|f(z)| = |a_n|\,|z|^n \left|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_1}{a_n z^{n-1}} + \frac{a_0}{a_n z^n}\right|,$$

and hence

$$\lim_{|z|\to\infty} \frac{|f(z)|}{|a_n||z|^n} = \lim_{|z|\to\infty} \left|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_1}{a_n z^{n-1}} + \frac{a_0}{a_n z^n}\right| = 1.$$

This implies that

$$\lim_{|z|\to\infty} |g(z)| = \lim_{|z|\to\infty} \frac{1}{|f(z)|} = \lim_{|z|\to\infty} \frac{1}{|a_n||z|^n} = 0,$$

and hence there is a positive constant M such that $|g(z)| < 1$ if $|z| > M$. Furthermore, $\{|g(z)| \mid |z| \leq M\}$ is compact and hence bounded since it is the image by the continuous function $|g(z)|$ of the compact set $\{z \in \mathbb{C} \mid |z| \leq M\}$. Therefore, $g(z)$ is bounded on

the whole $\mathbb{C}$, and hence by Liouville's theorem, $g(z)$ becomes a constant function. This implies that $f(z)$ is also a constant function which is a contradiction. $\square$

Maximum modulus principle. *Let $f(z)$ be a holomorphic function on a connected domain D. If there exists a point a in the interior of D such that*

$$|f(a)| = \max_{z \in D} |f(z)|,$$

then $f(z)$ becomes a constant function.

Proof. Take a point a satisfying the assumption, and put

$$M = |f(a)| = \max_{z \in D} |f(z)|, \quad F = \{z \in D \mid |f(z)| = M\}.$$

Since $|f(z)|$ is a continuous function, F is a closed subset of D.

First, we will prove that $F = D$. Assume, on the contrary that, $F \neq D$. Then there is a point b on the boundary of F which is contained in the interior of D, and hence there is a positive number r such that

$$\{z \in \mathbb{C} \mid |z - b| < r\} \subset D.$$

If $0 < \rho < r$, then

$$f(z) = f(b) + f'(b)(z - b) + \cdots \quad (|z - b| \leq \rho),$$

and hence

$$\frac{f(z)}{z - b} = \frac{f(b)}{z - b} + f'(b) + \cdots.$$

Therefore, by the residue theorem,

$$f(b) = \mathrm{Res}_b \left(\frac{f(z)}{z - b} \right) = \frac{1}{2\pi\sqrt{-1}} \int_{|z-b|=\rho} \frac{f(z)}{z - b} dz.$$

Since $b \in F$ and $|f(z)| \leq M$ for any $z \in D$,

$$M = |f(b)| = \frac{1}{2\pi} \left| \int_{|z-b|=\rho} \frac{f(z)}{z - b} dz \right| \overset{(*)}{\leq} \frac{1}{2\pi} \left| \int_{|z-b|=\rho} \frac{M}{\rho} dz \right| = M.$$

Then $(*)$ is an equality, and hence by the continuity of $|f(z)|$, $|f(z)| = M$ if $|z - b| = \rho$. Therefore, $|f(z)| = M$ if $|z - b| < r$. Since b belongs to the boundary of F, there is a point z on D such that $|z - b| < r$ and $z \notin F$, and hence $|f(z)| < M$ which is a contradiction. Therefore, $F = D$ which means that $|f(z)| = M$ for any $z \in D$.

Second, we will prove that $f(z)$ is a constant function. For the above a,

$$g(z) = f(z) + f(a)$$

is a holomorphic function on D. If $z \in D$, then $|f(z)| = M$, and hence

$$|g(z)| \leq |f(z)| + |f(a)| = 2M.$$

Since $|g(a)| = |2f(a)| = 2M$, we have

$$\max_{z \in D} |g(z)| = |g(a)| = 2M.$$

Therefore, $g(z)$ satisfies the assumption of this theorem, and hence for any $z \in D$,

$$|g(z)| = |f(z) + f(a)| = 2M.$$

Since $|f(z)| = |f(a)| = M$, $f(z) = f(a)$ for any $z \in D$. Therefore, $f(z)$ is a constant function. $\square$

§3. Elliptic functions

3.1. History from Gauss. (cf. [T]) In 1797, as an extension of

$$\int \frac{dx}{\sqrt{1-x^2}} \overset{x=\sin\theta}{=} \int \frac{\cos\theta\ d\theta}{\cos\theta} = \theta = \sin^{-1} x;\ \text{the inverse function of sin},$$

Gauss found that the inverse function of

$$\int \frac{dx}{\sqrt{1-x^4}}$$

has a double periodicity as a complex function.

More precisely, Gauss considered the Lemniscate curve defined as $x^2 = \cos 2\theta$ in the polar coordinates (x, θ) which is equivalent to that the product of the distances from $(\pm 1/\sqrt{2}, 0)$ is equal to $1/2$. Put $X = x\cos\theta$, $Y = x\sin\theta$ which is the regular coordinates, and denote by u the distance along this Lemniscate curve between the origin $(0,0)$ and (X,Y) with $X, Y > 0$. Then

$$u \overset{\text{def}}{=} \int_0^X \sqrt{(dX)^2 + (dY)^2},$$

and hence

$$u = \int_0^x \sqrt{(dx)^2 + (xd\theta)^2} = \int_0^x \sqrt{1 + \left(x\frac{d\theta}{dx}\right)^2}\, dx = \int_0^x \frac{dx}{\sqrt{1-x^4}} \ \cdots\cdots (*).$$

This inverse function is extended to a smooth function $x = s(u)$ of $u \in \mathbb{R}$. Put

$$\omega = \int_0^1 \frac{dx}{\sqrt{1-x^4}}.$$

Therefore, by the geometric meaning of the Lemniscate curve, $s(u)$ has the periodicity $s(u+4\omega) = s(u)$. Furthermore, using $s\left(\sqrt{-1}u\right) = \sqrt{-1}s(u)$ and the addition law of $s(u)$, Gauss extended $s(u)$ for a complex variable u. Then $s(u)$ has the another periodicity $s\left(u + 4\omega\sqrt{-1}\right) = s(u)$, and

$$\begin{cases} s(u) = 0 & \Leftrightarrow \quad u = \left(2m + 2n\sqrt{-1}\right)\omega, \\ s(u) = \infty & \Leftrightarrow \quad u = \left\{(2m+1) + (2n+1)\sqrt{-1}\right\}\omega \end{cases}$$

for integers m, n. Therefore, as an analogy to Euler's infinite product presentation of $\sin x$, Gauss obtained an infinite product presentation of $s(u)$ as

$$s(u) = \frac{u \times \prod\limits_{m,n=0,1,2,\ldots,\ m\neq 0} \left(1 - \dfrac{1}{(m+n\sqrt{-1})^4}\left(\dfrac{u}{2\omega}\right)^4\right)}{\prod\limits_{m,n=1,3,5,\ldots} \left(1 - \dfrac{1}{(m+n\sqrt{-1})^4}\left(\dfrac{u}{\omega}\right)^4\right)}$$

which is a meromorphic function represented as the quotient of holomorphic functions called theta functions.

Exercise 3.1.1. Prove the above $(*)$.

Elliptic function. A meromorphic function $f(z)$ on $\mathbb{C}$ is called an *elliptic function* if $f(z)$ has double periodicity, namely there exist $\omega_1, \omega_2 \in \mathbb{C}$ which are linearly independent over $\mathbb{R}$ such that

$$f(z+\omega_1) = f(z), \quad f(z+\omega_2) = f(z)$$

for any $z \in \mathbb{C}$. The complex numbers ω_1, ω_2 are called *periods* of $f(z)$.

Exercise 3.1.2. Let $f(z)$ be an elliptic function with periods $\omega_1, \omega_2 \in \mathbb{C}$ which are linearly independent over $\mathbb{R}$. Then show the followings.

- The lattice in $\mathbb{C}$
$$L \stackrel{\text{def}}{=} \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$$
is a subgroup of $\mathbb{C}$ under the addition of numbers.
- For each $a \in L$, we have $f(z+a) = f(z)$ $(z \in \mathbb{C})$.
- Let
$$D = \{s\omega_1 + t\omega_2 \mid 0 \le s, t \le 1\}.$$
Then
$$\{f(z) \mid z \in \mathbb{C}\} = \{f(z) \mid z \in D\}.$$

Theorem 3.1. *If an elliptic function is holomorphic on the whole complex plane $\mathbb{C}$, then this is a constant function.*

Proof. Let $f(z)$ be a elliptic function with periods ω_1, ω_2, and assume that $f(z)$ is holomorphic on $\mathbb{C}$. Put

$$D = \{s\omega_1 + t\omega_2 \mid 0 \le s, t \le 1\}.$$

Then by Exercise 3.1.2,

$$\{f(z) \mid z \in \mathbb{C}\} = \{f(z) \mid z \in D\}$$

whose right hand side is the image of the compact set D by the continuous function $f(z)$. Therefore, this image is compact, and hence is bounded in $\mathbb{C}$. By Liouville's theorem, $f(z)$ is a constant function. $\square$

Exercise 3.1.3. Prove Theorem 3.1 using the maximum modulus principle.

3.2. Weierstrass' $\wp$-function.

$\wp$-function. For a lattice $L = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$ of $\mathbb{C}$, we define the associated Weierstrass' $\wp$-function as

$$\wp(z) = \wp_L(z) = \frac{1}{z^2} + \sum_{a \in L - \{0\}} \left(\frac{1}{(z-a)^2} - \frac{1}{a^2} \right).$$

Therorem 3.2.

(1) *$\wp(z)$ is a meromorphic function on $\mathbb{C}$ which is holomorphic outside L, and has poles of order 2 at points on L.*

(2) *$\wp(z)$ is an even function, namely $\wp(-z) = \wp(z)$, and for any $a \in L$, $\wp(z+a) = \wp(z)$.*

(3) $\wp(z) = \dfrac{1}{z^2} + \displaystyle\sum_{n=1}^{\infty} \left((2n+1) \sum_{a \in L - \{0\}} \frac{1}{a^{2n+2}} \right) z^{2n}$ *at $z = 0$.*

(4) *Put* $g_2 = 60 \displaystyle\sum_{a \in L - \{0\}} \frac{1}{a^4}$, $g_3 = 140 \displaystyle\sum_{a \in L - \{0\}} \frac{1}{a^6}$. *Then* $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.

Remark. If we put $\wp(z) = x$, then by (4),

$$\wp^{-1}(x) = z = \int dz = \int \frac{d\wp(z)}{\wp'(z)} = \int \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}},$$

and hence $\wp(z)$ is the inverse function of an elliptic integral.

Proof.

(1) Let R be a positive real number. If $|z| \leq R$, then there is a constant $c > 0$ such that for any $a \in \mathbb{C}$ with $|a| > 2R$,

$$\left| \frac{1}{(z-a)^2} - \frac{1}{a^2} \right| = \left| \frac{2za - z^2}{(z-a)^2 a^2} \right| < \frac{c}{|a|^3}.$$

Furthermore, there is a constant $r > 0$ such that $\{z \in \mathbb{C} \mid |z| \leq r\}$ is contained in $\{s\omega_1 + t\omega_2 \mid -1 \leq s, t \leq 1\}$. Then

$$\sum_{a \in L - \{0\}} \frac{1}{|a|^3} = \sum_{k=1}^{\infty} \sum_{\max\{|m|,|n|\}=k} \frac{1}{|m\omega_1 + n\omega_2|^3} \leq \sum_{k=1}^{\infty} \frac{8k}{(kr)^3} < +\infty,$$

and hence

$$\sum_{a \in L, |a| > 2R} \left(\frac{1}{(z-a)^2} - \frac{1}{a^2} \right)$$

is absolutely convergent uniformly on z with $|z| \leq R$. Therefore, the assertion follows since

$$\frac{1}{z^2} + \sum_{a \in L, 0<|a| \leq 2R} \left(\frac{1}{(z-a)^2} - \frac{1}{a^2} \right)$$

is a rational function of z with poles in L of order 2.

(2) By definition,

$$\wp(-z) = \frac{1}{z^2} + \sum_{a \in L - \{0\}} \left(\frac{1}{(z+a)^2} - \frac{1}{a^2} \right) \overset{b=-a}{=} \frac{1}{z^2} + \sum_{b \in L - \{0\}} \left(\frac{1}{(z-b)^2} - \frac{1}{b^2} \right) = \wp(z),$$

and hence $\wp(z)$ is an even function. Since

$$\wp'(z) = -\frac{2}{z^3} - \sum_{a \in L - \{0\}} \frac{2}{(z-a)^3} = -\sum_{b \in L} \frac{2}{(z-b)^3}$$

is absolutely convergent in the wider sense, for any $a \in L$,

$$\wp'(z+a) = -\sum_{b \in L} \frac{2}{(z+a-b)^3} \overset{c=b-a}{=} -\sum_{c \in L} \frac{2}{(z-c)^3} = \wp'(z).$$

Therefore, for each $a \in L$, $\wp(z+a) - \wp(z)$ is a constant independent of z. Since $\wp(z)$ is an even function, this constant is

$$\wp\left(-\frac{a}{2} + a\right) - \wp\left(-\frac{a}{2}\right) = \wp\left(\frac{a}{2}\right) - \wp\left(-\frac{a}{2}\right) = 0.$$

(3) Taking the derivatives by z of

$$\frac{1}{a-z} = \frac{1}{a}\left(1 - \frac{z}{a}\right)^{-1} = \frac{1}{a}\left(1 + \frac{z}{a} + \frac{z^2}{a^2} + \cdots\right),$$

we have

$$\frac{1}{(z-a)^2} = \frac{1}{a}\left(\frac{1}{a} + \frac{2z}{a^2} + \frac{3z^2}{a^3} + \cdots\right) = \sum_{n=0}^{\infty} (n+1)\frac{z^n}{a^{n+2}}.$$

$$\therefore\ \wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} \left((n+1) \sum_{a \in L - \{0\}} \frac{1}{a^{n+2}} \right) z^n.$$

Since $\wp(z)$ is an even function, this coefficients of z^n is 0 if n is odd, and hence (3) holds.

(4) Put

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

Then by (1) and (2), $f(z)$ is a meromorphic function on $\mathbb{C}$ which is holomorphic outside L and satisfies that $f(z+a) = f(z)$ for any $a \in L$. By the following Exercise 3.2.1, $f(z)$ is holomorphic at $z = 0$, and hence by (1), it is also holomorphic at each point on L.

Therefore, $f(z)$ is holomorphic on $\mathbb{C}$, and hence by Theorem 3.1, $f(z)$ becomes a constant function on $\mathbb{C}$. Furthermore, by Exercise 3.2.1, $f(0) = 0$, and hence $f(z) = 0$. $\square$

Exercise 3.2.1. Show that LHS $-$ RHS of (4) has a Taylor expansion at $z = 0$ of the form

$$c_1 z + c_2 z^2 + \cdots.$$

Exercise 3.2.2. Calculating the Taylor expansion of LHS $-$ RHS of (4), show that

$$\sum_{a \in L - \{0\}} \frac{1}{a^8} = \frac{3}{7} \left(\sum_{a \in L - \{0\}} \frac{1}{a^4} \right)^2.$$

3.3. Abel's theorem and elliptic curves.

Aim. Following [MM], we review Abel's proof of the addition formula of $\wp(z) = \wp_L(z)$:

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2.$$

Theorem 3.3. *If complex numbers z_i $(1 \leq i \leq 3)$ satisfies $z_1 + z_2 + z_3 = 0$, then*

$$\big(\wp(z_i), \wp'(z_i)\big) \ \ (1 \leq i \leq 3)$$

belong to a straight line.

Exercise 3.3.1. Using this theorem, show the above addition formula.

Proof. For $x = \wp(z)$, $y = \wp'(z)$, consider the equation $y^2 = 4x^3 - g_2x - g_3$ given in Theorem 3.2 (4) and a linear equation $y = ax + b$ together. Then the solutions e_i $(1 \leq i \leq 3)$ of these equations satisfy

$$F(x) \stackrel{\text{def}}{=} 4x^3 - g_2x - g_3 - (ax+b)^2 = 0.$$

Moving a and b, we study e_i as functions of a, b. Since

$$dF(x) = \frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial a}da + \frac{\partial F}{\partial b}db = 0 \ \ \text{at } x = e_i,$$

we have $F'(e_i)dx = 2(ax+b)(xda + db)$, and hence

$$\frac{dx}{y} = \frac{2(e_ida + db)}{F'(e_i)} \ \ \text{at } x = e_i \ \cdots (*)$$

Since $F(x) = 4(x-e_1)(x-e_2)(x-e_3)$,

$$\sum_{i=1}^{3} \frac{2(e_ida + db)}{F'(e_i)} = 0.$$

We take $z_i \in \mathbb{C}$ satisfying $\wp(z_i) = e_i$. Since $dx/y = d\wp(z)/\wp'(z) = dz$, by $(*)$ we have

$$\sum_{i=1}^{3} dz_i = \sum_{i=1}^{3} \frac{2(e_ida + db)}{F'(e_i)} = 0,$$

and hence $c = z_1 + z_2 + z_3$ is a constant as a function of a, b. If we put $a = 0$ and let $b \to \infty$, then each e_i tends to ∞, namely z_i tends to a point on L. Therefore,

$$z_1 + z_2 + z_3 = c \in L; \ \textbf{Abel's theorem!}$$

and hence $z_1 + z_2 + (z_3 - c) = 0$. Then the three points

$$\big(\wp(z_i), \wp'(z_i)\big) = (e_i, ae_i + b) \ \ (1 \leq i \leq 3)$$

belong to the line defined by $y = ax + b$, and this line is uniquely determined by the two points $(\wp(z_1), \wp'(z_1))$, $(\wp(z_2), \wp'(z_2))$. Since $(\wp(z_3), \wp'(z_3)) = (\wp(z_3 - c), \wp'(z_3 - c))$, we completes the proof. $\square$

Elliptic curve. The 1-dimensional algebraic variety

$$\begin{aligned} E &= \left\{(x, y) \mid y^2 = 4x^3 - g_2 x - g_3\right\} \cup \{\infty\} \\ &= \left\{(X : Y : Z)) \in \mathbb{P}^2 \mid Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3\right\} \end{aligned}$$

becomes an abelian group with ∞ as its identity satisfying that if two or three points (x_i, y_i) belong to one straight line, then their sum is equal to the identity ∞. We call E an *elliptic curve* over $\mathbb{C}$.

The meaning of Abel's theorem. The map $\mathbb{C} \to E$ given by

$$z \mapsto \begin{cases} (\wp(z), \wp'(z)) & (z \notin L), \\ \infty & (z \in L) \end{cases}$$

is a homomorphism which gives a morphism

$$\varphi : \mathbb{C}/L \to E$$

between complex manifolds. Since the image of φ is an open and closed subset of the connected space E, φ is a surjection. Furthermore, if each fiber of φ contains two points, then $\wp(z)$ has poles except 0 which is a contradiction. Therefore, φ is an injection, and hence is an isomorphism $\mathbb{C}/L \xrightarrow{\sim} E$.

Remark. The original version of Abel's theorem is a generalization of the above theorem which shows an addition formula on integrals of general algebraic functions.

Arithmetic of elliptic curves.

- **Mordell's theorem**. Let E be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = f(x)$, where $f(x)$ is a polynomial over $\mathbb{Q}$ of degree 3 without multiple root. Then the abelian group
$$E(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = f(x)\right\} \cup \{\infty\}$$
of its $\mathbb{Q}$-rational points is generated by finite elements.

- **Birch and Swinnerton-Dyer's conjecture**. This conjecture claims that for an elliptic curve E over $\mathbb{Q}$, the rank of $E(\mathbb{Q})$ is equal to the order of the L-function $L(E, s)$ of E at $s = 1$.

- **Kume's example**. The elliptic curve defined by $y^2 = x^3 - 34^2 x$ has rank 2 over $\mathbb{Q}$, and Kume found its linearly independent $\mathbb{Q}$-rational points as

$$\begin{aligned}(x, y) &= \left(\frac{145^2}{12^2}, \frac{145 \cdot 20447}{12^3}\right), \left(\frac{353^2}{60^2}, \frac{353 \cdot 23359}{60^3}\right); \text{ linearly independent} \\ &\leftrightarrow \left(24, \frac{17}{6}, \frac{145}{6}\right), \left(\frac{136}{15}, \frac{15}{2}, \frac{353}{30}\right); \text{ right triangles with area 34.}\end{aligned}$$

- **Application to Cryptography**. Elliptic curves over finite fields are applied to factorizing integers and constructing cryptography.

3.4. Jacobi's theta function and the triple product.

Theta function. Fix $\tau \in \mathbb{C}$ with positive imaginary part, and define Jacobi's theta function of $z \in \mathbb{C}$ as

$$\begin{aligned}\theta(z)(=\theta_3(z)) &= \sum_{m\in\mathbb{Z}} \exp\left(\pi\sqrt{-1}m^2\tau + 2\pi\sqrt{-1}mz\right) \\ &= \sum_{m\in\mathbb{Z}} q^{m^2/2}\cdot\zeta^m;\ q^{1/2} = e^{\pi\sqrt{-1}\tau}, \zeta = e^{2\pi\sqrt{-1}z}.\end{aligned}$$

This function is not an elliptic function, however it is a holomorphic function of z having the following property close to the double periodicity.

Proposition 3.4. *The function $\theta(z)$ is a holomorphic function over $\mathbb{C}$ and satisfies*

$$\theta(z+1) = \theta(z),\ \theta(z+\tau) = q^{-1/2}\zeta^{-1}\theta(z).$$

Proof. Since $|q| < 1$, for positive integers m,

$$\left|\frac{q^{(m+1)^2/2}\cdot\zeta^{m+1}}{q^{m^2/2}\cdot\zeta^m}\right| = \left|q^{m+1/2}\cdot\zeta\right| \to 0,\ \left|\frac{q^{(-m-1)^2/2}\cdot\zeta^{-m-1}}{q^{(-m)^2/2}\cdot\zeta^{-m}}\right| = \left|q^{m+1/2}\cdot\zeta^{-1}\right| \to 0$$

as $m \to \infty$. Then the series defining $\theta(z)$ is absolutely convergent in the wider sense, and hence is a holomorphic function of $z \in \mathbb{C}$. If $z \mapsto z+1$, then $\zeta = e^{2\pi\sqrt{-1}z}$ is invariant, and hence the function $\theta(z)$ is invariant since it is a function of ζ. Furthermore,

$$\theta(z+\tau) = \sum_{m\in\mathbb{Z}} q^{m^2/2}(\zeta q)^m = \sum_{m\in\mathbb{Z}} q^{(m+1)^2/2}\cdot q^{-1/2}\cdot\zeta^{m+1}\cdot\zeta^{-1} = q^{-1/2}\zeta^{-1}\theta(z)$$

which completes the proof. □

Theorem 3.4 (Gauss, Jacobi). $\theta(z) = \prod_{n=1}^{\infty}(1-q^n)\left(1+q^{n-1/2}\zeta\right)\left(1+q^{n-1/2}\zeta^{-1}\right)$.

Proof. First, we review Gauss' ingenious proof (cf. [T]) given in his note at 1818. Put

$$T(n) = 1 + \frac{a^n-1}{a-1}t + \frac{(a^n-1)(a^n-a)}{(a-1)(a^2-1)}t^2 + \cdots + \frac{(a^n-1)(a^n-a)\cdots(a^n-a^{n-1})}{(a-1)(a^2-1)\cdots(a^n-1)}t^n.$$

Then

$$\begin{aligned}&(1+a^nt)T(n) \\ =\ & 1 + a^nt + \frac{a^n-1}{a-1}t + \frac{a^n(a^n-1)}{a-1}t^2 + \frac{(a^n-1)(a^n-a)}{(a-1)(a^2-1)}t^2 + \\ & \cdots + \frac{a^n(a^n-1)(a^n-a)\cdots(a^n-a^{n-1})}{(a-1)(a^2-1)\cdots(a^n-1)}t^{n+1}\end{aligned}$$

$$
\begin{aligned}
&= 1+\frac{a^{n+1}-1}{a-1}t+\frac{(a^{n+1}-1)(a^{n+1}-a)}{(a-1)(a^2-1)}t^2+\\
&\quad \cdots+\frac{(a^{n+1}-1)(a^{n+1}-a)\cdots(a^{n+1}-a^n)}{(a-1)(a^2-1)\cdots(a^{n+1}-1)}t^{n+1}\\
&= T(n+1).
\end{aligned}
$$

Therefore, since $T(1)=1+t$, we have

$$
T(n)=(1+t)(1+at)(1+a^2t)\cdots(1+a^{n-1}t).
$$

Let $n=2m$ be an even positive integer. Then by the above two expressions of $T(n)$,

$$
\begin{aligned}
&1+\frac{a^n-1}{a-1}t+\frac{(a^n-1)(a^n-a)}{(a-1)(a^2-1)}t^2+\cdots+\frac{(a^n-1)(a^n-a)\cdots(a^n-a^{m-1})}{(a-1)(a^2-1)\cdots(a^m-1)}t^m+\\
&\cdots+\frac{(a^n-1)(a^n-a)\cdots(a^n-a^{n-1})}{(a-1)(a^2-1)\cdots(a^n-1)}t^n\\
&= (1+t)(1+at)(1+a^2t)\cdots(1+a^{n-1}t).
\end{aligned}
$$

Putting $a=\alpha^2$, $t=\alpha^{1-n}\zeta$ and dividing the above formula by

$$
\frac{(a^n-1)(a^n-a)\cdots(a^n-a^{m-1})}{(a-1)(a^2-1)\cdots(a^m-1)}t^m=\frac{(1-\alpha^{2n})(1-\alpha^{2n-2})\cdots(1-\alpha^{n+2})}{(1-\alpha^2)(1-\alpha^4)\cdots(1-\alpha^n)}(\alpha^{m-n}\zeta)^m,
$$

we have

$$
\begin{aligned}
&1+\frac{1-\alpha^n}{1-\alpha^{n+2}}\alpha(\zeta+\zeta^{-1})+\frac{(1-\alpha^n)(1-\alpha^{n-2})}{(1-\alpha^{n+2})(1-\alpha^{n+4})}\alpha^4(\zeta^2+\zeta^{-2})+\\
&\cdots+\frac{(1-\alpha^n)(1-\alpha^{n-2})\cdots(1-\alpha^2)}{(1-\alpha^{n+2})(1-\alpha^{n+4})\cdots(1-\alpha^{2n})}\alpha^{(n/2)^2}(\zeta^{n/2}+\zeta^{-n/2})\\
&= (1+\alpha\zeta)(1+\alpha\zeta^{-1})(1+\alpha^3\zeta)(1+\alpha^3\zeta^{-1})\cdots(1+\alpha^{n-1}\zeta)(1+\alpha^{n-1}\zeta^{-1})\\
&\quad\times\frac{(1-\alpha^2)(1-\alpha^4)\cdots(1-\alpha^n)}{(1-\alpha^{n+2})(1-\alpha^{n+4})\cdots(1-\alpha^{2n})}.
\end{aligned}
$$

Therefore, as an equality between formal power series of α whose coefficients are polynomials of $\zeta^{\pm1}$,

$$
\begin{aligned}
\sum_{m\in\mathbb{Z}}\alpha^{m^2}\zeta^m &= 1+\alpha(\zeta+\zeta^{-1})+\alpha^4(\zeta^2+\zeta^{-2})+\alpha^9(\zeta^3+\zeta^{-3})+\cdots\\
&= (1+\alpha\zeta)(1+\alpha\zeta^{-1})(1+\alpha^3\zeta)(1+\alpha^3\zeta^{-1})\cdots\\
&\quad\times(1-\alpha^2)(1-\alpha^4)(1-\alpha^6)\cdots\\
&= \prod_{n=1}^{\infty}(1-\alpha^{2n})(1+\alpha^{2n-1}\zeta)(1+\alpha^{2n-1}\zeta^{-1}).
\end{aligned}
$$

Then putting $\alpha=q^{1/2}$, we complete the proof. $\square$

Second, we give this proof using the pentagon number theorem and the function theory. Since $|q| < 1$, the infinite product

$$f(z) = \prod_{n=1}^{\infty} \left(1 + q^{n-1/2}\zeta\right)\left(1 + q^{n-1/2}\zeta^{-1}\right)$$

is absolutely convergent in the wider sense, and hence is a holomorphic function of z. Note that

$$\begin{aligned} f(z) = 0 &\Leftrightarrow \zeta = -q^{\pm(n-1/2)} \ (n \in \mathbb{N}) \\ &\Leftrightarrow z = \pm\left(n - \frac{1}{2}\right)\tau + m + \frac{1}{2} \ \ (n \in \mathbb{N},\ m \in \mathbb{Z}) \\ &\Leftrightarrow z = \left(n - \frac{1}{2}\right)\tau + m + \frac{1}{2} \left(\Leftrightarrow \zeta = -q^{n-1/2}\right) \ \ (n, m \in \mathbb{Z}), \end{aligned}$$

and that for any $n, m \in \mathbb{Z}$,

$$\begin{aligned} &\frac{d}{dz}\left(1 + q^{n-1/2}e^{-2\pi\sqrt{-1}z}\right)\Big|_{z=\left(n-\frac{1}{2}\right)\tau+m+\frac{1}{2}} \\ &= \left(q^{n-1/2}(-2\pi\sqrt{-1})e^{-2\pi\sqrt{-1}z}\right)\Big|_{z=\left(n-\frac{1}{2}\right)\tau+m+\frac{1}{2}} \\ &= 2\pi\sqrt{-1} \neq 0. \end{aligned}$$

Therefore, $f(z)$ has a zero of order 1 at

$$\left(n - \frac{1}{2}\right)\tau + m + \frac{1}{2} \ \ (n, m \in \mathbb{Z}).$$

Furthermore, for any $n \in \mathbb{Z}$,

$$\begin{aligned} \theta(z)|_{\zeta=-q^{n-1/2}} &= \sum_{m\in\mathbb{Z}} (-1)^m q^{m^2/2+m(n-1/2)} \\ &= \sum_{m\in\mathbb{Z}} (-1)^m q^{\{(m+(n-1/2))^2-(n-1/2)^2\}/2} \\ &= -\sum_{l\in\mathbb{Z}} (-1)^l q^{l^2/2+l(n-1/2)} \end{aligned}$$

by putting $l = -m + (1 - 2n)$, we have

$$\theta(z)|_{\zeta=-q^{n-1/2}} = 0.$$

Hence the quotient function $g(z) = \theta(z)/f(z)$ is a holomorphic function on $\mathbb{C}$. Further,

$$g(z+1) = \frac{\theta(z+1)}{f(z+1)} = \frac{\theta(z)}{f(z)} = g(z),$$

and by Proposition 3.4,

$$g(z+\tau) = \frac{\theta(z+\tau)}{f(z+\tau)} = \frac{q^{-1/2}\zeta^{-1}\theta(z)}{q^{-1/2}\zeta^{-1}f(z)} = g(z)$$

since

$$\begin{aligned} f(z+\tau) &= \prod_{n=1}^{\infty}(1+q^{n+1/2}\zeta)(1+q^{n-3/2}\zeta^{-1}) \\ &= \frac{1+q^{-1/2}\zeta^{-1}}{1+q^{1/2}\zeta}\prod_{n=1}^{\infty}(1+q^{n-1/2}\zeta)(1+q^{n-1/2}\zeta^{-1}) \\ &= q^{-1/2}\zeta^{-1}f(z). \end{aligned}$$

Therefore, $g(z)$ is a double periodic holomorphic function on $\mathbb{C}$, and hence is a constant C by Theorem 3.1. Putting $\zeta = -q^{-1/6}$, the Euler's pentagon theorem implies that

$$\theta(z)|_{\zeta=-q^{-1/6}} = \sum_{m\in\mathbb{Z}}(-1)^m(q^{1/3})^{m(3m-1)/2} = \prod_{n=1}^{\infty}(1-q^{n/3}),$$

and

$$f(z)|_{\zeta=-q^{-1/6}} = \prod_{n=1}^{\infty}(1-q^{n-2/3})(1-q^{n-1/3}) = \prod_{n=1}^{\infty}\frac{1-q^{n/3}}{1-q^n}.$$

Therefore,

$$g(z) = C = \prod_{n=1}^{\infty}(1-q^n)$$

which completes the proof. □

§4. Modular forms

4.1. Eisenstein series.

Exercise 4.1.1. Show that

$$SL_2(\mathbb{Z}) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \;\middle|\; \begin{array}{l} a, b, c, d \in \mathbb{Z}, \\ ad - bc = 1 \end{array} \right\}.$$

becomes a group under the product of matrices, and that $SL_2(\mathbb{Z})$ is not a commutative group. This group is called the *modular group*.

Exercise 4.1.2. Let

$$\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$$

be the *Poincaré upper half plane*. Then show the followings.

- For any $\tau \in \mathbb{H}$ and $\gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z})$, put $\gamma(\tau) \stackrel{\text{def}}{=} \dfrac{a\tau + b}{c\tau + d}$. Then

  $$\mathrm{Im}\left(\gamma(\tau)\right) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

  and $\tau \mapsto \gamma(\tau)$ gives a bijective map from $\mathbb{H}$ onto $\mathbb{H}$.

- For any $\gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$, $\gamma_1\left(\gamma_2(\tau)\right) = (\gamma_1\gamma_2)(\tau)$ $(\tau \in \mathbb{H})$.

Definition. Eisenstein series are functions of $\tau \in \mathbb{H}$ which appear in the coefficients of the Laurent expansion of $\wp_{\mathbb{Z}+\mathbb{Z}\tau}(z)$ at $z = 0$. More precisely, for an even integer $k \geq 4$, we define the Eisenstein series of weight k as

$$E_k(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(m\tau + n)^k} \quad (\tau \in \mathbb{H}).$$

Theorem 4.1.

(1) *The series $E_k(\tau)$ is uniformly absolutely convergent in the wider sense, and hence is a holomorphic function of τ.*

(2) *The function $E_k(\tau)$ of $\tau \in \mathbb{H}$ satisfies that*

$$E_k(\gamma(\tau)) := E_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k E_k(\tau) \quad \left(\gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z})\right).$$

(3) *The function $E_k(\tau)$ is represented as a (nonnegative) power series of $q = e^{2\pi\sqrt{-1}\tau}$.*

(4) *Denote by*

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k},$$

the value at k of the Riemann zeta function, and by

$$\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$$

the sum over the $(k-1)$th powers of positive divisors of a positive integer n. Then

$$E_k(\tau) = 2\zeta(k) + 2\frac{(2\pi\sqrt{-1})^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

Definition. A *modular form* (for $SL_2(\mathbb{Z})$) of weight k is defined as a function of $\tau \in \mathbb{H}$ satisfying the above conditions (1)–(3).

Proof of Theorem 4.1. Let $L = \{m\tau + n \mid m, n \in \mathbb{Z}\}$ be the lattice of $\mathbb{C}$ generated by 1 and $\tau \in \mathbb{H}$. Since $k \geq 4$, as is shown in the proof of Theorem 3.2 (1), there is a positive number r such that

$$\sum_{\alpha \in L-\{0\}} \frac{1}{|\alpha|^k} \leq \sum_{n=1}^{\infty} \frac{8n}{(nr)^k} = \frac{8}{r^k}\sum_{n=1}^{\infty}\frac{1}{n^{k-1}} < \infty,$$

and hence the assertion (1) follows.

Next, we show (2). For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, the map $\varphi_\gamma : L \to L$ defined as $\varphi_\gamma(m\tau + n) = (ma + nc)\tau + (mb + nd)$ is a bijection since it has the inverse map given by $m'\tau + n' \mapsto (m'd - n'c)\tau + (-m'b + n'a)$. Therefore,

$$\frac{1}{(c\tau+d)^k}E_k\left(\frac{a\tau+b}{c\tau+d}\right) = \sum_{\alpha\in L-\{0\}}\frac{1}{\varphi_\gamma(\alpha)^k} = \sum_{\varphi_\gamma(\alpha)\in L-\{0\}}\frac{1}{\varphi_\gamma(\alpha)^k} = E_k(\tau)$$

since the series $E_k(\tau)$ is absolutely convergent.

Finally, we show (4) from which (3) immediately follows. By taking the logarithmic derivative of the both sides of Euler's theorem shown in 1.1

$$\sin x = x\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2\pi^2}\right),$$

we have under $\mathrm{Im}(x) > 0$,

$$\begin{aligned}
\text{LHS} &= \frac{d\log(\sin x)}{dx} = \frac{\cos x}{\sin x} = \sqrt{-1}\frac{e^{2\sqrt{-1}x}+1}{e^{2\sqrt{-1}x}-1} = \sqrt{-1} - 2\sqrt{-1}\sum_{n=0}^{\infty}e^{2\sqrt{-1}nx}, \\
\text{RHS} &= \frac{d\log x}{dx} + \sum_{n=1}^{\infty}\frac{d}{dx}\log\left(1-\frac{x^2}{n^2\pi^2}\right) = \frac{1}{x} + \sum_{n=1}^{\infty}\left(\frac{1}{x+n\pi} + \frac{1}{x-n\pi}\right).
\end{aligned}$$

Then by putting $x = \pi\tau$ and multiplying the both sides by π, we have

$$\sqrt{-1}\pi - 2\pi\sqrt{-1}\sum_{n=0}^{\infty} q^n = \frac{1}{\tau} + \sum_{m=1}^{\infty}\left(\frac{1}{\tau+n} + \frac{1}{\tau-n}\right),$$

and hence by taking the $k-1(\geq 1)$th derivative of the both sides,

$$-(2\pi\sqrt{-1})^k \sum_{n=1}^{\infty} n^{k-1}q^n = (-1)^{k-1}(k-1)! \sum_{m\in\mathbb{Z}} \frac{1}{(\tau+m)^k}.$$

Therefore,

$$\sum_{m\in\mathbb{Z}} \frac{1}{(\tau+m)^k} = \frac{1}{(k-1)!}(-2\pi\sqrt{-1})^k \sum_{n=1}^{\infty} n^{k-1}q^n.$$

Since k is even, by the above formlura,

$$\begin{aligned}
E_k(\tau) &= \sum_{(m,n)\in\mathbb{Z}-\{(0,0)\}} \frac{1}{(m\tau+n)^k} \\
&= 2\sum_{n=1}^{\infty}\frac{1}{n^k} + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k} \\
&= 2\sum_{n=1}^{\infty}\frac{1}{n^k} + 2\sum_{m=1}^{\infty}\frac{1}{(k-1)!}(-2\pi\sqrt{-1})^k\sum_{n=1}^{\infty} n^{k-1}q^{nm} \\
&= 2\zeta(k) + \frac{2(2\pi\sqrt{-1})^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1}q^{nm} \\
&= 2\zeta(k) + \frac{2(2\pi\sqrt{-1})^k}{(k-1)!}\sum_{l=1}^{\infty}\sigma_{k-1}(l)q^l \quad \text{by putting } l = nm.
\end{aligned}$$

This completes the proof. □

Example.

$$\begin{aligned}
E_4(\tau) &= 2\frac{\pi^4}{90} + 2\frac{(2\pi)^4}{6}\sum_{n=1}^{\infty}\sigma_3(n)q^n = \frac{2\pi^4}{2\cdot 3^2\cdot 5}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \\
E_6(\tau) &= \frac{2\pi^6}{3^3\cdot 5\cdot 7}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right), \\
E_8(\tau) &= \frac{2\pi^8}{2\cdot 3^3\cdot 5^2\cdot 7}\left(1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n\right), \\
E_{10}(\tau) &= \frac{2\pi^{10}}{3^5\cdot 5\cdot 7\cdot 11}\left(1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n\right).
\end{aligned}$$

4.2. Discriminant of elliptic curves.

Definition.

- The *Poincaré upper half plane* is defined as

$$\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$$

  which gives a model of non-Euclidean geometry.

- Let k be an integer. Then a function $f(\tau)$ on $\mathbb{H}$ is called a *modular form of weight* k (for $SL_2(\mathbb{Z})$) if $f(\tau)$ satisfies the following conditions

  (1) **Holomorphic condition**. $f(\tau)$ is a holomorphic function of $\tau \in \mathbb{H}$.

  (2) **Automorphic condition**. For any $\tau \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$,

$$f(\gamma(\tau)) := f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau).$$

  (3) **Cusp condition**. $f(\tau)$ is expanded to a nonnegative power series of $q = e^{2\pi\sqrt{-1}\tau}$ as

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n$$

  which is called the *Fourier expansion* of $f(\tau)$.

- Denote by M_k the space of modular forms of weight k.

Exercise 4.2.1.

- We define the linear combination of $f(\tau), g(\tau) \in M_k$ as

$$(af + bg)(\tau) = af(\tau) + bg(\tau) \quad (a, b \in \mathbb{C}).$$

  Then show that M_k becomes a vector space over $\mathbb{C}$.

- We define the product of $f(\tau) \in M_k$ and $g(\tau) \in M_l$ as

$$(fg)(\tau) = f(\tau)g(\tau).$$

  Then show that $(fg)(\tau)$ belongs to M_{k+l}.

Remark.

- Let $f(\tau)$ be a modular form of weight k. Then for any $n \in \mathbb{Z}$, taking $\gamma = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ the automorphic condition (2) implies that $f(\tau + n) = f(\tau)$. On the other hand, $\tau \mapsto e^{2\pi\sqrt{-1}\tau}$ gives a surjective map

$$\varphi : \mathbb{H} \to D^{\times} \stackrel{\text{def}}{=} \{q \in \mathbb{C} \mid 0 < |q| < 1\}$$

such that $\varphi(\tau) = \varphi(\tau')$ if and only if $\tau \in \tau' + \mathbb{Z}$. Therefore, $f(\tau)$ is regarded as a holomorphic function on $D^{\times}$, and hence has a Laurent expansion of q. The cusp condition (3) says that $f(\tau)$ has actually a Taylor expansion of q.

- The space M_k consists of global sections of a certain (automorphic) line bundle on the compactified modular curve

$$\mathbb{H}/SL_2(\mathbb{Z}) \cup \left\{\sqrt{-1}\infty\right\},$$

and hence by Riemann-Roch's theorem, M_k is seen to be finite dimensional. In 4.3, we will show the dimension formula of M_k using the following theorems.

Theorem 4.2. *The space M_0 of modular forms of weight 0 consists of constant functions.*

Theorem 4.3. *The modular form $\Delta(\tau)$ of weight 12 defined as*

$$\Delta(\tau) = \frac{(60E_4(\tau))^3 - 27(140E_6(\tau))^2}{(2\pi)^{12}} = q - 24q^2 + \cdots$$

has no zero on $\mathbb{H}$, namely $\Delta(\tau) \neq 0$ for any $\tau \in \mathbb{H}$.

Proof of Theorem 4.2. First, we show that

$$D \stackrel{\text{def}}{=} \left\{\tau \in \mathbb{H} \;\middle|\; -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2},\ |\tau| \geq 1\right\}$$

is a fundamental domain for $SL_2(\mathbb{Z})$, especially

$$\bigcup_{\gamma \in SL_2(\mathbb{Z})} \gamma(D) = \mathbb{H} \quad \cdots (*).$$

It is clear that the left hand side is contained in the right hand side. For $\tau \in \mathbb{H}$,

$$\left\{|c\tau + d| \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\right\} \subset \left\{|c\tau + d| \;\middle|\; \begin{array}{l} c, d \in \mathbb{Z} \\ (c, d) \neq (0, 0) \end{array}\right\},$$

and hence there exists the value

$$m = \min\left\{|c\tau + d| \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\right\}$$

as a positive real number. Take an element

$$\gamma_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in SL_2(\mathbb{Z})$$

such that $m = |c_0\tau + d_0|$. By Exercise 4.1.2,

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2} \quad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\right),$$

and hence we have

$$\mathrm{Im}(\gamma_0(\tau)) = \max\{\mathrm{Im}(\gamma(\tau)) \mid \gamma \in SL_2(\mathbb{Z})\} \ \cdots (**).$$

Put

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z}),$$

and let n be an integer satisfying

$$n - \frac{1}{2} \leq \mathrm{Re}(\gamma_0(\tau)) \leq n + \frac{1}{2}.$$

If we assume that $|T^{-n}\gamma_0(\tau)| < 1$, then by Exercise 4.1.2,

$$\mathrm{Im}\left(ST^{-n}\gamma_0(\tau)\right) = \frac{\mathrm{Im}\left(T^{-n}\gamma_0(\tau)\right)}{|T^{-n}\gamma_0(\tau)|} > \mathrm{Im}\left(T^{-n}\gamma_0(\tau)\right) = \mathrm{Im}\left(\gamma_0(\tau)\right).$$

which contradicts to $(**)$. Therefore, $|T^{-n}\gamma_0(\tau)| \geq 1$, and hence $T^{-n}\gamma_0(\tau) \in D$. This implies that τ is contained in

$$\gamma_0^{-1}T^n(D) \subset \bigcup_{\gamma \in SL_2(\mathbb{Z})} \gamma(D),$$

and hence $(*)$ holds.

Second, we prove that M_0 consists of constant functions. For an element $f(\tau) \in M_0$, by the automorphic condition (2) and by $(*)$,

$$\{f(\tau) \mid \tau \in \mathbb{H}\} = \{f(\tau) \mid \tau \in D\} = \left\{ f(\tau) \;\middle|\; \mathrm{Im}(\tau) \geq \frac{\sqrt{3}}{2} \right\}.$$

Let $f(q)$ denote $f(\tau)$ which is regarded as a function of q. Then by the above,

$$\{f(q) \mid 0 < |q| < 1\} = \left\{ f(q) \;\middle|\; 0 < |q| \leq e^{-\sqrt{3}\pi} \right\}.$$

Furthermore, by the cusp condition (3), $f(q)$ is holomorphic at $q = 0$, and hence

$$\{f(q) \mid |q| < 1\} = \left\{ f(q) \;\middle|\; |q| \leq e^{-\sqrt{3}\pi} \right\}$$

is a compact set as the image by the continuous function $f(q)$ of the compact set $\left\{ q \in \mathbb{C} \;\middle|\; |q| \leq e^{-\sqrt{3}\pi} \right\}$. Therefore, there exists a complex number q_0 with $|q_0| \leq e^{-\sqrt{3}\pi}$ such that

$$f(q_0) = \max \{ f(q) \mid |q| < 1 \},$$

and hence by the maximum modulus principle in 2.2, $f(q)$ is a constant function. $\square$

Proof of Theorem 4.3. For an element τ of $\mathbb{H}$, let $L = \{m + n\tau \mid m, n \in \mathbb{Z}\}$ be the lattice in $\mathbb{C}$ generated by 1, τ, and let $F(x, y)$ be the polynomial $y^2 - \varphi(x)$, where

$$\varphi(x) = 4x^3 - 60E_4(\tau)x - 140E_6(\tau).$$

Then by Abel's theorem in 3.3, the map

$$z \mapsto \begin{cases} (\wp_L(z), \wp'_L(z)) & (z \in \mathbb{C} - L), \\ \infty & (z \in L) \end{cases}$$

gives an isomorphism from the complex torus $\mathbb{C}/L$ to the elliptic curve

$$\{(x, y) \in \mathbb{C} \times \mathbb{C} \mid F(x, y) = 0\} \cup \{\infty\}.$$

Since $\mathbb{C}/L$ is a smooth manifold, if $F(x, y) = 0$, then

$$\frac{\partial F}{\partial x} = -\varphi'(x), \quad \frac{\partial F}{\partial y} = 2y$$

have no common zero. By the fact that

$$\varphi'(x) = 0,\ y = 0 \ \Leftrightarrow\ \varphi(x) = \varphi'(x) = 0 \ \Leftrightarrow\ x \text{ is a double root of } \varphi = 0,$$

$\varphi(x) = 0$ has no double root, and hence the discriminant of $\varphi(x)$, which is defined as the square of differences of its three roots, is not 0. Therefore, this discriminant given by

$$-27 \left\{ \left(\frac{-140E_6(\tau)}{4} \right)^2 + \frac{4}{27} \left(\frac{-60E_4(\tau)}{4} \right)^3 \right\} = \frac{(2\pi)^{12}}{16} \Delta(\tau)$$

is not 0 for any $\tau \in \mathbb{H}$. $\square$

Fundamental domain for $\Gamma(2)$ given by Gauss.

4.3. Enumeration of modular forms.

Aim. Using Theorems 4.2 and 4.3, we show the following dimension formula.

Theorem 4.4. *Denote by M_k the space of of modular forms of weight k. Then we have*

$$\dim_{\mathbb{C}} M_k = \begin{cases} 0 & (k\text{: odd}), \\ 0 & (k < 0), \\ 1 & (k = 0), \\ 0 & (k = 2), \\ 1 & (k\text{: even, } 4 \le k \le 10), \\ \dim_{\mathbb{C}} M_{k-12} + 1 & (k\text{: even, } k \ge 12). \end{cases}$$

Example.

$$\dim_{\mathbb{C}} M_{100} = \dim_{\mathbb{C}} M_{88} + 1 = \cdots = \dim_{\mathbb{C}} M_{100-12\times 8} + 8 = \dim_{\mathbb{C}} M_4 + 8 = 9.$$

Proof.

- **k: odd.** For $f(\tau) \in M_k$, if $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$, then

$$f(\tau) = f\left(\frac{-\tau + 0}{0 - 1}\right) = f(\gamma(\tau)) = (-1)^k f(\tau) = -f(\tau),$$

  and hence $f(\tau) = 0$ for any $\tau \in \mathbb{H}$. Therefore, $\dim_{\mathbb{C}} M_k = 0$.

- **$k = 0$.** By Theorem 4.2, M_k consists of constant functions, and hence $\dim_{\mathbb{C}} M_k = 1$.

- **$k < 0$.** For $f(\tau) \in M_k$, by Exercise 4.2.1,

$$f(\tau)^{12} \cdot \Delta(\tau)^{-k} \in M_{12\cdot k - k\cdot 12} = M_0 = \{\text{constant functions}\}.$$

  If the Fourier expansion of $f(\tau)$ is represented as $\alpha_n q^n + \cdots$ with nonzero α_n, then

$$f(\tau)^{12} \cdot \Delta(\tau)^{-k} = \alpha_n^{12} q^{12n-k} + \cdots$$

  is not a constant function since $\alpha_n^{12} \neq 0$ and $12n - k > 0$. Therefore, $f(\tau) = 0$ for any $\tau \in \mathbb{H}$, and hence $\dim_{\mathbb{C}} M_k = 0$.

- **k: even, $4 \le k \le 10$.** Since the Eisenstein series $E_k(\tau)$ belongs to M_k,

$$\mathbb{C} \cdot E_k(\tau) \stackrel{\text{def}}{=} \{aE_k(\tau) \mid a \in \mathbb{C}\} \subset M_k.$$

  The Fourier expansion of E_k has the positive constant term

$$2\zeta(k) = 2\sum_{n=1}^{\infty} \frac{1}{n^k},$$

and hence for $f(\tau) \in M_k$ with Fourier expansion $\alpha_0 + \alpha_1 q + \cdots$,

$$f(\tau) - \frac{\alpha_0}{2\zeta(k)} E_k(\tau) \in M_k$$

has the Fourier expansion as $\beta_1 q + \cdots$. As is shown in Theorem 4.3, $\Delta(\tau)$ has no zero on $\mathbb{H}$, and hence the quotient

$$\frac{f(\tau) - \dfrac{\alpha_0}{2\zeta(k)} E_k(\tau)}{\Delta(\tau)} = \beta_1 + \cdots$$

belongs to the space M_{k-12} which becomes $\{0\}$ since $k - 12 < 0$. Therefore,

$$f(\tau) = \frac{\alpha_0}{2\zeta(k)} E_k(\tau) \in \mathbb{C} \cdot E_k(\tau),$$

and hence $M_k = \mathbb{C} \cdot E_k(\tau)$ has dimension 1.

- ***k*: even, $k \geq 12$.** If $f(\tau) = \alpha_0 + \alpha_1 q + \cdots \in M_k$, then as is shown above

$$\left(f(\tau) - \frac{\alpha_0}{2\zeta(k)} E_k(\tau) \right) \Big/ \Delta(\tau) \in M_{k-12}.$$

$$\therefore \ f(\tau) \in \frac{\alpha_0}{2\zeta(k)} E_k(\tau) + \Delta(\tau) \cdot M_{k-12},$$

where

$$\Delta(\tau) \cdot M_{k-12} = \{ \Delta(\tau) \cdot g(\tau) \mid g(\tau) \in M_{k-12} \}.$$

Therefore, $\Delta(\tau) \cdot M_{k-12} + \mathbb{C} \cdot E_k(\tau) = M_k$. Further, by the following Exercise 4.3.1,

$$\dim_{\mathbb{C}} M_k = \dim_{\mathbb{C}} (\Delta(\tau) \cdot M_{k-12}) + \dim_{\mathbb{C}} (\mathbb{C} \cdot E_k(\tau)) = \dim_{\mathbb{C}} M_{k-12} + 1.$$

Exercise 4.3.1. Prove that $\Delta(\tau) \cdot M_{k-12} \cap \mathbb{C} \cdot E_k(\tau) = \{0\}$.

- **$k = 2$.** Let $f(\tau) = \alpha_0 + \alpha_1 q + \cdots$ be an element of M_2. If $\alpha_0 = 0$, then

$$f(\tau)/\Delta(\tau) \in M_{2-12} = M_{-10} = \{0\},$$

and hence $f(\tau)$ is identically 0. If $\alpha_0 \neq 0$, then

$$(f(\tau)/\alpha_0)^2 \in M_4 = \mathbb{C} \cdot E_4(\tau), \quad (f(\tau)/\alpha_0)^3 \in M_6 = \mathbb{C} \cdot E_6(\tau),$$

and hence there are constants c_1, c_2 such that

$$(1 + (\alpha_1/\alpha_0)q + \cdots)^2 = c_1(1+240q+\cdots), \ (1 + (\alpha_1/\alpha_0)q + \cdots)^3 = c_2(1-504q+\cdots).$$

This implies that $c_1 = c_2 = 1$ and that $2(\alpha_1/\alpha_0) = 240$, $3(\alpha_1/\alpha_0) = -504$ which is a contradiction. Therefore, $M_2 = \{0\}$ has dimension 0. $\square$

Exercise 4.3.2. Prove that any element of M_k is represented as a polynomial of $E_4(\tau)$ and $E_6(\tau)$.

Theorem 4.5 (Jacobi). *For $\tau \in \mathbb{H}$, put $q = e^{2\pi\sqrt{-1}\tau}$. Then $\Delta(\tau)$ is equal to Ramanujan's delta function*

$$q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Proof (see [K] for its detail). Put $L = \mathbb{Z} + \mathbb{Z}\tau$, and $\wp(z) = \wp_L(z)$. As is shown in 4-2, if we put $\wp'(z)^2 = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$, then

$$(2\pi)^{12}\Delta(\tau) = \{4(e_1-e_2)(e_1-e_3)(e_2-e_3)\}^2.$$

For $\alpha = 1/2, \tau/2, (1+\tau)/2,\ 2\alpha \in L$, namely $-\alpha \in \alpha + L$, and hence $\wp'(\alpha) = \wp'(-\alpha)$. Since $\wp'(z)$ is an odd function satisfying $\wp'(-\alpha) = -\wp'(\alpha)$, we have $\wp'(\alpha) = 0$. Hence $\wp(\alpha) \in \{e_1, e_2, e_3\}$, and actually $\{e_1, e_2, e_3\} = \{\wp(1/2), \wp(\tau/2), \wp((1+\tau)/2)\}$. Therefore, $\Delta(\tau)$ is expressed as

$$\frac{16}{(2\pi)^{12}}\left\{\wp\left(\frac{1}{2}\right)-\wp\left(\frac{\tau}{2}\right)\right\}^2\left\{\wp\left(\frac{1}{2}\right)-\wp\left(\frac{1+\tau}{2}\right)\right\}^2\left\{\wp\left(\frac{\tau}{2}\right)-\wp\left(\frac{1+\tau}{2}\right)\right\}^2\cdots(\sharp).$$

Put $\zeta = e^{2\pi\sqrt{-1}z}$, and define a theta function as an absolutely convergent product:

$$\theta(\zeta) = (1-\zeta)\prod_{n=1}^{\infty}\frac{(1-q^n\zeta)(1-q^n\zeta^{-1})}{(1-q^n)^2}$$

Then $\theta(\zeta)$ is invariant under $z \mapsto z+1$ ($\Rightarrow \zeta \mapsto \zeta$) and satisfies that

$$\theta(q\zeta) = -\frac{1}{\zeta}\theta(\zeta)$$

under $z \mapsto z+\tau$. Therefore,

$$\zeta_2\frac{\theta(\zeta_1\zeta_2)\theta(\zeta_1\zeta_2^{-1})}{\theta(\zeta_1)^2\theta(\zeta_2)^2}\ \cdots(*1)$$

is invariant under $\zeta_1 \mapsto q\zeta_1$, $\zeta_2 \mapsto q\zeta_2$. Let ζ_1 be a point on $\mathbb{C}^\times - \langle q\rangle$. Then the function $(*1)$ of $\zeta_2 \in \mathbb{C}^\times$ becomes an elliptic function on $\mathbb{C}^\times/\langle q\rangle \cong \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ which has zeros of order 1 at $\zeta_2 = \zeta_1^{\pm 1}q^n$ ($n \in \mathbb{Z}$), and has poles of order 2 at $\zeta_2 = q^n$ ($n \in \mathbb{Z}$). On the other hand, for $z_1 \notin \mathbb{Z}+\mathbb{Z}\tau$, the function

$$\wp(z_1) - \wp(z_2)\ \cdots(*2)$$

of $\zeta_2 = \exp\left(2\pi\sqrt{-1}z_2\right)$ is an elliptic function on $\mathbb{C}^\times/\langle q\rangle \cong \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ which has zero at $\zeta_2 = \zeta_1^{\pm 1}q^n$ ($n \in \mathbb{Z}$), and has poles of order 2 at $\zeta_2 = q^n$ ($n \in \mathbb{Z}$), where $\zeta_1 = \exp\left(2\pi\sqrt{-1}z_1\right)$. Therefore, the function

$$C(z_1, z_2) = \frac{(*2)}{(*1)}$$

of z_2 is a holomorphic elliptic function, and hence is a constant function. In a similar way, one can see that $C(z_1, z_2)$ is also a constant function of z_1. Since

$$\begin{aligned}\lim_{z_2\to 0} z_2^2\cdot(*1) &= \frac{\theta(\zeta_1)\theta(\zeta_1)}{\theta(\zeta_1)^2}\lim_{z_2\to 0}\frac{z_2^2}{(1-e^{2\pi\sqrt{-1}z_2})^2} = \frac{1}{(2\pi\sqrt{-1})^2},\\ \lim_{z_2\to 0} z_2^2\cdot(*2) &= \lim_{z_2\to 0}\left(z_2^2\frac{-1}{z_2^2}\right) = -1\end{aligned}$$

which imply that $C(z_1, z_2) = -\left(2\pi\sqrt{-1}\right)^2 = (2\pi)^2$. Therefore, we have the formula:

$$\wp(z_1)-\wp(z_2) = (2\pi)^2\zeta_2\frac{\theta(\zeta_1\zeta_2)\theta(\zeta_1\zeta_2^{-1})}{\theta(\zeta_1)^2\theta(\zeta_2)^2}$$

which was shown in [Si, Chapter V, Proposition 1.3] using Weierstrass' σ-function. Substituting this formula to (♯), we have

$$\begin{aligned}\Delta(\tau) &= \frac{16}{(2\pi)^{12}}\cdot(2\pi)^{12}q^3\frac{\theta(-q)^2\theta(-q^{-1/2})^2\theta(q^{-1/2})^2}{\theta(-1)^6\theta(q^{1/2})^6\theta(-q^{1/2})^6}\\ &= \frac{16q}{\theta(-1)^4\theta(q^{1/2})^4\theta(-q^{1/2})^4}\\ &= q\prod_{n=1}^{\infty}(1-q^n)^{24}.\end{aligned}$$

This completes the proof. □

Corollary. *The infinite product* $q\prod_{n=1}^{\infty}(1-q^n)^{24}$ $\left(q = e^{2\pi\sqrt{-1}\tau}\right)$ *is a modular form of weight* 12.

Remark. Hurwitz, Siegel and Weil proved this fact directly.

Remark. The function

$$\eta(\tau) = e^{(\pi\sqrt{-1}\tau)/12}\prod_{n=1}^{\infty}\left(1-e^{2\pi\sqrt{-1}n\tau}\right) = \Delta(\tau)^{1/24}$$

is called Dedekind's eta function which becomes a modular form of (half integral) weight 1/2. By Euler's pentagon number theorem,

$$\eta(\tau) = e^{(\pi\sqrt{-1}\tau)/12}\sum_{n=-\infty}^{\infty}(-1)^n e^{\pi\sqrt{-1}(3n^2-n)\tau}.$$

4.4. Application to number theory.

Example 1. By Theorem 4.4, M_8 has dimension 1, and hence is $\mathbb{C}\cdot E_4(\tau)^2$ and $\mathbb{C}\cdot E_8(\tau)$. Since

$$\begin{aligned} E_4(\tau) &= \frac{2\pi^4}{2\cdot 3^2\cdot 5}\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \\ E_8(\tau) &= \frac{2\pi^8}{2\cdot 3^3\cdot 5^2\cdot 7}\left(1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n\right), \end{aligned}$$

there is a nonzero constant c such that

$$1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n = c\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^2.$$

By comparing their constant terms, we have $c=1$, and hence

$$\begin{aligned} 1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n &= \left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^2 \\ &= 1+480\sum_{n=1}^{\infty}\sigma_3(n)q^n+240^2\sum_{n=1}^{\infty}\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m)q^n. \end{aligned}$$

Therefore, comparing their coefficients of q, we have

$$\sigma_7(n)=\sigma_3(n)+120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m).$$

Remark. Without using Theorem 4.4, we have $E_8(\tau)=\frac{3}{7}E_4(\tau)^2$ by Exercise 3.2.2.

Exercise 4.4.1. In a similar way as above, show

$$11\sigma_9(n)=21\sigma_5(n)-10\sigma_3(n)+5040\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m)$$

using

$$\begin{aligned} E_4(\tau) &= \frac{2\pi^4}{2\cdot 3^2\cdot 5}\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \\ E_6(\tau) &= \frac{2\pi^6}{3^3\cdot 5\cdot 7}\left(1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right), \\ E_{10}(\tau) &= \frac{2\pi^{10}}{3^5\cdot 5\cdot 7\cdot 11}\left(1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n\right). \end{aligned}$$

Example 2. Jacobi proved the following formula

$$\left(\sum_{m\in\mathbb{Z}} q^{m^2}\right)^4 = 1 - 32\sum_{4|n}\sigma_1(n/4)q^n + 8\sum_{n=1}^{\infty}\sigma_1(n)q^n$$

which is regarded as an equality between modular forms of weight 2 for $\Gamma(2)$. By this formula, Jacobi showed that for any positive integer n,

$$\sharp\left\{(m_1,m_2,m_3,m_4)\in\mathbb{Z}^4 \;\middle|\; \sum_{i=1}^{4} m_i^2 = n\right\} = 8\left(\sum_{0<d|n,4\nmid d} d\right) > 0,$$

where $\sharp S$ denotes the number of elements of a finite set S.

Example 3. Euler proved that a prime p decomposes in $\mathbb{Q}\left(\sqrt{-1}\right)$ as follows:

- if $p = 2$, then $2 = \sqrt{-1}\left(1-\sqrt{-1}\right)^2$.
- if $p \equiv 1 \bmod(4)$, then $p = \left(a+b\sqrt{-1}\right)\left(a-b\sqrt{-1}\right)$ for certain integers a and b.
- if $p \equiv 3 \bmod(4)$, then p does not decompose and remains prime.

This result is an example of class field theory by Hilbert and Takagi which describes the decomposition rule of prime ideals in abelian extensions in terms of the congruence condition on these prime ideals.

Serre gives an example of nonabelian class field theory which describes the decomposition of prime ideals in nonabelian extensions. More precisely, let L be the decomposition field of $x^3 - x - 1 = 0$. Then L is a Galois extension over $\mathbb{Q}$ whose Galois group is isomorphic to the symmetric group of degree 3, and L contains $K = \mathbb{Q}\left(\sqrt{-23}\right)$. Let

$$\begin{aligned} f(\tau) &= q\prod_{n=1}^{\infty}(1-q^n)\left(1-q^{23n}\right) \\ &= \frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+mn+6n^2} - \sum_{m,n\in\mathbb{Z}} q^{2m^2+mn+3n^2}\right); \quad q = e^{2\pi\sqrt{-1}\tau}. \end{aligned}$$

It is known that $f(\tau)$ is a modular form of weight 1 with level 23. Denote the Fourier expansion of $f(\tau)$ by $\sum_{n=1}^{\infty} a(n)q^n$. Then the ideal (p) of $\mathbb{Q}$ generated by a prime $p \neq 23$ is unramified in L and its decomposition rule is described as follows:

- $a(p) = 2$ if and only if (p) is decomposed completely in K and L, and hence (p) is decomposed to the product of distinct 6 prime ideals of L.
- $a(p) = -1$ if and only if (p) is decomposed to the product of distinct 2 ideals of K which remain prime in L.

- $a(p) = 0$ if and only if (p) remains a prime ideal of K which is decomposed to the product of distinct 3 prime ideals of L.

Ramanujan conjecture. For the coefficients $\tau(m)$ of Ramanujan's delta function defined as

$$\sum_{m=1}^{\infty} \tau(m) q^m = q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

Ramanujan conjectured the followings

(1) If m and n are coprime, then $\tau(mn) = \tau(m)\tau(n)$.

(2) If p is a prime number, then $\tau\left(p^{n+1}\right) = \tau(p)\tau\left(p^n\right) - p^{11}\tau\left(p^{n-1}\right)$.

(3) If p is a prime number, then $|\tau(p)| \leq 2p^{11/2}$.

Later Mordell proved (1) and (2) using a theory of Hecke (Mordell?) operators, and Deligne proved (3) using the Weil conjecture which was also proved by Deligne. More precisely, Deligne applied the Weil conjecture to the modular curve

$$X_\Gamma = \mathbb{H}/\Gamma \cup \{\text{cusps}\} = \left(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})\right)/\Gamma$$

associated with a congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ and to its fiber space whose fibers are products of elliptic curves.

Example. Picture of $X_{SL_2(\mathbb{Z})}$.

Shimura(-Taniyama) conjecture (proved by Wiles and others). For each elliptic curve E over $\mathbb{Q}$, there exists a positive integer N and a surjective morphism $\varphi : X_{\Gamma_0(N)} \to E$, where

$$\Gamma_0(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod(N) \right\}$$

is a congruence subgroup of $SL_2(\mathbb{Z})$. As its applications, we have

- The analytic continuation and functional equation of the L-function of E:

$$\begin{aligned} L(E,s) &= \prod_{p:\text{ good prime}} \left(1 - a_p(E)p^{-s} + p^{1-2s}\right)^{-1} \\ &; \quad a_p(E) = p + 1 - \sharp\left(E(\mathbb{Z}/p\mathbb{Z})\right). \end{aligned}$$

- The Gross-Zagier formula contributes the Birch and Swinnerton-Dyer conjecture:

$$\text{Rank of } E(\mathbb{Q}) = \text{Order of } L(E,s) \text{ at } s = 1.$$

- Proof of the Fermat conjecture (see 1.1).

§5. Infinite products in modern mathematics

5.1. Moonshine (nonsense?) conjecture and Borcherds product.

Infinite product on the modular function. Since

$$\frac{45}{\pi^4}E_4(\tau) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,\ \Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \quad (q = e^{2\pi i\tau})$$

are modular forms of weight 4, 12 respectively,

$$\begin{aligned} j(\tau) &= \frac{\left(\frac{45}{\pi^4}E_4(\tau)\right)^3}{\Delta(\tau)} = q^{-1}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3\prod_{n=1}^{\infty}\left(1+q^n+q^{2n}+\cdots\right)^{24} \\ &= q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 \\ &\quad + 333202640600q^5 + 4252023300096q^6 + 44656994071935q^7 + \cdots \end{aligned}$$

is a modular function, namely satisfies that

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau) \ \text{ for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Remark. $j(\tau)$ is equal to an invariant (called the j-invariant) of the isomorphism classes containing the elliptic curves

$$y^2 = 4x^3 - 60E_4(\tau)x - 140E_6(\tau).$$

Theorem 5.1. *Put $j(q) = \sum_{n=-1}^{\infty}c(n)q^n$. Then for independent variables p and q,*

$$\textbf{(B1)} \qquad j(p) - j(q) = \left(\frac{1}{p} - \frac{1}{q}\right)\prod_{m,n=1}^{\infty}(1-p^mq^n)^{c(mn)}.$$

This formula was proved independently in the 1980's by Koike, Norton and Zagier.

Calculation of (B1). Multiplying the both sides of **(B1)** by

$$\frac{1}{1/p - 1/q} = -\frac{pq}{p-q},$$

we have

$$\begin{aligned} \textbf{(B1')} \qquad & 1 - c(1)pq - c(2)\left(p^2q + pq^2\right) - c(3)\left(p^3q + p^2q^2 + pq^3\right) - \cdots \\ & - c(n)\left(p^nq + p^{n-1}q^2 + \cdots + pq^n\right) - \cdots \\ = \ & (1-pq)^{c(1)}\left(1-p^2q\right)^{c(2)}\left(1-pq^2\right)^{c(2)}\left(1-p^3q\right)^{c(3)}\left(1-pq^3\right)^{c(3)} \\ & \times\left(1-p^4q\right)^{c(4)}\left(1-p^2q^2\right)^{c(4)}\left(1-pq^4\right)^{c(4)}\left(1-p^5q\right)^{c(5)}\left(1-pq^5\right)^{c(5)}\cdots. \end{aligned}$$

Therefore, by comparing the coefficients of p^2q^2 in

$$\begin{aligned}\cdots - c(3)\left(p^3q + p^2q^2 + pq^3\right) - \cdots &= (1-pq)^{c(1)} \cdots \left(1-p^2q^2\right)^{c(4)} \cdots \\ &= \left(1 - c(1)pq + \frac{c(1)(c(1)-1)}{2}p^2q^2 + \cdots\right) \\ &\quad \times \left(1 - c(4)p^2q^2 + \cdots\right) \cdots,\end{aligned}$$

we have

$$\begin{aligned}-c(3) &= -c(4) + \frac{c(1)(c(1)-1)}{2}. \\ \therefore -864,299,970 &= -20,245,856,256 + \frac{196,884 \times 196,883}{2}.\end{aligned}$$

Exercise 5.1.1. By comparing the coefficients of p^3q^2 in the both sides of **(B1')**, show

$$\begin{aligned}-c(4) &= -c(6) + c(1)c(2). \\ \therefore -20,245,856,256 &= -4,252,023,300,096 + 196,884 \times 21,493,760.\end{aligned}$$

Theorem 5.2 (Recurrence of $c(n)$). *Assume that Theorem 5.1 holds. Then for any $n \geq 6$, $c(n)$ is expressed as a polynomial over $\mathbb{Z}$ of $c(m)$ $(0 < m < n)$. Consequently, for any $n \geq 1$, any $c(n)$ is expressed as a polynomial over $\mathbb{Z}$ of $c(1), c(2), ..., c(5)$.*

Proof. First, comparing the coefficients of p^nq^2 $(n \geq 2)$ in **(B1')**,

$$-c(n+1) = -c(2n) + \text{a polynomial over } \mathbb{Z} \text{ of } c(m)\ (0 < m < n),$$

and hence when $n \geq 2$ $(\Rightarrow 2n \geq 4)$, $c(2n)$ is expressed as a polynomial over $\mathbb{Z}$ of $c(m)$ $(0 < m < 2n)$. Furthermore, comparing the coefficients of $p^{2n}q^2$, p^nq^4 and of p^mq^3 $(0 < m < n)$ in **(B1')**, we have

$$\begin{cases} -c(2n+1) &= -c(4n) + \text{a polynomial over } \mathbb{Z} \text{ of } c(m)\ (0 < m < 2n), \\ -c(n+3) &= -c(4n) + \text{a polynomial over } \mathbb{Z} \text{ of } c(m), c(2m), c(3m)\ (0 < m < n), \\ -c(m+2) &= -c(3m) + \text{a polynomial over } \mathbb{Z} \text{ of } c(l), c(2l)\ (0 < l < m), \end{cases}$$

and hence

$$c(2n+1) = c(n+3) + \text{a polynomial over } \mathbb{Z} \text{ of } \begin{cases} c(m) & (0 < m < 2n), \\ c(2l), c(l+2) & (0 < l < n). \end{cases}$$

Therefore, when $n \geq 3$ $(\Rightarrow 2n+1 \geq 7)$, $c(2n+1)$ is expressed as a polynomial over $\mathbb{Z}$ of $c(m)$ $(0 < m < 2n+1)$. $\square$

Monster group. Finite simple groups are shown to be one of the followings:

- Cyclic groups of prime order,

- Alternative groups of degree ≥ 5 (Galois),
- Certain matrix groups over finite fields (Chevalley, Suzuki,...),
- 26 Sporadic groups which are not the above groups.

The monster group is the sporadic simple group with maximal order (54 bits), and the sizes of its irreducible representations are

$$d_1 = 1, \quad d_2 = 196883, \quad d_3 = 21296876, ...$$

Then Mckay and Thompson found that d_n are related with certain Fourier coefficients $c(n)$ of $j(\tau)$ as

$$c(1) = d_1 + d_2, \quad c(2) = d_1 + d_2 + d_3, ...$$

Moonshine conjecture (proved by Borcherds (1992) based on Conway-Norton's work). There is a sequences $\{H_n\}$ of representations of the monster group M such that for each $g \in M$,

$$J_g(\tau) = \sum_{n=-1}^{\infty} \text{Trace}\,(g|_{H_n})\, e^{2\pi\sqrt{-1}n}$$

is a modular function. Especially, if $g = 1$, then $J_1(\tau) = j(\tau) + \text{constant}$, and hence $\dim H_n = c(n)$.

Idea of the proof. By the denominator formula of the characters of an infinite dimensional Lie algebra associated to M, we have the same infinite product on $J_1(\tau)$ as for $j(\tau)$. Then by the recurrence of $J_1(\tau)$ and $j(\tau)$, $J_1(\tau) = j(\tau) + \text{constant}$.

5.2. Proof of Borcherds product.

Proposition 5.3. *For a positive integer n, put*

$$T(n) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \;\middle|\; \begin{array}{l} a,b,c,d \in \mathbb{Z}, \\ ad - bc = n \end{array} \right\}.$$

Then we have the followings:

(1) *For any $\gamma \in SL_2(\mathbb{Z})$, $\varphi_\gamma(\alpha) = \alpha\gamma$ $(\alpha \in T(n))$ gives a bijection $\varphi_\gamma : T(n) \xrightarrow{\sim} T(n)$.*

(2) *Define a subset of $T(n)$ as*

$$\Delta(n) = \left\{ \left(\begin{array}{cc} a & b \\ 0 & d \end{array} \right) \in T(n) \;\middle|\; \begin{array}{l} a,b > 0, \\ 0 \le b < d \end{array} \right\}.$$

Then any element α of $T(n)$ is uniquely expressed as

$$\alpha = \gamma \cdot \beta \;\; (\beta \in \Delta(n),\; \gamma \in SL_2(\mathbb{Z}))\,,$$

namely, there exists a unique element $(\beta, \gamma) \in \Delta(n) \times SL_2(\mathbb{Z})$ satisfying $\alpha = \gamma \cdot \beta$.

(3) *Let γ be an element of $SL_2(\mathbb{Z})$. Then for any $\beta \in \Delta(n)$, there exists an element $(\beta', \gamma') \in \Delta(n) \times SL_2(\mathbb{Z})$ such that $\beta\gamma = \gamma'\beta'$. Furthermore, $\beta \mapsto \beta'$ gives a bijection $\psi_\gamma : \Delta(n) \xrightarrow{\sim} \Delta(n)$.*

Exercise 5.2.1. Prove (1).

Proof. First, we show the uniqueness in (2). Assume that $\beta, \beta' \in \Delta(n)$ and $\gamma, \gamma' \in SL_2(\mathbb{Z})$ satisfy $\gamma\beta = \gamma'\beta'$. Then $(\gamma')^{-1}\gamma \in SL_2(\mathbb{Z})$ and $(\gamma')^{-1}\gamma\beta = \beta'$. Put

$$(\gamma')^{-1}\gamma = \left(\begin{array}{cc} x & y \\ z & w \end{array} \right), \quad \beta = \left(\begin{array}{cc} a & b \\ 0 & d \end{array} \right), \quad \beta' = \left(\begin{array}{cc} a' & b' \\ 0 & d' \end{array} \right).$$

Then

$$\left(\begin{array}{cc} ax & bx + dy \\ az & bz + dw \end{array} \right) = \left(\begin{array}{cc} a' & b' \\ 0 & d' \end{array} \right),$$

and hence $az = 0$, $ax = a'$, $bz + dw = d'$. Since $a, a', d, d' > 0$, we have $z = 0$ and $x > 0$. Therefore, the integers x, w satisfy $xw = 1$, hence $x = w = 1$, $a = a'$ and $d = d'$. Then $b + dy = b'$ and $d|y| = |b - b'|$. Since $0 \le b, b' < d$ and $y \in \mathbb{Z}$, we have $y = 0$, and hence

$$(\gamma')^{-1}\gamma = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right).$$

This implies $\gamma = \gamma'$ and $\beta = \beta'$.

Second, we show the existence in (2). Put

$$\alpha = \begin{pmatrix} s & t \\ u & v \end{pmatrix}, \quad \beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad \gamma = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.$$

Since $\beta \in \Delta(n)$, $\gamma \in SL_2(\mathbb{Z})$ and $\alpha = \gamma\beta$, we may find integers a, b, d, x, y, z, w satisfying

(A) $a, d > 0$, $ad = n$, $0 \leq b < d$.

(B) $xy - yz = 1$.

(C) $\begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} ax & bx + dy \\ az & bz + dw \end{pmatrix}$.

By (B), x, z are coprime, and hence

$$a = \gcd(ax, az) \overset{\text{(C)}}{=} \gcd(s, u)$$

which is a divisor of $sv - tu = n$. Therefore, d, x, z are determined as

$$d \overset{\text{(A)}}{=} \frac{n}{a}, \quad x \overset{\text{(C)}}{=} \frac{s}{a}, \quad z \overset{\text{(C)}}{=} \frac{u}{a}.$$

Since x, z are coprime, there are integers y', w' such that $xw' - y'z = 1$ from which we will construct integers y, w satisfying (C). Multiplying this equality by $n = ad$, we have $axdw' - dy'az = n$, and hence by (C), $sdw' - dy'u = n$. Therefore, from the fact that $sv - tu = n$, we have $s(v - dw') = u(t - dy')$ which implies $x(v - dw') = z(t - dy')$ by (C). Since x, z are coprime, there is an integer m satisfying $v - dw' = mz$ and $t - dy' = mx$, and hence one can take integers q, b such that $m = qd + b$ $0 \leq b < d$. Then $t = mx + dy' = bx + d(y' + qx)$ and $v = mz + dw' = bz + d(w' + qz)$. Therefore, the above a, b, d, x, z and $y = y' + qx$, $w = w' + qz$ satisfy (A)–(C).

Finally, we prove (3). By (2), we have

$$T(n) = \bigsqcup_{\beta \in \Delta(n)} SL_2(\mathbb{Z}) \cdot \beta,$$

and hence by (1), for any $\gamma \in SL_2(\mathbb{Z})$,

$$T(n) = \varphi_\gamma(T(n)) = \bigsqcup_{\beta \in \Delta(n)} SL_2(\mathbb{Z}) \cdot \beta\gamma = \bigsqcup_{\beta \in \Delta(n)} SL_2(\mathbb{Z}) \cdot \psi_\gamma(\beta).$$

Therefore,

$$\bigsqcup_{\beta \in \Delta(n)} SL_2(\mathbb{Z}) \cdot \psi_\gamma(\beta) = T(n) = \bigsqcup_{\beta \in \Delta(n)} SL_2(\mathbb{Z}) \cdot \beta,$$

and hence ψ_γ is a bijection. $\square$

Proof of **(B1)** (following Asai's talk in Algebra Symposium). Put $j_1(\tau) = j(\tau) - 744$, and for each integer $m > 1$, using the Hecke operator define $j_m(\tau)$ as

$$j_m(\tau) = \sum_{\beta \in \Delta(m)} j_1(\beta(\tau)) = \sum_{ad=m, 0 \leq b < d} j_1\left(\frac{a\tau + b}{d}\right).$$

Since $\tau \in \mathbb{H} \Rightarrow (a\tau + b)/d \in \mathbb{H}$, $j_m(\tau)$ is a holomorphic function on $\mathbb{H}$, and by Proposition 5.3, for any $\gamma \in SL_2(\mathbb{Z})$,

$$j_m(\gamma(\tau)) = \sum_{\beta \in \Delta(m)} j_1(\beta \cdot \gamma(\tau)) = \sum_{\beta \in \Delta(m)} j_1(\gamma' \cdot \psi_\gamma(\beta)(\tau)),$$

where $\psi_\gamma(\beta) \in \Delta(m)$, $\gamma' \in SL_2(\mathbb{Z})$ such that $\beta \cdot \gamma = \gamma' \cdot \psi_\gamma(\beta)$. Since $j_1(\tau)$ is a modular function, namely

$$j_1(\gamma' \cdot \psi_\gamma(\beta)(\tau)) = j_1(\psi_\gamma(\beta)(\tau)),$$

and hence

$$j_m(\gamma(\tau)) = \sum_{\beta \in \Delta(m)} j_1(\psi_\gamma(\beta)(\tau)) = j_m(\tau).$$

Therefore, $j_m(\tau)$ is also a modular function. Let

$$j_m(\tau) = \sum_{n \in \mathbb{Z}} c_m(n) q^n$$

denote the Fourier expansion. Then

$$c_1(n) = \begin{cases} c(n) & (n = -1, n > 0), \\ 0 & (n < -1, n = 0), \end{cases}$$

and

$$\begin{aligned} j_m(\tau) &= \sum_{ad=m} \sum_{b=0}^{d-1} c_1(n) \exp\left(2\pi\sqrt{-1}\frac{a\tau + b}{d} n\right) \\ &= \sum_{n=-1}^{\infty} c_1(n) \sum_{ad=m} \exp\left(2\pi\sqrt{-1}\frac{an}{d}\tau\right) \sum_{b=0}^{d-1} \exp\left(2\pi\sqrt{-1}\frac{bn}{d}\right). \end{aligned}$$

Since $d = m/a$ and

$$\sum_{b=0}^{d-1} \exp\left(2\pi\sqrt{-1}\frac{bn}{d}\right) = \begin{cases} d & (\text{if } n \text{ is a multiple of } d), \\ 0 & (\text{otherwise}), \end{cases}$$

by putting $l = (a^2 n)/m$, we have

$$\begin{aligned} j_m(\tau) &= \sum_{n=-1}^{\infty} c_1(n) \sum_{a|m,\ m|na} \frac{m}{a} \exp\left(2\pi\sqrt{-1}\frac{a^2 n}{m}\tau\right) \\ &= \sum_{l \in \mathbb{Z}} c_1\left(\frac{ml}{a^2}\right) \sum_{a|m,\ a|l} \frac{m}{a} \exp\left(2\pi\sqrt{-1} l \tau\right). \end{aligned}$$

Therefore,

$$c_m(l) = \sum_{a|m,\ a|l} \frac{m}{a} c_1\left(\frac{ml}{a^2}\right). \quad \therefore\ c_m(1) = m \cdot c_1(m) = m \cdot c(m) \cdots (*),$$

and hence

- if $l < -m$, then
$$\frac{ml}{a^2} < -\frac{m^2}{a^2} \leq -1$$
which implies that $c_1\left((ml)/a^2\right) = 0$, and hence $c_m(l) = 0$,
- if $l = -m$, then
$$\frac{ml}{a^2} = -\frac{m^2}{a^2} \leq -1 \ \text{(the equality holds} \Leftrightarrow a = m)$$
which implies that $c_m(l) = c_1(-1) = 1$,
- if $-m < l \leq 0$, then
$$\frac{ml}{a^2} = \frac{(-m)(-l)}{a^2} < -\frac{l^2}{a^2} \leq -1$$
which implies that $c_1\left((ml)/a^2\right) = 0$, and hence $c_m(l) = 0$.

Therefore, $j_m(\tau)$ has a pole of order m at $q = 0$, and hence there exists a polynomial φ_m of degree m such that

$$j_m(\tau) - \varphi_m(j(\tau)) = O(q)$$

which is a modular form of weight 0, and hence is a constant function as is shown in 4-3. Since this function is 0 at $q = 0$, $j_m(\tau) = \varphi_m(j(\tau))$. Therefore,

$$\begin{aligned} j(\tau) &= q^{-1} + \sum_{l=0}^{m} c(m-l) q^{m-l} + O(q^{m+1}), \\ \varphi_m(j(\tau)) &= q^{-m} + c_m(1)q + O(q^2) \overset{(*)}{=} q^{-m} + mc(m)q + O(q^2), \end{aligned}$$

and hence by putting $\varphi_0 = 1$,

$$\begin{aligned} j(\tau)\varphi_m(j(\tau)) &= q^{-m-1} + \sum_{l=0}^{m} c(m-l) q^{-l} + mc(m) + O(q) \\ &= \varphi_{m+1}(j(\tau)) + \sum_{l=0}^{m} c(m-l)\varphi_l(j(\tau)) + mc(m) + O(q). \end{aligned}$$

By the same reason as above, putting $j = j(\tau) = j(q)$,

$$j \cdot \varphi_m(j) = \varphi_{m+1}(j) + \sum_{l=0}^{m} c(m-l)\varphi_l(j) + mc(m),$$

and hence for a variable p,

$$mc(m)p^m = j\cdot\varphi_m(j)p^m - \varphi_{m+1}(j)p^m - \sum_{l=0}^{m} c(m-l)p^{m-l}\varphi_l(j)p^l.$$

By taking the sum over $m \geq 1$ of the above equality,

$$\begin{aligned}
\sum_{m=1}^{\infty}\mathrm{LHS} &= p\frac{d}{dp}\left(j(p)-p^{-1}\right) = p\frac{d}{dp}j(p)+p^{-1},\\
\sum_{m=1}^{\infty}\mathrm{RHS} &= j\sum_{m=1}^{\infty}\varphi_m(j)p^m - p^{-1}\sum_{m=1}^{\infty}p^m + \varphi_1(j)\\
&\quad - \left(j(p)-p^{-1}\right)\left(1+\sum_{m=1}^{\infty}\varphi_m(j)p^m\right) + c(0)\varphi_0(j)\\
&= \left(j-j(p)\right)\left(1+\sum_{m=1}^{\infty}\varphi_m(j)p^m\right) + p^{-1}
\end{aligned}$$

since $\varphi_1(j) = j - 744$ and $c(0)\varphi_0(j) = 744$. Therefore,

$$p\frac{d}{dp}j(p) = \left(j-j(p)\right)\left(1+\sum_{m=1}^{\infty}\varphi_m(j)p^m\right),$$

and hence

$$\frac{d\log(p(j(p)-j))}{dp} = p^{-1} + \frac{1}{j(p)-j}\frac{dj(p)}{dp} = \frac{d}{dp}\left(-\sum_{m=1}^{\infty}\frac{\varphi_m(j)}{m}p^m\right).$$

Since $\log(p(j(p)-j)) = \log(1+p(j(p)-p^{-1}-j)) = O(p)$,

$$\log(p(j(p)-j(q))) = -\sum_{m=1}^{\infty}\frac{\varphi_m(j(q))}{m}p^m.$$

By $(*)$,

$$\varphi_m(j(q)) = j_m(q) = \sum_{n\in\mathbb{Z}}c_m(n)q^n = \sum_{n}\sum_{a|m,\ a|n}\frac{m}{a}c_1\left(\frac{mn}{a^2}\right)q^n,$$

and hence

$$\begin{aligned}
\log(p(j(p)-j(q)) &= -\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\sum_{a|m,\ a|n}\frac{1}{a}c_1\left(\frac{mn}{a^2}\right)p^mq^n\\
&= \sum_{m=1}^{\infty}\sum_{n=-1}^{\infty}\sum_{a=1}^{\infty}-\frac{1}{a}c_1(mn)p^{ma}q^{na}\\
&\quad \text{(replacing } m/a,\ n/a \text{ with } m,\ n \text{ respectively)}\\
&= \sum_{m=1}^{\infty}\sum_{n=-1}^{\infty}c_1(mn)\log\left(1-p^mq^n\right).
\end{aligned}$$

Therefore,

$$\begin{aligned} j(p) - j(q) &= p^{-1} \prod_{m\geq 1,\ n\geq -1} (1 - p^m q^n)^{c_1(mn)} \\ &= p^{-1} \left(1 - pq^{-1}\right)^{c_1(-1)} \prod_{m,n=1}^{\infty} (1 - p^m q^n)^{c_1(mn)} \\ &= \left(p^{-1} - q^{-1}\right) \prod_{m,n\geq 1}^{\infty} (1 - p^m q^n)^{c(mn)}. \end{aligned}$$

This completes the proof. □

Theory of Hecke operators.

- For each $m \in \mathbb{N}$ and $f(\tau) \in M_k = \{\text{modular forms of weight } k\}$,

$$(T(m)f)(\tau) = m^{k-1} \sum_{ad=m, 0\leq b<d} f\left(\frac{a\tau + b}{d}\right) d^{-k} \in M_k.$$

  Therefore, $T(m)$ gives a $\mathbb{C}$-linear endomorphism on M_k.

- By the property of products of double coset classes over $SL_2(\mathbb{Z})$, we have

$$\begin{cases} \gcd(m,n) = 1 & \Rightarrow \quad T(mn) = T(m)T(n), \\ p\text{: prime} & \Rightarrow \quad T\left(p^{n+1}\right) = T(p)T\left(p^n\right) - p^{k-1}T\left(p^{n-1}\right). \end{cases}$$

- If $f(\tau) = \sum_{n=0}^{\infty} a_n q^n \in M_k$ is a cusp form, i.e., $a_0 = 0$, then $(T(m)f)(\tau) = a_m q + \cdots$.

From these facts and that the space of cusp forms in M_{12} is spanned by the Ramanujan delta function $\Delta(\tau) = \sum_{n=1}^{\infty} \tau(n) q^n$ (cf. Theorem 4.4), one can see that $(T(n)\Delta)(\tau) = \tau(n)\Delta(\tau)$ for any $n \in \mathbb{N}$, and that the Ramanujan conjecture (1), (2) in 4.4 holds. Furthermore, the zeta (L-)function $L(\Delta, s) = \sum_{n=1}^{\infty} \tau(n) n^{-s}$ of $\Delta(\tau)$ has the infinite product, called the Euler product

$$\prod_{p:\text{prime}} \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}$$

which is an analog of that of the Riemann zeta function $\sum_{n=1}^{\infty} n^{-s} = \prod_{p:\text{prime}} (1 - p^{-s})^{-1}$.

5.3. Modular forms and Borcherds product.

Aim. Using **(B1)**, we give an example of infinite product of modular forms.

Exercise 5.3.1. If $f(\tau)$ is a holomorphic function on $\mathbb{H}$ and satisfies $f(\gamma(\tau)) = f(\tau)$ for any $\gamma \in SL_2(\mathbb{Z})$, then

$$g(\tau) = \frac{df(\tau)}{d\tau}$$

a holomorphic function on $\mathbb{H}$ and satisfies

$$g(\gamma(\tau)) = (c\tau + d)^2 g(\tau) \quad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\right).$$

Since $j(\gamma(\tau)) = j(\tau)$ for any $\gamma \in SL_2(\mathbb{Z})$ and $j(q) = q^{-1} + \cdots$, by Exercise 5.3.1,

$$h(\tau) = -\frac{1}{2\pi\sqrt{-1}} \frac{dj(\tau)}{d\tau} = -q\frac{dj(q)}{dq}$$

is a holomorphic function on $\mathbb{H}$ with automorphic condition of weight 2 and is expanded as $q^{-1} + \cdots$. On the other hand, since $E_{14}(\tau)/(2\zeta(14)) = 1 + O(q)$, $\Delta(\tau) = q + O(q^2)$ are modular forms of weight 14, 12 respectively,

$$\frac{E_{14}(\tau)}{2\zeta(14)\Delta(\tau)} = q^{-1} + \cdots$$

has the same properties as for $h(\tau)$. Therefore,

$$\frac{E_{14}(\tau)}{2\zeta(14)\Delta(\tau)} - h(\tau)$$

is a modular form of weight 2 which is 0 by Theorem 4.4, and hence

$$\frac{E_{14}(\tau)}{2\zeta(14)\Delta(\tau)} = h(\tau) = -q\frac{dj(q)}{dq}.$$

Dividing $p - q$ of the both sides of **(B1)** and letting $p = q$, i.e., taking the derivatives by q,

$$\begin{aligned} \frac{d}{dq} j(q) &= \left(\frac{p^{-1} - q^{-1}}{p - q}\right)\Big|_{p=q} \prod_{m,n\geq 1} \left(1 - q^{m+n}\right)^{c(mn)} \\ &= -\frac{1}{q^2} \prod_{l\geq 2} \left(1 - q^l\right)^{b(l)}; \quad b(l) \stackrel{\text{def}}{=} \sum_{m,n\geq 1,\ m+n=l} c(mn), \end{aligned}$$

and hence

$$\frac{E_{14}(\tau)}{2\zeta(14)\Delta(\tau)} = -q\frac{dj(q)}{dq} = q^{-1} \prod_{l=2}^{\infty} \left(1 - q^l\right)^{b(l)}.$$

We define a theta series as

$$\theta(2\tau) = \sum_{m\in\mathbb{Z}} e^{2\pi\sqrt{-1}m^2\tau} = \sum_{m\in\mathbb{Z}} q^{m^2},$$

and put

$$\sum_{l=-4}^{\infty} a(l)q^l = (j(4\tau) - 744)\theta(2\tau) = \sum_{n=-1}^{\infty}\sum_{m\in\mathbb{Z}} c_1(n)q^{4n+m^2}.$$

Then for any $l > 0$,

$$a\left(l^2\right) = \sum_{4n+m^2=l^2} c_1(n) = \sum_{m\in\mathbb{Z}} c_1\left(\frac{l+m}{2}\frac{l-m}{2}\right) = \sum_{m,n\geq 1,\ m+n=l} c(mn) = b(l),$$

and hence

$$\frac{E_{14}(\tau)}{2\zeta(14)} = \Delta(\tau)q^{-1}\prod_{l=1}^{\infty}\left(1-q^l\right)^{a(l^2)} = \prod_{l=1}^{\infty}\left(1-q^l\right)^{a(l^2)+24}.$$

This is a special case of the following Borcherds correspondence:

Theorem 5.4 (Proof is omitted). *Let $f(\tau) = \sum_{n\in\mathbb{Z}} a(n)q^n$ be a "modular form" of weight $1/2$ such that $a(n) \in \mathbb{Z}$ and that $a(n) = 0$ if $n \equiv 2, 3 \bmod(4)$. Then there exists an integer h such that*

$$\Psi_f(\tau) = q^h\prod_{n=1}^{\infty}(1-q^n)^{a(n^2)}$$

becomes a modular form.

Examples.

- $f(\tau) = 12\theta(2\tau) = 12 + \sum_{n=1}^{\infty} 24q^{n^2}$
  $\Rightarrow \Psi_f(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \Delta(\tau)$.
- $f(\tau) = (j(4\tau) - 732)\theta(2\tau) = (j(4\tau) - 744)\theta(2\tau) + 12\theta(2\tau)$
  $\Rightarrow \Psi_f(\tau) = \dfrac{E_{14}(\tau)}{2\zeta(14)\Delta(\tau)}\Delta(\tau) = \dfrac{E_{14}(\tau)}{2\zeta(14)}$.
- Other examples of $\Psi_f(\tau)$: $j(\tau)$, $E_k(\tau)/(2\zeta(k))$ $(k = 4, 6, 8, 10)$.

5.4. Borcherds lifts.

Aim. Using infinite products called Borcherds products, we construct modular forms of many variables with applications to

- Proof of the Moonshine conjecture that the character of the Monster group becomes a modular function,
- Construction of Jacobi forms,
- Construction of modular forms associated with $O(n, 2)$.

Merit. We can construct modular forms whose zeros and poles are explicitly given.

Definition. For a positive integer N, a map $a : \mathbb{R}^N \to \mathbb{Z}$ is a *vector system* if the following conditions are satisfied:

- $R \stackrel{\text{def}}{=} \{l \in \mathbb{R}^N \mid a(l) \neq 0\}$ is a finite set,
- $L \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{Z}}(R)$ is a lattice of $\mathbb{R}^N$ with rank N,
- For any $l \in R$, $a(l) = a(-l)$,
- $\mu \stackrel{\text{def}}{=} \dfrac{\sum_{l \in R} a(l)\langle v, l\rangle^2}{2\langle v, v\rangle}$ is independent of $v \in \mathbb{R}^N - \{0\}$.

Construction of Jacobi forms. For a vector system $a : \mathbb{R}^N \to \mathbb{Z}$, take a subset R^+ of R such that

$$R^+ \cup (-R^+) = R - \{0\},\ R^+ \cap (-R^+) = \emptyset,$$

and put

$$\rho \stackrel{\text{def}}{=} \sum_{l \in R^+} a(l) l \in \mathbb{R}^N,\ d \stackrel{\text{def}}{=} \sum_{l \in R} a(l) \in \mathbb{Z}.$$

Then a Jacobi form $\varphi_a(\tau, z)$ is defined as a function of $(\tau, z) \in \mathbb{H} \times \mathbb{C}^N$ by

$$\varphi_a(\tau, z) \stackrel{\text{def}}{=} q^{d/24} \zeta^{-\rho/2} \prod_{(n,l)>0} \left(1 - q^n \zeta^l\right)^{a(l)},$$

where

$$\begin{aligned} q^n &\stackrel{\text{def}}{=} \exp(2\pi\sqrt{-1} n\tau)\ (n \in \mathbb{R}), \\ \zeta^l &\stackrel{\text{def}}{=} \exp\left(2\pi\sqrt{-1}\langle l, z\rangle\right)\ (l \in \mathbb{R}^N), \\ (n, l) > 0 &\stackrel{\text{def}}{\Leftrightarrow} n \in \mathbb{N}, l \in R \text{ or } n = 0, l \in R^+. \end{aligned}$$

Theorem 5.5 (Borcherds,...) (Proof is omitted). *$\varphi_a(\tau, z)$ is a holomorphic function on $\mathbb{H}\times\mathbb{C}$ called a Jacobi form. In particular, if φ_a is holomorphic at cusps and $a(0) = N$, then*

$$\varphi_a(\tau, z) = \sum_{v\in(L-\rho/2)/\mu L^*} c_v\theta_v(\tau, z);\ \textit{i.e., infinite product = infinite sum}$$

for certain constants c_v and theta functions

$$\theta_v(\tau, z) \stackrel{\text{def}}{=} \sum_{x\in L^*} (-1)^{\langle x,\rho\rangle} q^{\langle v+\mu x, v+\mu x\rangle/(2\mu)}\zeta^{v+\mu x}.$$

Example 1. Put $N = 1$, $R = \{0, \pm 1\}$, $a(0) = a(\pm 1) = 1$. Then

$$L = \mathbb{Z},\ \mu = 1,\ R^+ = \{1\},\ \rho = 1,\ d = 3,$$

and hence by the theorem, there is a constant c such that

$$\begin{aligned}\varphi_a(\tau, z) &= q^{1/8}\zeta^{-1/2}(1-\zeta)\prod_{n=1}^{\infty}(1-q^n)(1-q^n\zeta)(1-q^n\zeta^{-1})\\ &= c\sum_{x\in\mathbb{Z}}(-1)^x q^{\langle -1/2+x,-1/2+x\rangle/2}\zeta^{-1/2+x}\\ &= c\sum_{m\in\mathbb{Z}}(-1)^{m+1}q^{\frac{1}{2}(m+\frac{1}{2})^2}\zeta^{m+\frac{1}{2}}.\end{aligned}$$

Since the coefficients of $q^{1/8}$ of the left and right hand sides are

$$\zeta^{-1/2}(1-\zeta) \text{ and } c(-\zeta^{1/2}+\zeta^{-1/2})$$

respectively, we have $c = 1$. Therefore,

$$q^{1/8}\zeta^{-1/2}(1-\zeta)\prod_{n=1}^{\infty}(1-q^n)(1-q^n\zeta)(1-q^n\zeta^{-1}) = \sum_{m\in\mathbb{Z}}(-1)^{m+1}q^{\frac{1}{2}(m+\frac{1}{2})^2}\zeta^{m+\frac{1}{2}}.$$

Exercise 5.4.1. Show Jacobi's triple product identity by substituting $\zeta \mapsto -q^{1/2}\zeta$ in the above formula.

Example 2. Put $N = 1$, $R = \{0, \pm 1, \pm 2\}$, $a(0) = 1$, $a(\pm 1) = -1$, $a(\pm 2) = 1$. Then

$$L = \mathbb{Z},\ \mu = \frac{-2+8}{2} = 3,\ R^+ = \{1, 2\},\ \rho = 1,\ d = 1,$$

and hence

$$\varphi_a(\tau, z) = q^{1/24}\zeta^{-1/2}\frac{1-\zeta^2}{1-\zeta}\prod_{n=1}^{\infty}\frac{(1-q^n)(1-q^n\zeta^2)(1-q^n\zeta^{-2})}{(1-q^n\zeta)(1-q^n\zeta^{-1})}.$$

Since

$$\Big(L-\frac{\rho}{2}\Big)\Big/\mu L^* \;=\; \Big(\mathbb{Z}-\frac{1}{2}\Big)\Big/3\mathbb{Z} \;=\; \Big\{\pm\frac{1}{2},\frac{3}{2}\Big\},$$

$$\begin{aligned}
\theta_{1/2}(\tau,z) &= \sum_{m\in\mathbb{Z}}(-1)^m q^{\frac{1}{6}(3m+\frac{1}{2})^2}\zeta^{3m+\frac{1}{2}},\\
\theta_{-1/2}(\tau,z) &= \sum_{m\in\mathbb{Z}}(-1)^m q^{\frac{1}{6}(3m+\frac{1}{2})^2}\zeta^{-3m-\frac{1}{2}},\\
\theta_{3/2}(\tau,z) &= \sum_{m\in\mathbb{Z}}(-1)^m q^{\frac{1}{6}(3m+\frac{3}{2})^2}\zeta^{3m+\frac{3}{2}}.
\end{aligned}$$

Then comparing the coefficients of $q^{1/24}$ in the theorem,

$$\zeta^{-1/2}\frac{1-\zeta^2}{1-\zeta} = c_{1/2}\zeta^{1/2}+c_{-1/2}\zeta^{-1/2},$$

$$\therefore\; c_{1/2}=c_{-1/2}=1.$$

Furthermore, comparing the coefficients of $q^{3/8}$ in the theorem,

$$0 = c_{3/2}(-\zeta^{-3/2}).\;\; \therefore c_{3/2}=0.$$

$$\begin{aligned}
\therefore \qquad & q^{1/24}\zeta^{-1/2}\frac{1-\zeta^2}{1-\zeta}\prod_{n=1}^{\infty}\frac{(1-q^n)(1-q^n\zeta^2)(1-q^n\zeta^{-2})}{(1-q^n\zeta)(1-q^n\zeta^{-1})}\\
= \;& \sum_{m\in\mathbb{Z}}(-1)^m q^{\frac{3}{2}(m+\frac{1}{6})^2}\left(\zeta^{3(m+\frac{1}{6})}+\zeta^{-3(m+\frac{1}{6})}\right).
\end{aligned}$$

Exercise 5.4.2. Show Watson's quintuple product identity:

$$\begin{aligned}
&\prod_{n=1}^{\infty}(1-q^n)(1-q^n\zeta)(1-q^{n-1}\zeta^{-1})(1-q^{2n-1}\zeta^2)(1-q^{2n-1}\zeta^{-2})\\
=\;& \sum_{m\in\mathbb{Z}} q^{m(3m+1)/2}\left(\zeta^{3m}-\zeta^{-3m-1}\right)
\end{aligned}$$

by substituting $\zeta\mapsto-\zeta^{-1}$ in the above formula.

Borcherds lift. For a Jacobi form $\varphi(\tau,z)$ of weight k on $\mathbb{H}\times\mathbb{C}$,

$$\begin{aligned}
\left(\varphi|_{V(m)}\right)(\tau,z) &\overset{\text{def}}{=} m^{k-1}\sum_{ad=m,a>0}\sum_{b=0}^{d-1}d^{-k}\varphi((a\tau+b)/d,az),\\
(ML(\varphi))\begin{pmatrix}\tau & z\\ z & \omega\end{pmatrix} &\overset{\text{def}}{=} \sum_{m=1}^{\infty}\left(\varphi|_{V(m)}\right)(\tau,z)\cdot p^m;\;\; p=\exp(2\pi\sqrt{-1}\omega)\\
&: \quad \text{Maass (Saito-Kurokawa) lift.}
\end{aligned}$$

Then

$$\varphi(\tau,z)=\sum_{n,l\in\mathbb{Z}}c(n,l)q^n\zeta^l \text{ has weight } k=0 \text{ and } c(n,l)\in\mathbb{Z}$$

$$\Longrightarrow \quad \exp(-ML(\varphi))=\prod_{n,m,l\in\mathbb{Z}}(1-q^n\zeta^l p^m)^{c(nm,l)} \text{ is a Siegel modular function.}$$

As its modified version, Borcherds showed:

Theorem 5.6 (Borcherds) (Proof is omitted). *For a Jacobi form*

$$\varphi(\tau,z)=\sum_{n,l\in\mathbb{Z}}c(n,l)q^n\zeta^l$$

on $\mathbb{H}\times\mathbb{C}$ *such that* $c(n,l)\in\mathbb{Z}$, *put*

$$a=\frac{1}{24}\sum_{l\in\mathbb{Z}}c(0,l),\ b=\frac{1}{2}\sum_{l\in\mathbb{Z}}c(0,l)\cdot l,\ a=\frac{1}{2}\sum_{l\in\mathbb{Z}}c(0,l)\cdot l^2,$$

$$BP(\varphi)\begin{pmatrix}\tau & z\\ z & \omega\end{pmatrix} \overset{\text{def}}{=} q^a\zeta^{-b}p^c\prod_{(n,m,l)>0}(1-q^n\zeta^l p^m)^{c(nm,l)} : \textit{ Borcherds lift}$$

$$;(n,m,l)>0 \overset{\text{def}}{\Leftrightarrow} \begin{cases} & m\in\mathbb{N},\ n,l\in\mathbb{Z},\\ or & m=0,\ n\in\mathbb{N},\ l\in\mathbb{Z},\\ or & m=n=0,\ l\in\mathbb{Z}.\end{cases}$$

Then $BP(\varphi)$ *is a Siegel modular form of degree* 2 *and weight* $c(0,0)/2$.

Remark. In general, Borcherds showed that

Borcherds lifts of Jacobi forms on $\mathbb{H}\times\mathbb{C}^N \Rightarrow$ modular forms attached to $O(N+2,2)$.

Appendices

A1. Rogers-Ramanujan's identity and the mock theta conjecture

Notation. For variables a and q,

$$\begin{aligned}(a)_0 &= (a;q)_0 \stackrel{\text{def}}{=} 1,\\ (a)_n &= (a;q)_n \stackrel{\text{def}}{=} \prod_{k=0}^{n-1}\left(1-aq^k\right): \text{ polynomial of } q \text{ and } a\ (n\geq 1),\\ (a)_\infty &= (a;q)_\infty \stackrel{\text{def}}{=} \prod_{k=0}^{\infty}\left(1-aq^k\right): \text{ power series of } q.\end{aligned}$$

Rogers-Ramanujan's identity (founded by Rogers and Ramanujan independently).

$$\begin{aligned}G(q) &\stackrel{\text{def}}{=} 1+\sum_{n=1}^{\infty}\frac{q^{n^2}}{(1-q)\cdots(1-q^n)}=\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q)_n},\\ H(q) &\stackrel{\text{def}}{=} 1+\sum_{n=1}^{\infty}\frac{q^{n^2+n}}{(1-q)\cdots(1-q^n)}=\sum_{n=0}^{\infty}\frac{q^{n^2+n}}{(q)_n}.\end{aligned}$$

Then

$$\begin{aligned}G(q) &= \prod_{n=1}^{\infty}\frac{1}{(1-q^{5n-4})(1-q^{5n-1})},\\ H(q) &= \prod_{n=1}^{\infty}\frac{1}{(1-q^{5n-3})(1-q^{5n-2})}.\end{aligned}$$

Ramanujan's proof (cf. [R]).

Step 1. Put

$$F(x)\stackrel{\text{def}}{=}1+\frac{xq}{1-q}+\frac{x^2q^4}{(1-q)(1-q^2)}+\frac{x^3q^9}{(1-q)(1-q^2)(1-q^3)}+\cdots.$$

Then

$$\begin{aligned}F(1) &= G(q),\\ F(q) &= H(q),\\ F(x) &= F(xq)+xqF(xq^2)\ \cdots(1).\end{aligned}$$

$(\because)$

$$\begin{aligned}F(x)-F(xq) &= \frac{xq(1-q)}{1-q}+\frac{x^2q^4(1-q^2)}{(1-q)(1-q^2)}+\frac{x^3q^9(1-q^3)}{(1-q)(1-q^2)(1-q^3)}+\cdots\\ &= xq\left(1+\frac{xq^3}{1-q}+\frac{x^2q^8}{(1-q)(1-q^2)}+\cdots\right)\\ &= xqF(xq^2).\end{aligned}$$

This completes the proof. □

Remark A1.1. $F(x)$ is a unique power series of x satisfying (1) and that $F(0) = 1$.

Exercise A1.1. Show Remark A1.1.

Step 2. Put $E(x) \stackrel{\text{def}}{=} F(x)(1-xq)(1-xq^2)(1-xq^3)\cdots = F(x)(xq)_\infty$. Then

$$\begin{aligned} E(1) &= F(1)(q)_\infty = G(q)(q)_\infty, \\ E(q) &= F(q)(q^2)_\infty = H(q)(q)_\infty/(1-q), \\ E(x) &= (1-xq)E(xq) + xq(1-xq)(1-xq^2)E(xq^2) \ \cdots(2). \end{aligned}$$

$(\because)$

$$\begin{aligned} \text{RHS of (2)} &= (1-xq)F(xq)(1-xq^2)(1-xq^3)(1-xq^4)\cdots \\ &\quad + xq(1-xq)(1-xq^2)F(xq^2)(1-xq^3)(1-xq^4)\cdots \\ &= (xq)_\infty \left\{F(xq) + xqF(xq^2)\right\} \\ &\stackrel{(1)}{=} (xq)_\infty F(x) \\ &= \text{LHS of (2). } \square \end{aligned}$$

Remark A1.2. $E(x)$ is a unique power series of x satisfying (2) and that $E(0) = 1$.

Key point (Genius of Ramanujan!). Put

$$\begin{aligned} R(x) &\stackrel{\text{def}}{=} 1 + \sum_{n=1}^{\infty} (-1)^n x^{2n} q^{n(5n-1)/2} (1-xq^{2n}) \frac{(xq)_{n-1}}{(q)_n} \\ &= 1 - x^2q^2(1-xq^2)\frac{1}{1-q} + x^4q^9(1-xq^4)\frac{1-xq}{(1-q)(1-q^2)} - \cdots. \end{aligned}$$

Then

$$\begin{aligned} R(0) &= 1, \\ R(x) &= (1-xq)R(xq) + xq(1-xq)(1-xq^2)R(xq^2) \ \cdots(3). \end{aligned}$$

$(\because)$ Since $1 - xq^{2n} = 1 - q^n + q^n(1-xq^n)$,

$$R(x) = (1-x^2q^2) - x^2q^3(1-x^2q^6)\frac{1-xq}{1-q} + x^4q^{11}(1-x^2q^{10})\frac{(1-xq)(1-xq^2)}{(1-q)(1-q^2)} - \cdots.$$

$$\begin{aligned} \therefore \quad & \frac{R(x)}{1-xq} - R(xq) \\ &= xq(1-xq^2)\left\{1 - x^2q^6(1-xq^4)\frac{1}{1-q} + x^4q^{17}(1-xq^6)\frac{1-xq^3}{(1-q)(1-q^2)}\right. \\ &\quad \left. - x^6q^{33}(1-xq^8)\frac{(1-xq^3)(1-xq^4)}{(1-q)(1-q^2)(1-q^3)} + \cdots\right\} \\ &= xq(1-xq^2)R(xq^2). \ \square \end{aligned}$$

End of proof. By the Key point and Remark A1.2,

$$E(x) = R(x).$$

Then putting $x = 1$,

$$\begin{aligned} R(1) &= E(1) = G(q)(q)_\infty, \\ R(1) &= 1 + \sum_{n=1}^{\infty} (-1)^n q^{n(5n-1)/2} \frac{1-q^{2n}}{1-q^n} \overset{(*)}{=} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+1)/2}. \end{aligned}$$

$$\therefore\ G(q) = \frac{1}{(q)_\infty} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+1)/2} \ \cdots (4).$$

Further, putting $x = q$,

$$\begin{aligned} R(q) &= E(q) = H(q)(q)_\infty/(1-q), \\ R(q) &= 1 + \sum_{n=1}^{\infty} (-1)^n q^{2n} q^{n(5n-1)/2} \frac{1-q^{2n+1}}{1-q} \overset{(\sharp)}{=} \frac{1}{1-q} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+3)/2}. \end{aligned}$$

$$\therefore\ H(q) = \frac{1}{(q)_\infty} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+3)/2} \ \cdots (5).$$

Recall Jacobi's triple product:

$$\prod_{n=1}^{\infty} (1-q^n)(1+\zeta q^{n-1/2})(1-\zeta^{-1} q^{n-1/2}) = \sum_{n=-\infty}^{\infty} \zeta^n q^{n^2/2}.$$

Then substituting $q \mapsto q^5$ and $\zeta \mapsto -q^{1/2}$,

$$\prod_{n=1}^{\infty} (1-q^{5n})(1-q^{5n-2})(1-q^{5n-3}) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+1)/2}.$$

Dividing this by $(q)_\infty = \prod_{n=1}^{\infty}(1-q^n)$,

$$\prod_{n=1}^{\infty} \frac{1}{(1-q^{5n-4})(1-q^{5n-1})} = \frac{1}{(q)_\infty} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+1)/2} \overset{(4)}{=} G(q);\ \text{R-R's identity.}$$

Further, substituting $q \mapsto q^5$ and $\zeta \mapsto -q^{3/2}$,

$$\prod_{n=1}^{\infty} (1-q^{5n})(1-q^{5n-1})(1-q^{5n-4}) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+3)/2}.$$

Dividing this by $(q)_\infty$,

$$\prod_{n=1}^{\infty} \frac{1}{(1-q^{5n-3})(1-q^{5n-2})} = \frac{1}{(q)_\infty} \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+3)/2} \overset{(5)}{=} H(q);\ \text{R-R's identity.}\ \square$$

Exercise A1.2. Show $(*)$ and $(\sharp)$.

Application to continued fractions.

$$1+\frac{q}{1}\ +\ \frac{q^2}{1}\ +\ \frac{q^3}{1}\ +\ \cdots \overset{\text{def}}{=} 1+\frac{q}{1+\frac{q^2}{1+\frac{q^3}{1+\cdots}}}\ ?$$

Since

$$\begin{aligned} K(x) &\overset{\text{def}}{=} \frac{E(x)}{(1-xq)E(xq)} \overset{(2)}{=} 1+\frac{xq}{K(xq)} = 1+\frac{xq}{1+\frac{xq^2}{K(xq^2)}} = \cdots \\ &= 1+\frac{xq}{1}\ +\ \frac{xq^2}{1}\ +\ \frac{xq^3}{1}\ +\ \cdots, \end{aligned}$$

$$1+\frac{q}{1}\ +\ \frac{q^2}{1}\ +\ \frac{q^3}{1}\ +\ \cdots = \frac{E(1)}{(1-q)E(q)} = \frac{G(q)(q)_\infty}{H(q)(q)_\infty} = \frac{G(q)}{H(q)},$$

and hence by R-R's identity,

$$1+\frac{q}{1}\ +\ \frac{q^2}{1}\ +\ \frac{q^3}{1}\ +\ \cdots = \prod_{n=1}^{\infty}\frac{(1-q^{5n-3})(1-q^{5n-2})}{(1-q^{5n-4})(1-q^{5n-1})}.$$

Remark A1.3. Denote the Poincaré upper half plane by $\mathbb{H}=\{\tau\in\mathbb{C}\mid \mathrm{Im}(\tau)>0\}$. Then R-R's continued fraction

$$\frac{q^{1/5}}{1}\ +\ \frac{q}{1}\ +\ \frac{q^2}{1}\ +\ \frac{q^3}{1}\ +\ \cdots = q^{1/5}\frac{H(q)}{G(q)}$$

becomes a modular function of $\tau\in\mathbb{H}$, where $q=e^{2\pi\sqrt{-1}\tau}$.

Mock theta conjecture by Ramanujan on the 5th order case.

$$\begin{aligned} \sum_{n=0}^{\infty}\frac{q^{n^2}}{(-q)_n} &= \frac{(q^5;q^5)_\infty(q^5;q^{10})_\infty}{(q;q^5)_\infty(q^4;q^5)_\infty} - 2\left(-1+\sum_{m=0}^{\infty}\frac{q^{10m^2}}{(q^2;q^{10})_{m+1}(q^8;q^{10})_m}\right), \\ \sum_{n=0}^{\infty}\frac{q^{n^2+n}}{(-q)_n} &= \frac{(q^5;q^5)_\infty(q^5;q^{10})_\infty}{(q^2;q^5)_\infty(q^3;q^5)_\infty} - \frac{2}{q}\left(-1+\sum_{m=0}^{\infty}\frac{q^{10m^2}}{(q^4;q^{10})_{m+1}(q^6;q^{10})_m}\right). \end{aligned}$$

In 1988, Hickerson proved this conjecture by technical calculation. In 2002, Zwegers obtained a fundamental result that

Mock theta functions = "holomorphic parts" of harmonic modular forms of weight 1/2.

A2. Representation theory and infinite product

Aim. As an example of infinite products arising from representation theory, we explain

Borcherds' proof of Jacobi's triple product identity (cf. [C])

using the Boson-Fermion correspondence.

Definition.

$$L \overset{\text{def}}{=} \mathbb{Z}+1/2 = \{\text{levels}\} = L_+ \cup L_-; \begin{cases} L_+ \overset{\text{def}}{=} \{i \in L \mid i > 0\}, \\ L_- \overset{\text{def}}{=} \{i \in L \mid i < 0\}. \end{cases}$$

$$S : \textit{(admissible) state} \overset{\text{def}}{\Longleftrightarrow} S : L \to \{\bullet : \text{occupied}, \circ : \text{unoccupied}\}$$
such that $S^{-1}(\bullet) \cap L_+$ and $S^{-1}(\circ) \cap L_-$ are finite sets.

For a state S,

$$Q(S) \overset{\text{def}}{=} \sharp\left(S^{-1}(\bullet) \cap L_+\right) - \sharp\left(S^{-1}(\circ) \cap L_-\right) : \text{ charge of } S.$$
$$H(S) \overset{\text{def}}{=} \sum_{i \in S^{-1}(\bullet) \cap L_+} i - \sum_{i \in S^{-1}(\circ) \cap L_-} i : \text{ (total) energy of } S.$$

Partition function. $Z(q,z) \overset{\text{def}}{=} \sum_{S\text{: states}} z^{Q(S)} q^{H(S)}$.

Fermionic evaluation of $Z(q,z)$.

$$\begin{aligned} Z(q,z) &= \sum z^{(\sharp S_+ - \sharp S_-)} q^{(\sum_{i \in S_+} i - \sum_{i \in S_-} i)} \ (S_+ : \text{finite} \subset L_+,\ S_- : \text{finite} \subset L_-) \\ &= \begin{array}{cccccccc} & \cdots & (1+zq^{3/2}) & (1+zq^{1/2}) & (1+z^{-1}q^{1/2}) & (1+z^{-1}q^{3/2}) & \cdots \\ i & \cdots & 3/2 & 1/2 & -1/2 & -3/2 & \end{array} \\ &= \prod_{i \in L_+} (1+zq^i) \cdot \prod_{i \in L_-} (1+z^{-1}q^{-i}) \\ &= \prod_{n=1}^{\infty} (1+zq^{n-1/2})(1+z^{-1}q^{n-1/2}) \ \cdots (1). \end{aligned}$$

Bosonic evaluation of $Z(q,z)$. Let $\mathrm{vac}(n)$ be the state defined by

$$\mathrm{vac}(n)^{-1}(\bullet) = \{i \in L \mid i < n\}.$$

Then for a state S with charge n, there are uniquely integers $\lambda_1 \geq \lambda_2 \geq \cdots > 0$ such that

$$\begin{aligned} S^{-1}(\bullet) &= \left(\mathrm{vac}(n)^{-1}(\bullet) - \left\{n - \frac{1}{2} > n - \frac{3}{2} > \cdots > n - k + \frac{1}{2}\right\}\right) \\ &\quad \bigcup \left\{n - \frac{1}{2} + \lambda_1 > n - \frac{3}{2} + \lambda_2 > \cdots > n - k + \frac{1}{2} + \lambda_k\right\}. \end{aligned}$$

Then

$$H(S) = H(\mathrm{vac}(n)) + \sum_i \lambda_i = \frac{n^2}{2} + \sum_i \lambda_i.$$

$$\therefore\ Z(q,z) = \sum_{n\in\mathbb{Z}} z^n \sum_{Q(S)=n} q^{H(S)} = \sum_{n\in\mathbb{Z}} z^n \sum_{\lambda_1\geq\lambda_2\geq\cdots>0} q^{n^2/2+\sum_i \lambda_i}.$$

Define the partition function $p(m)$ as $p(0)=1$ and for $m\in\mathbb{N}$,

$$p(m) \stackrel{\mathrm{def}}{=} \sharp \left\{ (\lambda_1,\lambda_2,...,\lambda_k) \;\middle|\; \begin{array}{l} \lambda_i \in \mathbb{N}, \\ \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k, \\ \sum_i \lambda_i = m \end{array} \right\}.$$

Then

$$\begin{aligned} & \sum_{m=0}^{\infty} p(m) q^m \\ \stackrel{(*)}{=}\ & \left(1+q^1+q^{1+1}+q^{1+1+1}+\cdots\right)\left(1+q^2+q^{2+2}+\cdots\right)\left(1+q^3+\cdots\right)\cdots \\ =\ & \frac{1}{1-q}\cdot\frac{1}{1-q^2}\cdot\frac{1}{1-q^3}\cdots, \end{aligned}$$

and hence

$$Z(q,z) = \sum_{n\in\mathbb{Z}} z^n q^{n^2/2} \left(\sum_{m=0}^{\infty} p(m) q^m\right) = \prod_{m=1}^{\infty} \frac{1}{1-q^m} \sum_{n\in\mathbb{Z}} z^n q^{n^2/2} \quad \cdots (2).$$

End of proof. Since the left hand sides of (1) and (2) are equal, multiplying $\prod_{n=1}^{\infty}(1-q^n)$ with these right hand sides,

$$\prod_{n=1}^{\infty}(1-q^n)(1+zq^{n-1/2})(1-z^{-1}q^{n-1/2}) = \sum_{m\in\mathbb{Z}} z^m q^{m^2/2}. \ \square$$

Exercise A2.1. Show $(*)$.

Remark. Put

$$\begin{aligned} \Lambda &: \text{the vector space spanned by all states,} \\ \Lambda_{d,m} &: \text{the vector space spanned by states with energy } d \text{ and charge } m, \\ \mathrm{ch}(\Lambda) &\stackrel{\mathrm{def}}{=} \sum_{d=0}^{\infty}\sum_{m=-\infty}^{\infty} (\dim \Lambda_{d,m})\, z^m q^d : \text{ the character of } \Lambda. \end{aligned}$$

Then the above result states

$$\text{Character formula on } \mathrm{ch}(\Lambda) \Longrightarrow \text{Jacobi's triple product.}$$

Similarly,

$$\text{Character formula on infinitely dimensional algebras} \Longrightarrow \begin{cases} \text{Macdonald identity} \Rightarrow \text{Euler's pentagon}, \\ \text{Rogers-Ramanujan's identity}, \\ \text{Proof of Moon shine conjecture}, \\ \cdots\cdots. \end{cases}$$

References

[A1] H. Aoki, A remark on Borcherds construction of Jacobi forms, http://www.ma.noda.tus.ac.jp/u/ha/Data/kyushu.pdf

[A2] H. Aoki, Borcherds product, http://www.ma.noda.tus.ac.jp/u/ha/Data/ss11aoki.pdf

[C] H-C. Chan, An invitation to q-series, 2011, World Scientific.

[K] S. Kitamura, On a theorem of Jacobi (in Japanese), Master thesis in Saga University at 2016.

[MM] H. McKean and V. Moll, Elliptic curves (function theory, geometry, arithmetic), Cambridge University Press, 1999.

[R] Rogers-Ramanujan Identities: A Proof by Ramanujan, http://paramanands.blogspot.jp/2013/05/rogers-ramanujan-identities-a-proof-by-ramanujan.html

[S] J. P. Serre, A Course in arithmetic, Graduate Texts in Math. vol. 7, Springer-Verlag, 1973.

[Si] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Math. vol. 151, Springer-Verlag, 1994.

[T] T. Takagi, Kinnsei Sugaku Shidan (in Japanese), Iwanami bunko, 1995.

[W] A. Weil, Number Theory, Birkhäuser, 2007.