国外数学名著系列
（影印版）72

Goro Shimura

Elementary Dirichlet Series and Modular Forms

初等Dirichlet级数和模形式

科学出版社

国外数学名著系列(影印版) 72

Elementary Dirichlet Series and Modular Forms

初等 Dirichlet 级数和模形式

Goro Shimura

科学出版社
北京

图字：01-2011-3323

图书在版编目(CIP)数据

初等 Dirichlet 级数和模形式= Elementary Dirichlet Series and Modular Forms / （美）希穆勒(Shimura, G.)编著. —影印版. —北京：科学出版社，2011

(国外数学名著系列；72)

ISBN 978-7-03-031390-4

I. ①初… II. ①希… III. ①级数-英文 IV. ①O173

中国版本图书馆 CIP 数据核字(2011) 第 105058 号

责任编辑：赵彦超 汪 操/责任印刷：钱玉芬/封面设计：陈 敬

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2011年6月第 一 版 开本：B5(720×1000)
2011年6月第一次印刷 印张：10 1/4
印数：1—2 500 字数：185 000

定价：56.00 元

(如有印装质量问题，我社负责调换)

《国外数学名著系列》(影印版) 序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格(Springer)出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了 23 本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这 23 本书中，包括基础数学书 5 本，应用数学书 6 本与计算数学书 12 本，其中有些书也具有交叉性质。 这些书都是很新的，2000 年以后出版的占绝大部分，共计 16 本，其余的也是 1990 年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23 本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王　元

2005 年 12 月 3 日

PREFACE

A book on any mathematical subject above textbook level is not of much value unless it contains new ideas and new perspectives. Also, the author may be encouraged to include new results, provided that they help the reader gain new insights and are presented along with known old results in a clear exposition.

It is with this philosophy that I write this volume. The two subjects, Dirichlet series and modular forms, are traditional, but I treat them in both orthodox and unorthodox ways. However, I try to make the book accessible to those who are not familiar with such topics, by including plenty of expository material. More specific descriptions of the contents will be given in the Introduction.

To some extent, this book has a supplementary nature to my previous book *Introduction to the Arithmetic Theory of Automorphic Functions,* published by Princeton University Press in 1971, though I do not write the present book with that intent. While the 1971 book grew out of my lectures in various places, the essential points of this new book have never been presented publicly or privately. I hope that it will draw an audience as large as that of the previous book.

Princeton
March 2007

Goro Shimura

TABLE OF CONTENTS

INTRODUCTION

There are two types of Dirichlet series that we discuss in this book:

$$(1)\qquad D^r_{a,N}(s) = \sum_{0\neq n\in a+N\mathbf{Z}} n^r|n|^{-r-s},$$

$$(2)\qquad L^r(s;\,\alpha,\,\mathfrak{b}) = \sum_{0\neq \xi\in\alpha+\mathfrak{b}} \xi^{-r}|\xi|^{r-2s}.$$

Here s is a complex variable as usual, r is 0 or 1 for $D^r_{a,N}$ and $0 < r \in \mathbf{Z}$ for the latter series; $a \in \mathbf{Z}$ and $0 < N \in \mathbf{Z}$. To define the series of (2) we take an imaginary quadratic field K embedded in $\mathbf{C}$ and take also an element α of K and a $\mathbf{Z}$-lattice $\mathfrak{b}$ in K. One of our principal problems is to investigate the nature of the values of these series at certain integer values of s. As a preliminary step, we discuss their analytic continuation and functional equaltions. We obtain Dirichlet L-functions and certain Hecke L-functions of K as suitable linear combinations of these series, and so the values of such L-functions are included in our objects of study. As will be explained below, these series are directly and indirectly related to elliptic modular forms, and the exposition of such functions in that context forms a substantial portion of this volume. Thus, as we said in the preface, the main objective of this book is to present some new ideas, new results, and new perspectives, along with old ones in this area covering certain aspects of the theory of modular forms and Dirichlet series.

To be more specific, let us first consider the Dirichlet L-function

$$L(s,\,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$$

with a primitive Dirichlet character χ modulo a positive integer N. It is well known that if k is a positive integer and $\chi(-1) = (-1)^k$, then

$$(3)\qquad \frac{2k!G(\overline{\chi})}{(2\pi i)^k}L(k,\,\chi) = -\sum_{a=1}^{N} \overline{\chi}(a)B_k(a/N),$$

where B_k is the Bernoulli polynomial of degree k and $G(\overline{\chi})$ is the Gauss sum of $\overline{\chi}$. If $k = 1$ in particular, the last sum for χ such that $\chi(-1) = -1$ becomes $\sum_{a=1}^{N} \overline{\chi}(a)a/N$, which reminds us of another well known result about the second factor of the class number of a cyclotomic field, which is written h_K/h_F. Here

h_K resp. h_F is the class number of K resp. F; K is an imaginary subfield of $\mathbf{Q}(\zeta)$ with a primitive mth root of unity ζ for some positive integer m and F is the maximal real subfield of K. There is a classical formula for h_K/h_F, which is easy factors times a product $\prod_{\chi\in X}\sum_a \chi(a)a$, where X is a certain set of primitive Dirichlet characters χ such that $\chi(-1) = -1$.

No alternative formulas have previously been presented except when K is an imaginary quadratic field $K = \mathbf{Q}(\sqrt{-d}\,)$. Given such a K, take a real character χ of conductor d that corresponds to K. Then it is well known that

$$(4) \qquad \frac{w_K\sqrt{d}}{2\pi}L(1,\,\chi) = h_K = \frac{w_K}{2(2-\chi(2))}\sum_{a=1}^{q}\chi(a), \quad q = [(d-1)/2],$$

where w_K is the number of roots of unity in K.

Now we will prove as one of the main results of this book that there are new formulas for $L(k,\,\chi)$. The most basic one is

$$(5) \qquad \frac{(k-1)!G(\overline{\chi})}{(2\pi i)^k}L(k,\,\chi) = \frac{1}{2(2^k-\chi(2))}\sum_{a=1}^{q}\overline{\chi}(a)E_{1,k-1}(2a/d),$$

where $q = [(d-1)/2]$ and $E_{1,k-1}(t)$ is the Euler polynomial of degree $k-1$. This clearly includes (4) (without h_K) as a special case, as $E_{1,0}(t) = 1$. This formula is better than (3) at least from the computational viewpoint, as $E_{1,k-1}(t)$ is a polynomial in t of degree $k-1$, whereas $B_k(t)$ is of degree k. We will present many more new formulas for $L(k,\,\chi)$ in Sections 4 and 6. As applications, we will prove some new formulas for the quotient h_K/h_F.

To avoid excessive details, we state it in this introduction only when $K = \mathbf{Q}(\zeta)$ with $m = 2^r > 4$:

$$\frac{h_K}{h_F} = 2^\gamma\prod_{s=3}^{r}\prod_{\chi\in Y_s}\left\{\sum_{a=1}^{d_s}\chi(a)\right\}, \quad d_s = 2^{s-2}-1, \quad \gamma = r-1-2^{r-2}.$$

Here Y_s is the set of primitive Dirichlet characters χ of conductor 2^s such that $\chi(-1) = -1$. Notice that we have $\sum_{a=1}^{d_s}\chi(a)$, which is of far "smaller size" than the sum $\sum_a \chi(a)a$ in the classical formula. A similar but somewhat different formula can be obtained in the case $m = \ell^r$ with an odd prime ℓ.

The latter part of the book concerns the critical values of the series of type (2). In this case we evaluate it at $k/2$ with an integer k such that $2-r \le k \le r$ and $r-k \in 2\mathbf{Z}$. Then we can show that:

(6) *There is a constant* γ *which depends only on* K *(that is, independent of* α, $\mathfrak{b}$, r, *and* k*) such that* $L^r(k/2;\,\alpha,\,\mathfrak{b})$ *is* $\pi^{(r+k)/2}\gamma^r$ *times an algebraic number.*

This was proved in one of the author's papers. Though we will give a proof of this fact in this book, it is merely the starting point. Indeed one of our main problems is to find a suitable γ so that the algebraic number can be computed. Before going into this problem, we note that the constant γ can be given as $\varphi(\tau)$ with a modular form φ of weight 1 and $\tau \in K \cap H$, where $H = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$.

If $r = k \neq 2$, the value $L^r(r/2;\, \alpha,\, \mathfrak{b})$ can be given as $\pi^r h(\tau)$ with a holomorphic modular form h of weight r. Thus our task is to find $(h/\varphi^r)(\tau)$. This can be achieved as follows. We fix a congruence subgroup Γ of $SL_2(\mathbf{Z})$ to which both φ and h belong, and assume that we can find two modular forms f and g that generate the algebra of all modular forms of all nonnegative weights with respect to Γ. Then $h = P(f,\, g)$ with a polynomial P, and $(h/\varphi^r)(\tau) = P\big((f/\varphi^k)(\tau),\, (g/\varphi^\ell)(\tau)\big)$, where k resp. ℓ is the weight of f resp. g. However there are two essential questions:

(I) How can we find P?

(II) In the general case in which $r \neq k$ or $k = 2$, $L^r(k/2;\, \alpha,\, \mathfrak{b})$ can be given as $\pi^{(r+k)/2}p(\tau)$ with some nonholomorphic modular form (which we call *nearly holomorphic*) p of weight r. Then, how can we handle $(p/\varphi^r)(\tau)$?

Problem (II) can be reduced to Problem (I) and Problem (II) for simpler p. In the easiest case we can express p as a polynomial $\sum_{a=0}^{[r/2]} E_2^a h_a$, where h_a is a holomorphic modular form of weight $r - 2a$ and E_2 is a well known nonholomorphic Eisenstein series of weight 2:

$$E_2(z) = \frac{1}{8\pi y} - \frac{1}{24} + \sum_{n=1}^{\infty}\Bigg(\sum_{0<d\mid n} d\Bigg)\mathbf{e}(nz).$$

Then the problem can be reduced to $(E_2/\varphi^2)(\tau)$ and $(h_a/\varphi^{r-2a})(\tau)$. The latter quantity is handled by P for h_a. As for E_2, we have to deal with it in a special way. For a given τ we will find a special holomorphic modular form q of weight 2 such that $(E_2/q)(\tau)$ can be explicitly given.

In this way the value of nonholomorphic functions can be reduced to the case of holomorphic modular forms, and to Problem (I). We also have to find $(f/\varphi^k)(\tau)$ and $(g/\varphi^\ell)(\tau)$, which is nontrivial, but our idea is to reduce infinitely many values to finitely many values. In general, there is no clear-cut answer to (I). However, we can produce two types of recurrence formulas for Eisenstein series, which seem to be new and by which the problem about h/φ^r of an arbitrary weight r can be reduced to the case of smaller r. (See (10.8) and (10.15c).) Without stating it, we content ourselves by mentioning its application to $L^r(k/2;\, \alpha,\, \mathfrak{b})$. Assuming that $\alpha \notin \mathfrak{b}$, $0 < k \leq r$, and $r - k \in 2\mathbf{Z}$, put $n = (r-k)/2$, and

$$\mathfrak{L}_k^n(\alpha,\, \mathfrak{b}) = (-1)^k(2\pi i)^{-k-n}\Gamma(k+n)L^r(k/2;\, \alpha,\, \mathfrak{b}) - \begin{cases} 2(2i)^n\mathrm{Im}(\tau)^n(D_2^n E_2)(\tau) & \text{if } k = 2, \\ 0 & \text{if } k \neq 2, \end{cases}$$

where D_2^n is a differential operator of the type mentioned above. Then we have a recurrence formula

$$\mathfrak{L}^n_{t+5}(\alpha,\, \mathfrak{b}) = 12\sum_{i=0}^{t}\binom{t}{i}\sum_{j=0}^{n}\binom{n}{j}\,\mathfrak{L}^j_{i+3}(\alpha,\, \mathfrak{b})\cdot\mathfrak{L}^{n-j}_{t-i+2}(\alpha,\, \mathfrak{b})$$

for $0 \le t \in \mathbf{Z}$ and $0 \le n \in \mathbf{Z}$. Thus the values of $\mathfrak{L}^n_k(\alpha,\, \mathfrak{b})$ for $k > 4$ can be reduced inductively to those for $2 \le k \le 4$. If $\alpha \in \mathfrak{b}$, there is another recurrence formula which reduces $\mathfrak{L}^n_{2k}(\alpha,\, \mathfrak{b})$ for $2k \ge 8$ to the cases with $2k = 4$ and $2k = 6$.

We can form a Hecke L-function $L(s,\, \lambda) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a})N(\mathfrak{a})^{-s}$, with a Hecke ideal character λ of K such that

$$\lambda(\alpha\mathfrak{r}) = \alpha^{-r}|\alpha|^r \quad \text{if} \quad \alpha \in K^\times \quad \text{and} \quad \alpha - 1 \in \mathfrak{c},$$

where $\mathfrak{c}$ is an integral ideal of K. Since this is a finite linear combination of series of type (2), statement (6) holds for $L(k/2,\, \lambda)$ in place of $L^r(k/2;\, \alpha,\, \mathfrak{b})$. In Section 13, we will present many examples of numerical values of $L(k/2,\, \lambda)$.

When $r = 1$, the function $L(s,\, \lambda)$ is closely connected with an elliptic curve C defined over an algebraic number field h with complex multiplication in K. In a certain case, it is indeed the zeta function of C over h. We will study this aspect in Section 14, and compare $L(1/2,\, \lambda)$ with a period of a holomorphic 1-form on C, when C is a member of a one-parameter family $\{C_z\}_{z\in H}$ of elliptic curves.

However, without going into details of this theory, let us end this introduction by briefly mentioning some other noteworthy features of the book.

(A) A discussion of irregular cusps of a congruence subgroup of $SL_2(\mathbf{Z})$ in §1.11 and Theorem 1.13.

(B) The functional equation of the Eisenstein series

$$\mathfrak{E}^N_k(z,\, s;\, p,\, q) = \mathrm{Im}(z)^s \sum_{(m,\, n)} (mz+n)^{-k}|mz+n|^{-2s}$$

under $s \mapsto 1-k-s$ (Theorem 9.7). Here $(z,\, s) \in H \times \mathbf{C}$, $0 < N < \mathbf{Z}$, $0 \le k \in \mathbf{Z}$, $(p,\, q) \in \mathbf{Z}^2$, and $(m,\, n)$ runs over $\mathbf{Z}^2$ under the condition $0 \ne (m,\, n) \equiv (p,\, q) \pmod{N\mathbf{Z}^2}$.

(C) The explicit Fourier expansion of $\mathfrak{E}^N_k(z,\, 1-k;\, p,\, q)$ given in (9.14).

(D) In Section 15, we discuss isomorphism classes of abelian varieties, elliptic curves in particular, with complex multiplication defined over a number field with the same zeta function.

(E) In Section 16 we present a new class of holomorphic differential operators $\{\mathfrak{A}^p_k\}_{p=2}^{\infty}$. The operator $\mathfrak{A}^p_k$ sends an automorphic form of weight k to that of weight $kp + 2p$, and every operator of the same nature can be reduced to this class.

CHAPTER I

PRELIMINARIES ON MODULAR FORMS AND DIRICHLET SERIES

1. Basic symbols and the definition of modular forms

Though some basic facts on elliptic modular forms are reviewed in this section, we do not need them in Sections 2 through 7. Therefore the reader may go directly to Section 2 after reading §1.1, Lemmas 1.6 and 1.12, and return to this section before going to Section 8.

1.1. The symbols $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ will mean as usual the ring of integers, the fields of rational numbers, real numbers, and complex numbers, respectively. Also, we denote by $\overline{\mathbf{Q}}$ the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Given an associative ring A with identity element, we denote by $A^\times$ the group of all invertible elements of A, and by $M_n(A)$ the ring of all $n \times n$-matrices with entries in A, and put $GL_n(R) = M_n(A)^\times$. The identity element of $M_n(A)$ is denoted by 1_n, or simply by 1, and the transpose of a matrix X by ${}^tX$. If A is commutative, we put

$$SL_n(A) = \{\alpha \in GL_n(A) \mid \det(\alpha) = 1\}.$$

Given a (2×2)-matrix γ with coefficients in any ring, we put $\gamma = \begin{bmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{bmatrix}$ whenever no confusion is expected. We now put

$$H = \{\, z \in \mathbf{C} \mid \mathrm{Im}(z) > 0 \,\}, \tag{1.1a}$$

$$G = GL_2(\mathbf{Q}), \qquad G^1 = SL_2(\mathbf{Q}), \tag{1.1b}$$

$$G_{\mathbf{a}} = GL_2(\mathbf{R}), \qquad G^1_{\mathbf{a}} = SL_2(\mathbf{R}), \tag{1.1c}$$

$$G_{\mathbf{a}+} = \{\alpha \in GL_n(\mathbf{R}) \mid \det(\alpha) > 0\}, \qquad G_+ = G \cap G_{\mathbf{a}+}. \tag{1.1d}$$

For $\gamma \in G_{\mathbf{a}+}$ and $z \in H$ we define $\gamma(z) \in H$ and $j_\gamma(z) \in \mathbf{C}^\times$ by

$$\gamma(z) = \gamma z = (a_\gamma z + b_\gamma)/(c_\gamma z + d_\gamma), \tag{1.2a}$$

$$j(\gamma, z) = j_\gamma(z) = \det(\gamma)^{-1/2}(c_\gamma z + d_\gamma). \tag{1.2b}$$

These can be expressed by a single equality

$$\det(\gamma)^{-1/2}\gamma \begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} \gamma(z) \\ 1 \end{bmatrix} j_\gamma(z). \tag{1.3}$$

We recall easy relations

(1.4a) $$j_{\alpha\beta}(z) = j_\alpha(\beta z) j_\beta(z),$$

(1.4b) $$\mathrm{Im}(\alpha z) = |j_\alpha(z)|^{-2}\mathrm{Im}(z), \qquad d(\alpha z)/dz = j_\alpha(z)^{-2}.$$

In fact, we can define γz by (1.2a) even for $\gamma \in GL_2(\mathbf{C})$ and $z \in \mathbf{C} \cup \{\infty\}$. Then the last formula of (1.4b) is meaningful for $\alpha \in GL_2(\mathbf{C})$.

1.2. For a function $f : H \to \mathbf{C}$, $k \in \mathbf{Z}$, and $\alpha \in G_{\mathbf{a}+}$, we define $f\|_k\alpha : H \to \mathbf{C}$ by

(1.5) $$(f\|_k\alpha)(z) = j_\alpha(z)^{-k} f(\alpha(z)) \qquad (z \in H).$$

We have

(1.6a) $$f\|_k(\alpha\beta) = (f\|_k\alpha)\|_k\beta,$$

(1.6b) $$f\|_k(c1_2) = \mathrm{sgn}(c)^k f \quad \text{if} \quad c \in \mathbf{R}^\times.$$

For a positive integer N we put

(1.7a) $$\Gamma(N) = \{\, \gamma \in SL_2(\mathbf{Z}) \mid \gamma \equiv 1_2 \pmod{N} \,\},$$

(1.7b) $$\Gamma^0(N) = \{\, \gamma \in SL_2(\mathbf{Z}) \mid b_\gamma \in N\mathbf{Z} \,\},$$

(1.7c) $$\Gamma_0(N) = \{\, \gamma \in SL_2(\mathbf{Z}) \mid c_\gamma \in N\mathbf{Z} \,\},$$

(1.7d) $$\Gamma_1(N) = \{\, \gamma \in \Gamma_0(N) \mid a_\gamma - 1 \in N\mathbf{Z} \,\}.$$

Then $\Gamma(1) = SL_2(\mathbf{Z})$, $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$, and $\Gamma(N)$ is a normal subgroup of $\Gamma(1)$. We call a sugroup of $\Gamma(1)$ a **congruence subgroup** if it contains $\Gamma(N)$ as a subgroup of finite index for some N.

1.3. Let us now recall the definition of a modular form. We refer the reader to [S71] for the basic facts on this subsect. We first put, for $c \in \mathbf{C}$,

(1.8) $$\mathbf{e}(c) = \exp(2\pi i c).$$

Given a congruence subgroup Γ and an integer k, we call a holomorphic function f on H a (holomorphic) **modular form of weight k with respect to Γ** if the following two conditions are satisfied:

(1.9a) *$f\|_k\gamma = f$ for every $\gamma \in \Gamma$.*

(1.9b) *For every $\alpha \in \Gamma(1)$ one has $(f\|_k\alpha)(z) = \sum_{n=0}^{\infty} c_{\alpha n} \cdot \mathbf{e}(nz/N_\alpha)$ with $c_{\alpha n} \in \mathbf{C}$ and $0 < N_\alpha \in \mathbf{Z}$.*

We denote by $\mathscr{M}_k(\Gamma)$ the set of all such f. The last condition implies in particular

(1.10) $$f(z) = \sum_{n=0}^{\infty} c_n \cdot \mathbf{e}(nz/N)$$

with $c_n \in \mathbf{C}$ and $0 < N \in \mathbf{Z}$. It is known that: (i) $\mathscr{M}_k(\Gamma)$ is a complex vector space of finite dimension; (ii) $\mathscr{M}_k(\Gamma) = \{0\}$ if $k < 0$; (iii) $\mathscr{M}_0(\Gamma) = \mathbf{C}$. From (1.6b) we see that $\mathscr{M}_k(\Gamma) = \{0\}$ if k is odd and $-1 \in \Gamma$. It is often convenient to consider modular forms without referring to Γ, so we put

$$\mathscr{M}_k = \bigcup_{\Gamma} \mathscr{M}_k(\Gamma), \tag{1.11}$$

where Γ runs over all congruence subgroups of $\Gamma(1)$. We call an element f of $\mathscr{M}_k$ a **cusp form** if $c_{\alpha 0}$ of (1.9b) is 0 for every $\alpha \in \Gamma(1)$. We denote by $\mathscr{S}_k$ the subset of $\mathscr{M}_k$ consisting of all the cusp forms, and put $\mathscr{S}_k(\Gamma) = \mathscr{S}_k \cap \mathscr{M}_k(\Gamma)$. For example, we recall a classical fact that $\mathscr{S}_{12}(\Gamma(1)) = \mathbf{C}\Delta$ with

$$\Delta(z) = \mathbf{q} \prod_{n=1}^{\infty} (1 - \mathbf{q}^n)^{24}, \qquad \mathbf{q} = \mathbf{e}(z). \tag{1.12}$$

Moreover, for $r \in \mathbf{Z}$ the function $\Delta^{r/24}$ can be defined by

$$\Delta^{r/24}(z) = \mathbf{e}(rz/24) \prod_{n=1}^{\infty} (1 - \mathbf{q}^n)^r, \tag{1.13}$$

and $\Delta^{r/24}(z) \in \mathscr{S}_{r/2}$ if $0 < r \in 2\mathbf{Z}$. These functions are nonzero everywhere on H. Let us now put

$$P_+ = \{\alpha \in G_+ \mid c_\alpha = 0\}. \tag{1.14}$$

Clearly $P_+ = \{\alpha \in G_+ \mid \alpha(\infty) = \infty\}$. We have

$$G_+ = \Gamma(1) P_+. \tag{1.15}$$

Indeed, if $\alpha \in G_+$ and $\alpha(\infty) \neq \infty$, then we can put $\alpha(\infty) = a/c$ with integers a and c that are relatively prime. We can find integers b and d such that $ad - bc = 1$. Put $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then $\gamma \in \Gamma(1)$ and $\gamma(\infty) = a/c = \alpha(\infty)$, and so $\gamma^{-1}\alpha \in P_+$. This proves (1.15). Because of this equality, we can replace $\Gamma(1)$ in condition (1.9b) by G_+.

1.4. Given a subfield Φ of $\mathbf{C}$, we denote by $\mathscr{M}_k(\Phi, \Gamma)$ the set of all elements f of $\mathscr{M}_k(\Gamma)$ of the form (1.10) with $c_n \in \Phi$ for all n. We then put $\mathscr{S}_k(\Phi, \Gamma) = \mathscr{S}_k \cap \mathscr{M}_k(\Phi, \Gamma)$. Furthermore, we put

$$\mathscr{M}_k(\Phi) = \bigcup_{\Gamma} \mathscr{M}_k(\Phi, \Gamma), \qquad \mathscr{S}_k(\Phi) = \bigcup_{\Gamma} \mathscr{S}_k(\Phi, \Gamma),$$

where Γ runs over all congruence subgroups of $\Gamma(1)$.

We extend this to meromorphic functions as follows. For $m \in \mathbf{Z}$ and Φ as above, we denote by $\mathscr{A}_m(\Phi)$ the set of all quotients p/q such that $p \in \mathscr{M}_{k+m}(\Phi)$ and $0 \neq q \in \mathscr{M}_k(\Phi)$ with any $k \in \mathbf{Z}, > 0$. We then put $\mathscr{A}_m = \mathscr{A}_m(\mathbf{C})$,

$$\mathscr{A}_m(\Gamma) = \{f \in \mathscr{A}_m \mid f\|_m\gamma = f \text{ for every } \gamma \in \Gamma\},$$
$$\mathscr{A}_m(\Phi, \Gamma) = \mathscr{A}_m(\Phi) \cap \mathscr{A}_m(\Gamma).$$

We call the elements of $\mathscr{A}_m(\Phi)$ **Φ-rational.** The elements of $\mathscr{A}_0(\Gamma)$ are called **modular functions** with respect to Γ. The orbit space $\Gamma\backslash(H \cup \mathbf{Q} \cup \{\infty\})$ has a structure of a compact Riemann surface, which can be presented as an algebraic curve defined over an algebraic number field. Thus $\mathscr{A}_0(\Phi, \Gamma)$ can be identified with the field of all algebraic functions on that curve over Φ for a suitable choice of Φ. For these the reader is referred to [S71, §6.7].

Let $\mathbf{Q}_{\mathrm{ab}}$ denote the maximal abelian extension of $\mathbf{Q}$ in $\mathbf{C}$. Then the field $\mathscr{A}_0(\mathbf{Q}_{\mathrm{ab}})$ is stable under the maps $f \mapsto f \circ \alpha$ for all $\alpha \in G_+$. To show this, by (1.15) we can reduce the problem to the cases where α belongs to $\Gamma(1)$ or P_+. The case $\alpha \in P_+$ is obvious. If $\alpha \in \Gamma(1)$, the result can be derived from the fact that $\mathscr{A}_0((\Gamma(N))$ is generated by $J(z)$ and "modified" N-division values of the Weierstrass $\wp$-function as stated in [S71, Proposition 6.9]. In [S71] the field $\mathscr{A}_0(\mathbf{Q}_{\mathrm{ab}})$ is denoted by $\mathfrak{F}$, and the stability of $\mathfrak{F}$ under G_+ is given in [S71, Proposition 6.22]. Somewhat more strongly we have

Theorem 1.5. *Let Φ be a subfield of $\mathbf{C}$ containing $\mathbf{Q}_{\mathrm{ab}}$. Then $f\|_m\alpha \in \mathscr{A}_m(\Phi)$ for every $f \in \mathscr{A}_m(\Phi)$ and every $\alpha \in G_+$. In particular, $f\|_m\alpha \in \mathscr{M}_m(\Phi)$ for every $\alpha \in G_+$ if $f \in \mathscr{M}_m(\Phi)$,*

PROOF. The field $\mathscr{A}_0$ is the composite of $\mathbf{C}$ and $\mathscr{A}_0(\mathbf{Q}_{\mathrm{ab}})$; also, $\mathscr{A}_0(\mathbf{Q}_{\mathrm{ab}})$ and $\mathbf{C}$ are linearly disjoint over $\mathbf{Q}_{\mathrm{ab}}$; see [S71, Proposition 6.1, Theorem 6.6 (4), Proposition 6.27]. Therefore $\mathscr{A}_0(\Phi)$ is the composite of Φ and $\mathscr{A}_0(\mathbf{Q}_{\mathrm{ab}})$, and so it is stable under G_+. Since $G_+ = \Gamma(1)P_+$ and our theorem is clear for $\alpha \in P_+$, it is sufficient to prove the case $\alpha \in \Gamma(1)$. Given $f \in \mathscr{A}_m(\Phi)$, we put $h = f/g$ with $g = \Delta^{m/12}$. From (1.13) we see that $g \in \mathscr{A}_m(\mathbf{Q})$, and so $h \in \mathscr{A}_0(\Phi)$. Thus $h \circ \alpha \in \mathscr{A}_0(\Phi)$ for every $\alpha \in \Gamma(1)$ for the reason explained above. Since $\Delta\|_{12}\alpha = \Delta$, we see that $g\|_m\alpha$ is g times a twelfth root of unity, and so it is contained in $\mathscr{A}_m(\Phi)$. This proves the first assertion of our theorem, as $f\|_m\alpha = (h \circ \alpha)g\|_m\alpha$, from which the assertion for $f \in \mathscr{M}_m(\Phi)$ follows immediately.

Lemma 1.6. *For a function f on H given by $f(z) = \sum_{n=0}^{\infty} a_n \mathbf{e}(nz/N)$ with $a_n \in \mathbf{C}$ and $0 < N \in \mathbf{Z}$, the following assertions hold. (In each statement, α is a positive constant.)*

(i) $f(x+iy) - a_0 = O(e^{-2\pi y/N})$ *uniformly as* $y \to \infty$.

(ii) $a_n = O(n^\alpha) \implies f(x+iy) = O(y^{-\alpha-1})$ *uniformly as* $y \to 0$.

(iii) $\sum_{n=0}^{\infty} |a_n| n^{-\alpha} < \infty \implies f(x+iy) = O(y^{-\alpha})$ *uniformly as* $y \to 0$.

(iv) $f(x+iy) = O(y^{-\alpha})$ *uniformly as* $y \to 0 \implies a_n = O(n^\alpha)$.

(v) $\overline{f(z)} = f(-\overline{z})$ *if* $a_n \in \mathbf{R}$ *for all* n.

PROOF. Changing f for $f(Nz)$, we may assume that $N = 1$. Assertion (i) is clear, as f is a convergent power series in $e^{2\pi iz}$. We will prove (ii) in the next section after (2.14). To prove (iii), let $g = f - a_0$. Then $\sum_{k=1}^{n} |a_k| \le \sum_{k=1}^{n} |a_k|(n/k)^\alpha \le n^\alpha \sum_{k=1}^{n} |a_k| k^{-\alpha} \le Bn^\alpha$ with some $B > 0$. Thus $\bigl(1 - e^{-2\pi y}\bigr)^{-1}|g(z)| \le \sum_{m=0}^{\infty} e^{-2\pi my} \cdot \sum_{n=1}^{\infty} |a_n| e^{-2\pi ny} = \sum_{n=1}^{\infty} e^{-2\pi ny} \sum_{k=1}^{n} |a_k| \le B\sum_{n=1}^{\infty} n^\alpha e^{-2\pi ny} = O(y^{-\alpha-1})$ as in (ii). Therefore we obtain (iii), as $1 - e^{-2\pi y} = O(y)$ as $y \to 0$. For f as in (iv) we have $|a_n e^{-2\pi ny}| = \bigl|\int_0^1 f(x+iy)e^{-2\pi inx}\,dx\bigr| \le$

$Ay^{-\alpha}$ with some $A > 0$ for sufficiently small y. Taking $y = 1/n$, we obtain (iv). The last assertion is an easy exercise.

Lemma 1.7. *Given $f \in \mathscr{M}_k$, there exists a positive constant K such that $|f(z)| \le K(1 + y^{-k})$ on the whole H. If $f \in \mathscr{S}_k$, then we can take K so that $|f(z)| \le Ky^{-k/2}$ on the whole H.*

PROOF. Suppose $f \in \mathscr{M}_k(\Gamma)$. Let $T = \{z \in H \,|\, \mathrm{Im}(z) > 1/2\}$. Since T contains the well known fundamental domian for $\Gamma(1)\backslash H$, we have $H = \Gamma(1)T$, and so we can find a finite subset A of $\Gamma(1)$ such that $H = \bigcup_{\alpha\in A} \Gamma\alpha T$. Put $f_\alpha = f\|_k\alpha$. Given $z \in H$, there exists $\alpha \in A$ such that $z \in \gamma\alpha T$ with some $\gamma \in \Gamma$. Put $\beta = \alpha^{-1}\gamma^{-1}$. Then $f = f\|_k\alpha\beta = f_\alpha\|_k\beta = j_\beta(z)^{-k}f_\alpha(\beta z)$. Now f_α is bounded on T, and hence there is a positive constant K such that $|f_\alpha(w)| \le K$ for every $w \in T$ and every $\alpha \in A$. Thus $|f(z)| \le K|c_\beta z + d_\beta|^{-k}$, as $\beta z \in T$. If $c_\beta \ne 0$, then $|f(z)| \le K|c_\beta y|^{-k} \le Ky^{-k}$, as $|c_\beta| \ge 1$; if $c_\beta = 0$, then $|f(z)| \le K$. This proves the first assertion. Suppose that f is a cusp form. Put $g(z) = y^k|f|^2$ and observe that g is Γ-invariant and $g \circ \alpha = y^k|f_\alpha|^2$, which is bounded on T, as f_α is a cusp form; see Lemma 1.6 (i). Thus we can find a positive constant M such that $|g(\alpha z)| \le M$ for every $\alpha \in A$ and $z \in T$. Given $z \in H$, take $\gamma \in \Gamma$, $\alpha \in A$, and $w \in T$ so that $z = \gamma\alpha w$. Then $|y^k f(z)^2| = g(z) = g(\gamma\alpha w) = g(\alpha w) \le M$. This completes the proof.

Lemma 1.8. *If $f(z) = \sum_{n=0}^{\infty} a_n \mathbf{e}(nz/N) \in \mathscr{M}_k$, then $a_n = O(n^k)$. If in particular f is a cusp form, then $a_n = O(n^{k/2})$.*

This follows from Lemma 1.6 (iv) combined with Lemma 1.7.

Theorem 1.9. (i) *For every $k \in \mathbf{Z}$, > 0, we have $\mathscr{M}_k = \mathscr{M}_k(\mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$.*

(ii) *Given $f(z) = \sum_{n=0}^{\infty} a_n \mathbf{e}(nz/N) \in \mathscr{M}_k$ and a field-automorphism σ of $\mathbf{C}$, define an infinite series $f^\sigma(z)$ formally by $f^\sigma(z) = \sum_{n=0}^{\infty} a_n^\sigma \mathbf{e}(nz/N)$. Then this defines a holomorphic function on H and $f^\sigma \in \mathscr{M}_k$.*

PROOF. Assertion (i) can easily be derived from the facts that the curve $C = \Gamma(N)\backslash(H \cup \mathbf{Q} \cup \{\infty\})$ has a $\mathbf{Q}$-rational model and that for every $\mathbf{Q}$-rational divisor X on C the linear system $\mathscr{L}(X)$ has a basis contained in $\mathscr{A}_0(\mathbf{Q}, \Gamma(N))$. These are explained in [S00, pp. 62–64] in a more general case; (i) is actually a special case of [S00, Theorem 9.9]. Given f as in (ii), we can put, in view of (i), $f = \sum_{g\in X} c_g g$ with a finite subset X of $\mathscr{M}_k(\mathbf{Q})$ and $c_g \in \mathbf{C}$. Then clearly $f^\sigma = \sum_{g\in X} c_g^\sigma g$, which proves (ii).

We can also prove that $\mathscr{M}_k(\mathbf{Q})$ can be spanned by the elements whose Fourier coefficients at ∞ are contained in $\mathbf{Z}$; see [S75d, Theorem 1] and [S76a, pp. 682–683]. See also [S71, Theorem 3.32], though the result stated there concerns only cusp forms. We will present explicit examples of generators of $\sum_{k=0}^{\infty} \mathscr{M}_k(\mathbf{Q})$ in Section 10.

1.10. In this and next subsections we recall some basic terms such as elliptic points and cusps, and discuss how they are related to the dimension formula for $\mathscr{M}_k(\Gamma)$. The full treatment of these topics can be found in the first two chapters of [S71]. First of all, we call an element α of G^1 **elliptic** if $\alpha \neq \pm 1$ and α has a fixed point on H. Such a fixed point is unique for α. Let Γ be a congruence subgroup of $\Gamma(1)$. An element $\alpha, \neq \pm 1$, of Γ is elliptic if and only if α is of finite order. The order of an elliptic element of Γ is 3, 4, or 6. By an **elliptic point** of Γ we understand a point fixed by an elliptic element of Γ. The images of an elliptic point of Γ under Γ are also elliptic points of Γ. We can then find a finite complete set of representatives for the elliptic points of Γ modulo Γ. Given an elliptic point w of Γ, we put

$$\overline{\Gamma}_w = \{\gamma \in \{\pm 1\}\Gamma \mid \gamma(w) = w\}. \tag{1.16}$$

Then $\overline{\Gamma}_w/\{\pm 1\}$ is of order 2 or 3. We call w an elliptic point of Γ of **order** 2 or 3 accordingly.

Next, there is a notion of a **cusp.** Since we are considering a subgroup Γ of $\Gamma(1)$, the set of cusps of Γ is merely $\mathbf{Q} \cup \{\infty\}$. Put

$$P^1 = \{\alpha \in G^1 \mid c_\alpha = 0\}, \qquad \Gamma_P = \Gamma \cap P^1. \tag{1.17}$$

In view of (1.15) we have $G^1 = \Gamma(1)P_1$, and the map $\alpha \mapsto \alpha(\infty)$ gives a bijection of $\Gamma(1)/\Gamma(1)_P$ onto $\mathbf{Q} \cup \{\infty\}$. Thus $\Gamma \backslash (\mathbf{Q} \cup \{\infty\})$ can be identified with $\Gamma \backslash \Gamma(1)/\Gamma(1)_P$, which is clearly a finite set. For $s \in \mathbf{Q} \cup \{\infty\}$ put

$$\Gamma_s = \{\alpha \in \Gamma \mid \alpha(s) = s\} \tag{1.18}$$

and let ρ be an element of $\Gamma(1)$ such that $\rho(s) = \infty$. Then we can find a positive integer h such that

$$\{\pm 1\}\rho\Gamma_s\rho^{-1} = \{\pm 1\}\left\{ \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^n \,\middle|\, n \in \mathbf{Z} \right\}. \tag{1.19}$$

If $-1 \in \Gamma$, we have $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \rho\Gamma_s\rho^{-1}$. If $-1 \notin \Gamma$, however, there are two possibilities; $\rho\Gamma_s\rho^{-1}$ is generated by $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ or by $-\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$. We say that s is a **regular cusp** or an **irregular cusp** of Γ accordingly. This definition does not depend on the choice of ρ. (We can define these with $\rho \in SL_2(\mathbf{R})$. Since our group Γ is contained in $\Gamma(1)$, we can restrict ρ to $\Gamma(1)$. Then h is always a positive integer.)

1.11. We fix a congruence subgroup of $\Gamma(1)$ and let ν_2 resp. ν_3 denote the number of Γ-inequivalent elliptic points of order 2 resp. 3. Further let m be the number of orbits in $\Gamma \backslash (\mathbf{Q} \cup \{\infty\})$. Then the genus g of the compact Riemann surface $\Gamma \backslash (H \cup \mathbf{Q} \cup \{\infty\})$ is determined by