Chapter VII

Modular Forms

§1. *The modular group*

1.1. *Definitions*

Let H denote the upper half plane of $\mathbf{C}$, i.e. the set of complex numbers z whose imaginary part $Im(z)$ is >0.

Let $\mathbf{SL}_2(\mathbf{R})$ be the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with real coefficients, such that $ad-bc = 1$. We make $\mathbf{SL}_2(\mathbf{R})$ act on $\tilde{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$ in the following way:

if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of $\mathbf{SL}_2(\mathbf{R})$, and if $z \in \tilde{\mathbf{C}}$, we put

$$gz = \frac{az+b}{cz+d}.$$

One checks easily the formula

$$Im(gz) = \frac{Im(z)}{|cz+d|^2}. \tag{1}$$

This shows that H is *stable* under the action of $\mathbf{SL}_2(\mathbf{R})$. Note that the element $-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ of $\mathbf{SL}_2(\mathbf{R})$ acts trivially on H. We can then consider that it is the group $\mathbf{PSL}_2(\mathbf{R}) = \mathbf{SL}_2(\mathbf{R})/\{\pm 1\}$ which operates (and this group acts *faithfully*—one can even show that it is the group of all analytic automorphisms of H).

Let $\mathbf{SL}_2(\mathbf{Z})$ be the subgroup of $\mathbf{SL}_2(\mathbf{R})$ consisting of the matrices with coefficients in $\mathbf{Z}$. It is a discrete subgroup of $\mathbf{SL}_2(\mathbf{R})$.

Definition 1.—*The group* $G = \mathbf{SL}_2(\mathbf{Z})/\{\pm 1\}$ *is called the modular group; it is the image of* $\mathbf{SL}_2(\mathbf{Z})$ *in* $\mathbf{PSL}_2(\mathbf{R})$.

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of $\mathbf{SL}_2(\mathbf{Z})$, we often use the same symbol to denote its image in the modular group G.

1.2. *Fundamental domain of the modular group*

Let S and T be the elements of G defined respectively by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. One has:

$$Sz = -1/z, \qquad Tz = z+1$$
$$S^2 = 1, \qquad (ST)^3 = 1$$

On the other hand, let D be the subset of H formed of all points z such that $|z| \geqq 1$ and $|Re(z)| \leqq 1/2$. The figure below represents the transforms of D by the elements:

$\{1, T, TS, ST^{-1}S, S, ST, STS, T^{-1}S, T^{-1}\}$ of the group G.

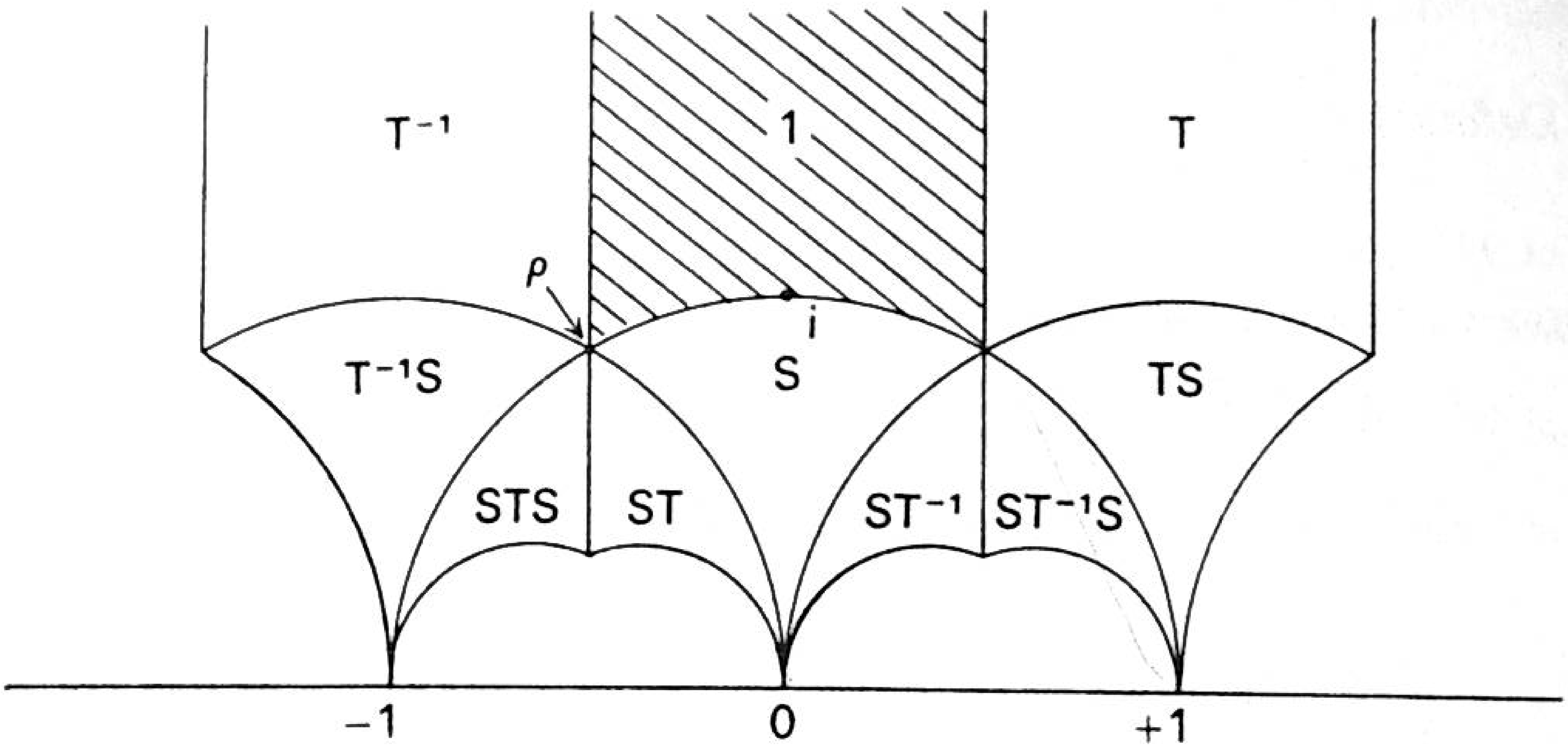

Fig. 1

We will show that D is a *fundamental domain* for the action of G on the half plane H. More precisely:

Theorem 1.—(1) *For every $z \in H$, there exists $g \in G$ such that $gz \in D$.*

(2) *Suppose that two distinct points z, z' of D are congruent modulo G. Then, $R(z) = \pm\frac{1}{2}$ and $z = z' \pm 1$, or $|z| = 1$ and $z' = -1/z$.*

(3) *Let $z \in D$ and let $I(z) = \{g | g \in G, gz = z\}$ the stabilizer of z in G. One has $I(z) = \{1\}$ except in the following three cases:*

$z = i$, in which case $I(z)$ is the group of order 2 generated by S;

$z = \rho = e^{2\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by ST;

$z = -\bar{\rho} = e^{\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by TS.

Assertions (1) and (2) imply:

Corollary.—*The canonical map $D \to H/G$ is surjective and its restriction to the interior of D is injective.*

Theorem 2.—*The group G is generated by S and T.*

Proof of theorems 1 *and* 2.—Let G' be the subgroup of G generated by S and T, and let $z \in H$. We are going to show that *there exists $g' \in G'$ such that $g'z \in D$*, and this will prove assertion (1) of theorem 1. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of G', then

(1) $$Im(gz) = \frac{Im(z)}{|cz+d|^2}.$$

Since c and d are integers, the numbers of pairs (c, d) such that $|cz+d|$ is less than a given number is *finite*. This shows that there exists $g \in G'$ such that $Im(gz)$ is maximum. Choose now an integer n such that $T^n gz$ has real part between $-\frac{1}{2}$ and $+\frac{1}{2}$. The element $z' = T^n gz$ *belongs to* D; indeed, it suffices to see that $|z'| \geqq 1$, but if $|z'| < 1$, the element $-1/z'$ would have an imaginary part strictly larger than $Im(z')$, which is impossible. Thus the element $g' = T^n g$ has the desired property.

We now prove assertions (2) and (3) of theorem 1. Let $z \in D$ and let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ such that $gz \in D$. Being free to replace (z, g) by (gz, g^{-1}), we may suppose that $Im(gz) \geqq Im(z)$, i.e. that $|cz+d|$ is $\leqq 1$. This is clearly impossible if $|c| \geqq 2$, leaving then the cases $c = 0, 1, -1$. If $c = 0$, we have $d = \pm 1$ and g is the translation by $\pm b$. Since $R(z)$ and $R(gz)$ are both between $-\frac{1}{2}$ and $\frac{1}{2}$, this implies either $b = 0$ and $g = 1$ or $b = \pm 1$ in which case one of the numbers $R(z)$ and $R(gz)$ must be equal to $-\frac{1}{2}$ and the other to $\frac{1}{2}$. If $c = 1$, the fact that $|z+d|$ is $\leqq 1$ implies $d = 0$ except if $z = \rho$ (resp. $-\bar{\rho}$) in which case we can have $d = 0, 1$ (resp, $d = 0, -1$). The case $d = 0$ gives $|z| \leq 1$ hence $|z| = 1$; on the other hand, $ad-bc = 1$ implies $b = -1$, hence $gz = a-1/z$ and the first part of the discussion proves that $a = 0$ except if $R(z) = \pm\frac{1}{2}$, i.e. if $z = \rho$ or $-\bar{\rho}$ in which case we have $a = 0, -1$ or $a = 0, 1$. The case $z = \rho$, $d = 1$ gives $a-b = 1$ and $g\rho = a-1/(1+\rho) = a+\rho$, hence $a = 0, 1$; we argue similarly when $z = -\bar{\rho}$, $d = -1$. Finally the case $c = -1$ leads to the case $c = 1$ by changing the signs of a, b, c, d (which does not change g, viewed as an element of G). This completes the verification of assertions (2) and (3).

It remains to prove that $G' = G$. Let g be an element of G. Choose a point z_0 *interior* to D (for example $z_0 = 2i$), and let $z = gz_0$. We have seen above that there exists $g' \in G'$ such that $g'z \in D$. The points z_0 and $g'z = g'gz_0$ of D are congruent modulo G, and one of them is interior to D. By (2) and (3), it follows that these points coincide and that $g'g = 1$. Hence we have $g \in G'$, which completes the proof.

Remark.—One can show that $\langle S, T;\ S^2, (ST)^3 \rangle$ is a *presentation* of G, or, equivalently, that G is the *free product of the cyclic group of order* 2 *generated by* S *and the cyclic group of order* 3 *generated by* ST.

§2. *Modular functions*

2.1. *Definitions*

Definition 2.—*Let k be an integer. We say a function f is weakly modular of weight $2k$*[1] *if f is meromorphic on the half plane H and verifies the relation*

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \quad \textit{for all} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}). \tag{2}$$

[1] Some authors say that f is "of weight $-2k$", others that f is "of weight k".

Let g be the image in G of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We have $d(gz)/dz = (cz+d)^{-2}$. The relation (2) can then be written:

$$\frac{f(gz)}{f(z)} = \left(\frac{d(gz)}{dz}\right)^{-k}$$

or

$$f(gz)d(gz)^k = f(z)dz^k. \tag{3}$$

It means that the "differential form of weight k" $f(z)dz^k$ is *invariant* under G. Since G is generated by the elements S and T (see th. 2), it suffices to check the invariance by S and by T. This gives:

Proposition 1.—*Let f be meromorphic on H. The function f is a weakly modular function of weight $2k$ if and only if it satisfies the two relations*:

$$f(z+1) = f(z) \tag{4}$$

$$f(-1/z) = z^{2k}f(z). \tag{5}$$

Suppose the relation (4) is verified. We can then express f as a function of $q = e^{2\pi iz}$, function which we will denote by $\tilde{f}$; it is meromorphic in the disk $|q| < 1$ with the origin removed. If $\tilde{f}$ extends to a meromorphic (resp. holomorphic) function at the origin, we say, by abuse of language, that f is *meromorphic* (resp. *holomorphic*) *at infinity*. This means that $\tilde{f}$ admits a Laurent expansion in a neighborhood of the origin

$$\tilde{f}(q) = \sum_{-\infty}^{+\infty} a_n q^n$$

where the a_n are zero for n small enough (resp. for $n < 0$).

Definition 3.—*A weakly modular function is called modular if it is meromorphic at infinity.*

When f is holomorphic at infinity, we set $f(\infty) = \tilde{f}(0)$. This is the *value* of f at infinity.

Definition 4.—*A modular function which is holomorphic everywhere (including infinity) is called a modular form; if such a function is zero at infinity, it is called a cusp form ("Spitzenform" in German—"forme parabolique" in French).*

A modular form of weight $2k$ is thus given by a series

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi inz} \tag{6}$$

which converges for $|q| < 1$ (i.e. for $Im(z) > 0$), and which verifies the identity

$$f(-1/z) = z^{2k}f(z). \tag{5}$$

It is a cusp form if $a_0 = 0$.

Examples

1) If f and f' are modular forms of weight $2k$ and $2k'$, the product ff' is a modular form of weight $2k+2k'$.

2) We will see later that the function

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} = q-24q^2+252q^3-1472q^4+\dots$$

is a cusp form of weight 12.

2.2. *Lattice functions and modular functions*

We recall first what is a *lattice* in a real vector space V of finite dimension. It is a subgroup Γ of V verifying one of the following equivalent conditions:

i) Γ is discrete and V/Γ is compact;
ii) Γ is discrete and generates the **R**-vector space V;
iii) There exists an **R**-basis $(e_1, \dots, e_n)$ of V which is a **Z**-basis of Γ (i.e. $\Gamma = \mathbf{Z}e_1 \oplus \dots \oplus \mathbf{Z}e_n$).

Let $\mathscr{R}$ be the *set of lattices* of **C** considered as an **R**-vector space. Let M be the set of pairs (ω_1, ω_2) of elements of $\mathbf{C}^*$ such that $Im(\omega_1/\omega_2) > 0$; to such a pair we associate the lattice

$$\Gamma(\omega_1, \omega_2) = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$$

with basis $\{\omega_1, \omega_2\}$. We thus obtain a map $M \to \mathscr{R}$ which is clearly *surjective*.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$ and let $(\omega_1, \omega_2) \in M$. We put

$$\omega_1' = a\omega_1 + b\omega_2 \quad \text{and} \quad \omega_2' = c\omega_1 + d\omega_2.$$

It is clear that $\{\omega_1', \omega_2'\}$ is a basis of $\Gamma(\omega_1, \omega_2)$. Moreover, if we set $z = \omega_1/\omega_2$ and $z' = \omega_1'/\omega_2'$, we have

$$z' = \frac{az+b}{cz+d} = gz.$$

This shows that $Im(z') > 0$, hence that (ω_1', ω_2') belongs to M.

Proposition 2.—*For two elements of M to define the same lattice it is necessary and sufficient that they are congruent modulo* $\mathbf{SL}_2(\mathbf{Z})$.

We just saw that the condition is sufficient. Conversely, if (ω_1, ω_2) and (ω_1', ω_2') are two elements of M which define the same lattice, there exists an integer matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of determinant ± 1 which transforms the first basis into the second. If $\det(g)$ was <0, the sign of $Im(\omega_1'/\omega_2')$ would be *the opposite* of $Im(\omega_1/\omega_2)$ as one sees by an immediate computation. The two signs being the same, we have necessarily $\det(g) = 1$ which proves the proposition.

Hence we can identify the *set $\mathscr{R}$ of lattices of* **C** *with the quotient of M by the action of* $\mathbf{SL}_2(\mathbf{Z})$.

Make now $\mathbf{C}^*$ act on $\mathscr{R}$ (resp. on M) by:

$$\Gamma \mapsto \lambda\Gamma \quad \text{(resp. } (\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)\text{)}, \quad \lambda \in \mathbf{C}^*.$$

The quotient $M/\mathbf{C}^*$ is identified with H by $(\omega_1, \omega_2) \mapsto z = \omega_1/\omega_2$, and this identification transforms the action of $\mathbf{SL}_2(\mathbf{Z})$ on M into that of $G = \mathbf{SL}_2(\mathbf{Z})/\{\pm 1\}$ on H (cf. n° 1.1). Hence:

Proposition 3.—*The map $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$ gives by passing to the quotient, a bijection of $\mathscr{R}/\mathbf{C}^*$ onto H/G.* (Thus, an element of H/G can be identified with a lattice of $\mathbf{C}$ defined up to a homothety.)

Remark.—Let us associate to a lattice Γ of $\mathbf{C}$ the *elliptic curve* $E_\Gamma = \mathbf{C}/\Gamma$. It is easy to see that two lattices Γ and Γ' define isomorphic elliptic curves if and only if they are homothetic. This gives a third description of $H/G = \mathscr{R}/\mathbf{C}^*$: it is the set of *isomorphism classes of elliptic curves.*

Let us pass now to *modular functions.* Let F be a function on $\mathscr{R}$, with complex values, and let $k \in \mathbf{Z}$. We say that F is of *weight* $2k$ if

$$F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma) \tag{7}$$

for all lattices Γ and all $\lambda \in \mathbf{C}^*$.

Let F be such a function. If $(\omega_1, \omega_2) \in M$, we denote by $F(\omega_1, \omega_2)$ the value of F on the lattice $\Gamma(\omega_1, \omega_2)$. The formula (7) translates to:

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k}F(\omega_1, \omega_2). \tag{8}$$

Moreover, $F(\omega_1, \omega_2)$ is invariant by the action of $\mathbf{SL}_2(\mathbf{Z})$ on M.

Formula (8) shows that the product $\omega_2^{2k}F(\omega_1, \omega_2)$ depends only on $z = \omega_1/\omega_2$. There exists then a function f on H such that

$$F(\omega_1, \omega_2) = \omega_2^{-2k}f(\omega_1/\omega_2). \tag{9}$$

Writing that F is invariant by $\mathbf{SL}_2(\mathbf{Z})$, we see that f satisfies the identity:

$$f(z) = (cz+d)^{-2k}f\left(\frac{az+b}{cz+d}\right) \quad \text{for all} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}). \tag{2}$$

Conversely, if f verifies (2), formula (9) associates to it a function F on $\mathscr{R}$ which is of weight $2k$. We can thus identify *modular functions of weight* $2k$ with some *lattice functions of weight* $2k$.

2.3. *Examples of modular functions; Eisenstein series*

Lemma 1.—*Let Γ be a lattice in $\mathbf{C}$. The series $\sum'_{\gamma\in\Gamma} 1/|\gamma|^\sigma$ is convergent for $\sigma > 2$.*

(The symbol Σ' signifies that the summation runs over the nonzero elements of Γ.)

We can proceed as with the series $\Sigma 1/n^\alpha$, i.e. majorize the series under consideration by a multiple of the double integral $\displaystyle\iint \frac{dx\,dy}{(x^2+y^2)^{\sigma/2}}$ extended over the plane deprived of a disk with center 0. The double integral is easily computed using "polar coordinates". Another method, essentially equivalent, consists in remarking that the number of elements of Γ such that $|\gamma|$ is between two consecutive integers n and $n+1$ is $O(n)$; the convergence of the series is thus reduced to that of the series $\Sigma 1/n^{\sigma-1}$.

Now let k be an integer >1. If Γ is a lattice of $\mathbf{C}$, put

(10) $$G_k(\Gamma) = \sum_{\gamma \in \Gamma}' 1/\gamma^{2k}.$$

This series converges absolutely, thanks to lemma 1. It is clear that G_k is of *weight* $2k$. It is called the *Eisenstein series* of index k (or index $2k$ following other authors). As in the preceding section, we can view G_k as a function on M, given by:

(11) $$G_k(\omega_1, \omega_2) = \sum_{m,n}' \frac{1}{(m\omega_1 + n\omega_2)^{2k}}.$$

Here again the symbol Σ' means that the summation runs over all pairs of integers (m, n) *distinct from* $(0, 0)$. The function on H corresponding to G_k (by the procedure given in the preceding section) is again denoted by G_k. By formulas (9) and (11), we have

(12) $$G_k(z) = \sum_{m,n}' \frac{1}{(mz+n)^{2k}}.$$

Proposition 4.—*Let k be an integer >1. The Eisenstein series $G_k(z)$ is a modular form of weight $2k$. We have $G_k(\infty) = 2\zeta(2k)$ where ζ denotes the Riemann zeta function.*

The above arguments show that $G_k(z)$ is *weakly modular* of weight $2k$. We have to show that G_k is everywhere holomorphic (including infinity). First suppose that z is contained in the fundamental domain D (cf. n° 1.2). Then

$$\begin{aligned} |mz+n|^2 &= m^2 z\bar{z} + 2mnR(z) + n^2 \\ &\geqq m^2 - mn + n^2 = |m\rho - n|^2. \end{aligned}$$

By lemma 1, the series $\Sigma' 1/|m\rho - n|^{2k}$ is convergent. This shows that the series $G_k(z)$ *converges normally in* D, thus also (applying the result to $G_k(g^{-1}z)$ with $g \in G$) in each of the transforms gD of D by G. Since these cover H (th. 1), we see that G_k is holomorphic in H. It remains to see that G_k is holomorphic at infinity (and to find the value at this point). This amounts to proving that G_k has a limit for $Im(z) \to \infty$. But one may suppose that z remains in the fundamental domain D; in view of the uniform convergence in D, we can make the passage to the limit term by term. The terms $1/(mz+n)^{2k}$ relative to $m \neq 0$ give 0; the others give $1/n^{2k}$. Thus

$$\lim. G_k(z) = \sum{}' 1/n^{2k} = 2\sum_{n=1}^{\infty} 1/n^{2k} = 2\zeta(2k) \quad \text{q.e.d.}$$

Remark.—We give in n° 4.2 below the expansion of G_k as a power series in $q = e^{2\pi i z}$.

Examples.—The Eisenstein series of lowest weights are G_2 and G_3, which are of weight 4 and 6. It is convenient (because of the theory of elliptic curves) to replace these by multiples:

$$g_2 = 60G_2, \qquad g_3 = 140G_3. \tag{13}$$

We have $g_2(\infty) = 120\zeta(4)$ and $g_3(\infty) = 280\zeta(6)$. Using the known values of $\zeta(4)$ and $\zeta(6)$ (see for example n° 4.1 below), one finds:

$$g_2(\infty) = \frac{4}{3}\pi^4, \qquad g_3(\infty) = \frac{8}{27}\pi^6. \tag{14}$$

If we put

$$\Delta = g_2^3 - 27g_3^2, \tag{15}$$

we have $\Delta(\infty) = 0$; that is to say, *Δ is a cusp form of weight* 12.

Relation with elliptic curves

Let Γ be a lattice of $\mathbf{C}$ and let

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{\gamma\in\Gamma}{}' \left(\frac{1}{(u-\gamma)^2} - \frac{1}{\gamma^2}\right) \tag{16}$$

be the corresponding Weierstrass function[(1)]. The $G_k(\Gamma)$ occur into the Laurent expansion of $\wp_\Gamma$:

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{k=2}^{\infty} (2k-1)G_k(\Gamma)u^{2k-2}. \tag{17}$$

If we put $x = \wp_\Gamma(u)$, $y = \wp'_\Gamma(u)$, we have

$$y^2 = 4x^3 - g_2x - g_3, \tag{18}$$

with $g_2 = 60G_2(\Gamma)$, $g_3 = 140G_3(\Gamma)$ as above. Up to a numerical factor, $\Delta = g_2^3 - 27g_3^2$ is equal to the *discriminant* of the polynomial $4x^3 - g_2x - g_3$.

One proves that the cubic defined by the equation (18) in the projective plane is isomorphic to the elliptic curve $\mathbf{C}/\Gamma$. In particular, it is a *nonsingular curve*, and this shows that Δ is $\neq 0$.

§3. *The space of modular forms*

3.1. *The zeros and poles of a modular function*

Let f be a meromorphic function on H, not identically zero, and let p be a point of H. The integer n such that $f/(z-p)^n$ is holomorphic and non-zero at p is called the *order of f at p* and is denoted by $v_p(f)$.

---

(1) See for example H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, chap. V, §2, n° 5. (English translation: Addison-Wesley Co.)

When f is a *modular function* of weight $2k$, the identity

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$$

shows that $v_p(f) = v_{g(p)}(f)$ if $g \in G$. In other terms, $v_p(f)$ depends only on the image of p in H/G. Moreover one can define $v_\infty(f)$ as the order for $q = 0$ of the function $\tilde{f}(q)$ associated to f (cf. n° 2.1).

Finally, we will denote by e_p the order of the stabilizer of the point p; we have $e_p = 2$ (resp. $e_p = 3$) if p is congruent modulo G to i (resp. to ρ) and $e_p = 1$ otherwise, cf. th. 1.

Theorem 3.—*Let f be a modular function of weight $2k$, not identically zero. One has:*

(19) $$v_\infty(f) + \sum_{p \in H/G} \frac{1}{e_p} v_p(f) = \frac{k}{6}.$$

[We can also write this formula in the form

(20) $$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in H/G}^{*} v_p(f) = \frac{k}{6}$$

where the symbol Σ^* means a summation over the points of H/G distinct from the classes of i and ρ.]

Observe first that the sum written in th. 3 makes sense, i.e. that f *has only a finite number of zeros and poles* modulo G. Indeed, since $\tilde{f}$ is meromorphic, there exists $r > 0$ such that $\tilde{f}$ has no zero nor pole for $0 < |q| < r$; this means that f has no zero nor pole for $Im(z) > \frac{1}{2\pi} \log(1/r)$. Now, the part D_r of the fundamental domain D defined by the inequality $Im(z) \leq \frac{1}{2\pi} \log(1/r)$ is *compact*; since f is meromorphic in H, it has only a finite number of zeros and of poles in D_r, hence our assertion.

To prove theorem 3, we will integrate $\frac{1}{2i\pi} \frac{df}{f}$ on the boundary of D. More precisely:

1) Suppose that f has no zero nor pole on the boundary of D except possibly i, ρ, and $-\bar{\rho}$. There exists a contour $\mathscr{C}$ as represented in Fig. 2 whose interior contains a representative of each zero or pole of f not congruent to i or ρ. By the residue theorem we have

$$\frac{1}{2\pi i} \int_{\mathscr{C}} \frac{df}{f} = \sum_{p \in H/G}^{*} v_p(f)$$

On the other hand:

a) The change of variables $q = e^{2\pi i z}$ transforms the arc EA into a circle ω centered at $q = 0$, with negative orientation, and not enclosing any zero or pole of $\tilde{f}$ except possibly 0. Hence

$$\frac{1}{2i\pi} \int_E^A \frac{df}{f} = \frac{1}{2i\pi} \int_\omega \frac{d\tilde{f}}{\tilde{f}} = -v_\infty(f).$$

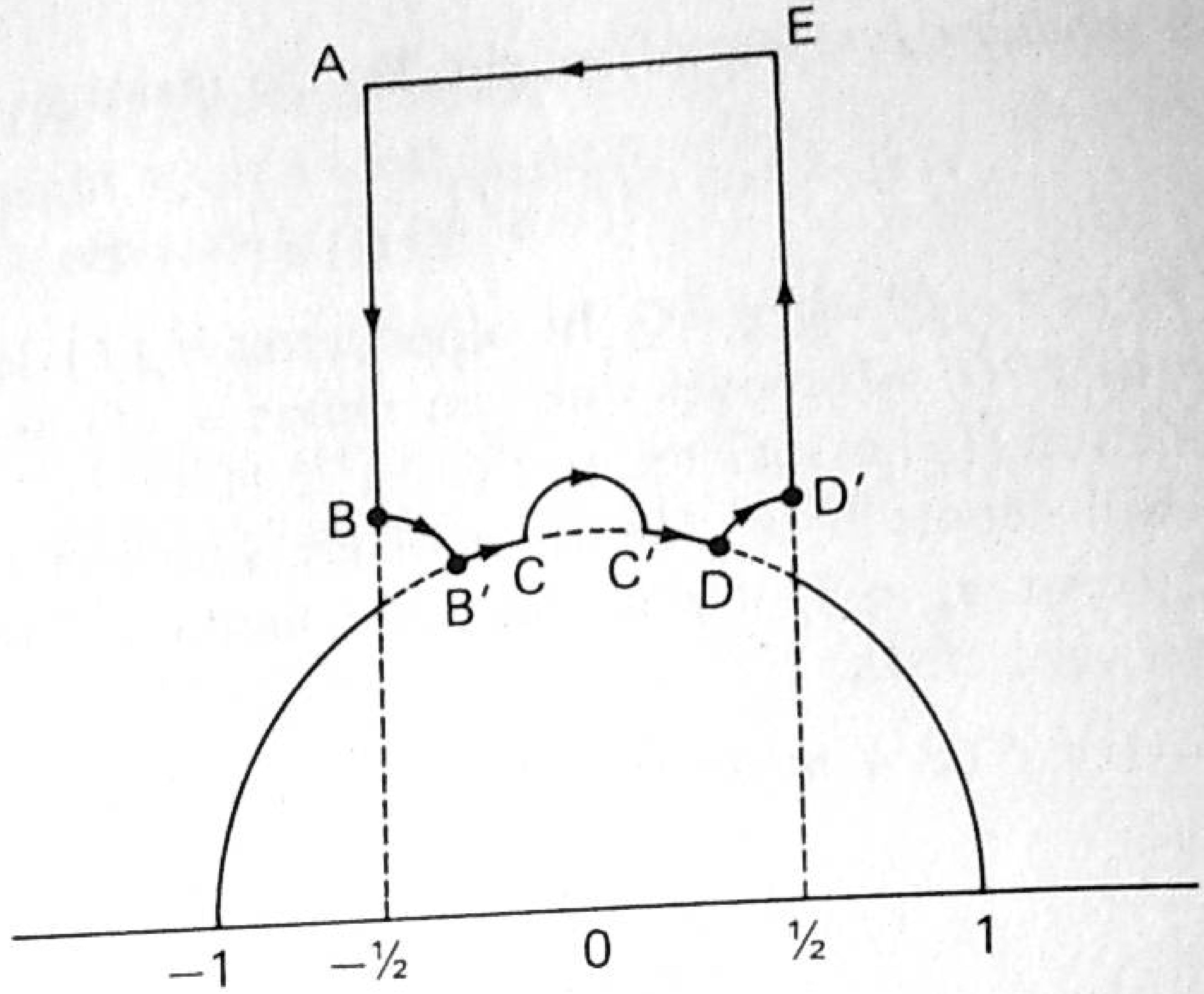

Fig. 2

b) The integral of $\frac{1}{2i\pi}\frac{df}{f}$ on the circle which contains the arc BB', oriented negatively, has the value $-v_\rho(f)$. When the radius of this circle tends to 0, the angle $\widehat{B_\rho B'}$ tends to $\frac{2\pi}{6}$. Hence:

$$\frac{1}{2i\pi}\int_{B}^{B'}\frac{df}{f} \to -\frac{1}{6}v_\rho(f).$$

Similarly when the radii of the arcs CC' and DD' tend to 0:

$$\frac{1}{2i\pi}\int_{C}^{C'}\frac{df}{f} \to -\frac{1}{2}v_i(f)$$

$$\frac{1}{2i\pi}\int_{D}^{D'}\frac{df}{f} \to -\frac{1}{6}v_\rho(f).$$

c) T transforms the arc AB into the arc ED'; since $f(Tz) = f(z)$, we get:

$$\frac{1}{2i\pi}\int_{A}^{B}\frac{df}{f} + \frac{1}{2i\pi}\int_{D'}^{E}\frac{df}{f} = 0.$$

d) S transforms the arc $B'C$ onto the arc DC'; since $f(Sz) = z^{2k}f(z)$, we get:

$$\frac{df(Sz)}{f(Sz)} = 2k\frac{dz}{z} + \frac{df(z)}{f(z)},$$

hence:

$$\frac{1}{2i\pi}\int_{B'}^{C}\frac{df}{f}+\frac{1}{2i\pi}\int_{C'}^{D}\frac{df}{f}=\frac{1}{2i\pi}\int_{B'}^{C}\left(\frac{df(z)}{f(z)}-\frac{df(Sz)}{f(Sz)}\right)$$

$$=\frac{1}{2i\pi}\int_{B'}^{C}\left(-2k\frac{dz}{z}\right)$$

$$\to -2k\left(-\frac{1}{12}\right)=\frac{k}{6}$$

when the radii of the arcs BB', CC', DD', tend to 0.

Writing now that the two expressions we get for $\frac{1}{2i\pi}\int_{\mathscr{C}}\frac{df}{f}$ are equal, and passing to the limit, we find formula (20).

2) Suppose that f has a zero or a pole λ on the half line

$$\left\{z \mid Re(z)=-\frac{1}{2},\ Im(z)>\frac{\sqrt{3}}{2}\right\}.$$

We repeat the above proof with a contour modified in a neighborhood of λ and of $T\lambda$ as in Fig. 3. (The arc circling around $T\lambda$ is the transform by T of the arc circling around λ.)

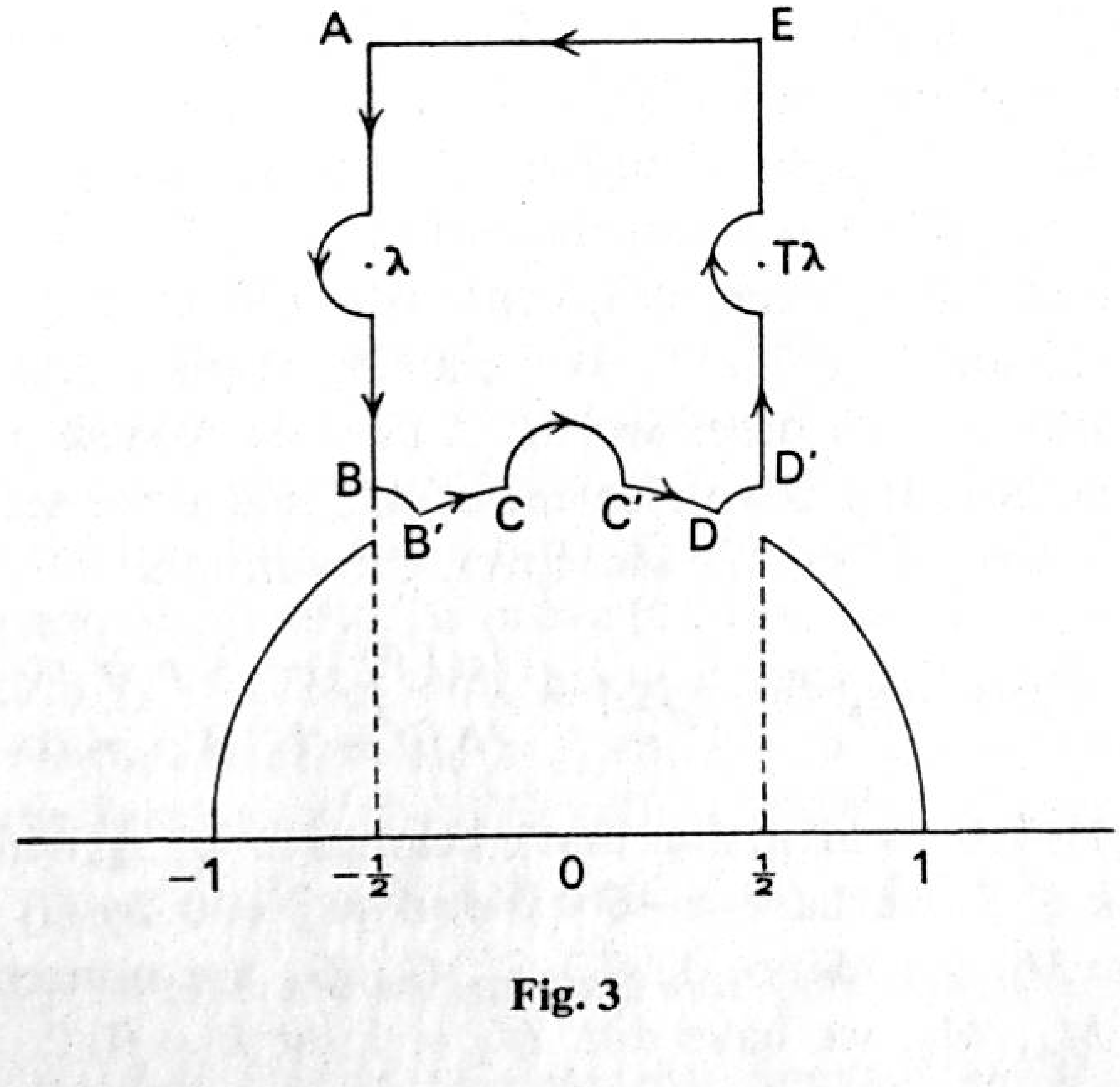

Fig. 3

We proceed in an analogous way if f has several zeros or poles on the boundary of D.

Remark.—This somewhat laborious proof could have been avoided if one had defined a complex analytic structure on the compactification of H/G

(see for instance *Seminar on Complex Multiplication*, Lecture Notes on Math., n° 21, lecture II).

3.2. *The algebra of modular forms*

If k is an integer, we denote by M_k (resp. M_k^0) the **C**-vector space of modular forms of weight $2k$ (resp. of cusp forms of weight $2k$) cf. n° 2.1, def. 4. By definition, M_k^0 is the kernel of the linear form $f \mapsto f(\infty)$ on M_k. Thus we have $\dim M_k/M_k^0 \leqq 1$. Moreover, for $k \geqq 2$, the Eisenstein series G_k is an element of M_k such that $G_k(\infty) \neq 0$, cf. n° 2.3, prop. 4. Hence we have

$$M_k = M_k^0 \oplus \mathbf{C}.G_k \quad (\text{for } k \geqq 2).$$

Finally recall that one denotes by Δ the element $g_2^3 - 27g_3^2$ of M_6^0 where $g_2 = 60G_2$ and $g_3 = 140G_3$.

Theorem 4.—(i) *We have* $M_k = 0$ *for* $k < 0$ *and* $k = 1$.

(ii) *For* $k = 0, 2, 3, 4, 5$, M_k *is a vector space of dimension* 1 *with basis* 1, G_2, G_3, G_4, G_5; *we have* $M_k^0 = 0$.

(iii) *Multiplication by* Δ *defines an isomorphism of* M_{k-6} *onto* M_k^0.

Let f be a nonzero element of M_k. All the terms on the left side of the formula

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in H/G}^{*} v_p(f) = \frac{k}{6} \tag{20}$$

are ≥ 0. Thus we have $k \geqq 0$ and also $k \neq 1$, since $\frac{1}{6}$ cannot be written in the form $n + n'/2 + n''/3$ with $n, n', n'' \geqq 0$. This proves (i).

Now apply (20) to $f = G_k$, $k = 2$. We can write $\frac{2}{6}$ in the form $n + n'/2 + n''/3$, $n, n', n'' \geqq 0$ only for $n = 0$, $n' = 0$, $n'' = 1$. This shows that $v_\rho(G_2) = 1$ and $v_p(G_2) = 0$ for $p \neq \rho$ (modulo G). The same argument applies to G_3 and proves that $v_i(G_3) = 1$ and that all the others $v_p(G_3)$ are zero. This already shows that Δ is not zero at i, hence is not identically zero. Since the weight of Δ is 12 and $v_\infty(\Delta) \geqq 1$, formula (20) implies that $v_p(\Delta) = 0$ for $p \neq \infty$ and $v_\infty(\Delta) = 1$. In other words, Δ *does not vanish on* H *and has a simple zero at infinity*. If f is an element of M_k^0 and if we set $g = f/\Delta$, it is clear that g is of weight $2k-12$. Moreover, the formula

$$v_p(g) = v_p(f) - v_p(\Delta) = \begin{cases} v_p(f) & \text{if } p \neq \infty \\ v_p(f) - 1 & \text{if } p = \infty \end{cases}$$

shows that $v_p(g)$ is $\geqq 0$ for all p, thus that g belongs to M_{k-6}, which proves (iii).

Finally, if $k \leqq 5$, we have $k - 6 < 0$ and $M_k^0 = 0$ by (i) and (iii); this shows that $\dim M_k \leqq 1$. Since $1, G_2, G_3, G_4, G_5$ are nonzero elements of M_0, M_2, M_3, M_4, M_5, we have $\dim M_k = 1$ for $k = 0, 2, 3, 4, 5$, which proves (ii).

Corollary 1.—*We have*

$$\dim M_k = \begin{cases} [k/6] & \text{if } k \equiv 1 \pmod 6,\ k \geqq 0 \\ [k/6] + 1 & \text{if } k \not\equiv 1 \pmod 6,\ k \geqq 0. \end{cases} \tag{21}$$

(Recall that $[x]$ denotes the *integral part* of x, i.e. the largest integer n such that $n \leqq x$.)

Formula (21) is true for $0 \leqq k < 6$ by (i) and (ii). Moreover, the two expressions increase by one unit when we replace k by $k+6$ (cf. (iii)). The formula is thus true for all $k \geqq 0$.

Corollary 2.—*The space M_k has for basis the family of monomials $G_2^\alpha G_3^\beta$ with α, β integers $\geqq 0$ and $2\alpha + 3\beta = k$.*

We show first that these monomials *generate* M_k. This is clear for $k \leqq 3$ by (i) and (ii). For $k \geqq 4$ we argue by induction on k. Choose a pair (γ, δ) of integers $\geqq 0$ such that $2\gamma + 3\delta = k$ (this is possible for all $k \geqq 2$). The modular form $g = G_2^\gamma G_3^\delta$ is not zero at infinity. If $f \in M_k$, there exists $\lambda \in \mathbf{C}$ such that $f - \lambda g$ is a cusp form, hence equal to Δh with $h \in M_{k-6}$, cf. (iii). One then applies the inductive hypothesis to h.

It remains to see that the above monomials are linearly independent; if they were not, the function G_2^3/G_3^2 would verify a nontrivial algebraic equation with coefficients in $\mathbf{C}$, thus would be constant, which is absurd because G_2 is zero at ρ but not G_3.

Remark.—Let $M = \sum_0^\infty M_k$ be the graded algebra which is the direct sum of the M_k and let $\varepsilon : \mathbf{C}[X, Y] \to M$ be the homomorphism which maps X on G_2 and Y on G_3. Cor. 2 is equivalent to saying that ε is an *isomorphism*. Hence, one can identify M with the polynomial algebra $\mathbf{C}[G_2, G_3]$.

3.3. *The modular invariant*

We put:

(22)
$$j = 1728 g_2^3/\Delta.$$

Proposition 5.—(a) *The function j is a modular function of weight* 0.

(b) *It is holomorphic in H and has a simple pole at infinity.*

(c) *It defines by passage to quotient a bijection of H/G onto* $\mathbf{C}$.

Assertion (a) comes from the fact that g_2^3 and Δ are both of weight 12; ← by proof of theorem 4 (b) comes from the fact that Δ is $\neq 0$ on H and has a simple zero at infinity, while g_2 is nonzero at infinity. To prove (c), one has to show that, if $\lambda \in \mathbf{C}$, the modular form $f_\lambda = 1728 g_2^3 - \lambda\Delta$ has a unique zero modulo G. To see this, one applies formula (20) with $f = f_\lambda$ and $k = 6$. The only decompositions of $k/6 = 1$ in the form $n + n'/2 + n''/3$ with $n, n', n'' \geqq 0$ correspond to

$$(n, n', n'') = (1, 0, 0) \text{ or } (0, 2, 0) \text{ or } (0, 0, 3).$$

This shows that f_λ is zero at one and only one point of H/G.

Proposition 6.—*Let f be a meromorphic function on H. The following properties are equivalent:*

(i) *f is a modular function of weight* 0;

(ii) *f is a quotient of two modular forms of the same weight;*

(iii) *f is a rational function of j.*

The implications (iii) ⇒ (ii) ⇒ (i) are immediate. We show that (i) ⇒ (iii). Let f be a modular function. Being free to multiply f by a suitable polynomial in j, we can suppose that f is holomorphic on H. Since Δ is zero at infinity, there exists an integer $n \geqq 0$ such that $g = \Delta^n f$ is holomorphic at infinity. The function g is then a modular form of weight $12n$; by cor. 2 of theorem 4 we can write it as a linear combination of the $G_2^\alpha G_3^\beta$ with $2\alpha+3\beta = 6n$. By linearity, we are reduced to the case $g = G_2^\alpha G_3^\beta$, i.e. $f = G_2^\alpha G_3^\beta/\Delta^n$. But the relation $2\alpha+3\beta = 6n$ shows that $p = \alpha/2$ and $q = \beta/3$ are integers and one has $f = G_2^{3p} G_3^{2q}/\Delta^{p+q}$. Thus we are reduced to see that G_2^3/Δ and G_3^2/Δ are rational functions of j, which is obvious.

Remarks.—1) As stated above, it is possible to define in a natural way a structure of *complex analytic manifold* on the compactification $\widehat{H/G}$ of H/G. Prop. 5 means then that j defines an *isomorphism of* $\widehat{H/G}$ onto the Riemann sphere $\mathbf{S}_2 = \mathbf{C} \cup \{\infty\}$. As for prop. 6, it amounts to the well known fact that the only meromorphic functions on $\mathbf{S}_2$ are the rational functions.

2) The coefficient $1728 = 2^6 3^3$ has been introduced in order that j has a residue equal to 1 at infinity. More precisely, the series expansions of §4 show that:

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n, \qquad z \in H, q = e^{2\pi i z}. \tag{23}$$

One has:

$$c(1) = 2^2 3^3\, 1823 = 196884, \quad c(2) = 2^{11} 5.2099 = 21493760.$$

The $c(n)$ are integers; they enjoy remarkable divisibility properties[1]:

$$\begin{aligned} n &\equiv 0 \pmod{2^a} \Rightarrow c(n) \equiv 0 \pmod{2^{3a+8}} \quad \text{if } a \geq 1\\ n &\equiv 0 \pmod{3^a} \Rightarrow c(n) \equiv 0 \pmod{3^{2a+3}} \quad \text{''}\\ n &\equiv 0 \pmod{5^a} \Rightarrow c(n) \equiv 0 \pmod{5^{a+1}} \quad \text{''}\\ n &\equiv 0 \pmod{7^a} \Rightarrow c(n) \equiv 0 \pmod{7^a}\\ n &\equiv 0 \pmod{11^a} \Rightarrow c(n) \equiv 0 \pmod{11^a}. \end{aligned}$$

§4. *Expansions at infinity*

4.1. *The Bernoulli numbers B_k*

They are defined by the power series expansion:[2]

---

(1) See on this subject A. O. L. ATKIN and J. N. O'BRIEN, Trans. Amer. Math. Soc., 126, 1967, as well as the paper of ATKIN in *Computers in mathematical research* (North Holland, 1968).

(2) In the literature, one also finds "Bernoulli numbers" b_k defined by

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} b_k x^k / k!\,,$$

hence $b_0 = 1$, $b_1 = -1/2$, $b_{2k+1} = 0$ if $k > 1$, and $b_{2k} = (-1)^{k-1} B_k$. The b notation is better adapted to the study of congruence properties, and also to generalizations à la Leopoldt.

(24) $$\frac{x}{e^x-1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}.$$

Numerical table

$$B_1 = \frac{1}{6}, \; B_2 = \frac{1}{30}, \; B_3 = \frac{1}{42}, \; B_4 = \frac{1}{30}, \; B_5 = \frac{5}{66}, \; B_6 = \frac{691}{2730},$$

$$B_7 = \frac{7}{6}, \; B_8 = \frac{3617}{510}, \; B_9 = \frac{43867}{798}, \; B_{10} = \frac{283.617}{330}, \; B_{11} = \frac{11.131.593}{138},$$

$$B_{12} = \frac{103.2294797}{2730}, \; B_{13} = \frac{13.657931}{6}, \; B_{14} = \frac{7.9349.362903}{870}.$$

The B_k give the values of the Riemann zeta function for the positive even integers (and also for the negative odd integers):

Proposition 7.—*If k is an integer $\geqq 1$, then*:

(25) $$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k}.$$

The identity

(26) $$z \operatorname{cotg} z = 1 - \sum_{k=1}^{\infty} B_k \frac{2^{2k} z^{2k}}{(2k)!}$$

follows from the definition of the B_k by putting $x = 2iz$. Moreover, taking the logarithmic derivative of

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

we get:

(28) $$z \operatorname{cotg} z = 1 + 2 \sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2}$$

$$= 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{z^{2k}}{n^{2k}\pi^{2k}}.$$

Comparing (26) and (28), we get (25).

Examples $\zeta(2) = \frac{\pi^2}{2.3}$, $\zeta(4) = \frac{\pi^4}{2.3^2.5}$, $\zeta(6) = \frac{\pi^6}{3^3.5.7}$,

$$\zeta(8) = \frac{\pi^8}{2.3^3.5^2.7}, \; \zeta(10) = \frac{\pi^{10}}{3^5.5.7.11}, \; \zeta(12) = \frac{691\pi^{12}}{3^6.5^3.7^2.11.13},$$

$$\zeta(14) = \frac{2\pi^{14}}{3^6.5^2.7.11.13}.$$

4.2. *Series expansions of the functions G_k*

We now give the Taylor expansion of the Eisenstein series $G_k(z)$ with respect to $q = e^{2\pi iz}$.

Let us start with the well known formula:

$$\pi \operatorname{cotg} \pi z = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right). \tag{29}$$

We have on the other hand:

$$\pi \operatorname{cotg} \pi z = \pi \frac{\cos \pi z}{\sin \pi z} = i\pi \frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi \sum_{n=0}^{\infty} q^n, \tag{30}$$

Comparing, we get:

$$\frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) = i\pi - 2i\pi \sum_{n=0}^{\infty} q^n. \tag{31}$$

By successive differentiations of (31), we obtain the following formula (valid for $k \geqq 2$):

$$\sum_{m \in \mathbf{Z}} \frac{1}{(m+z)^k} = \frac{1}{(k-1)!} (-2i\pi)^k \sum_{n=1}^{\infty} n^{k-1} q^n. \tag{32}$$

Denote now by $\sigma_k(n)$ the sum $\sum_{d|n} d^k$ of kth-powers of positive divisors of n.

Proposition 8.—*For every integer $k \geqq 2$, one has:*

$$G_k(z) = 2\zeta(2k) + 2 \frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n. \tag{33}$$

We expand:

$$G_k(z) = \sum_{(n,m) \neq (0,0)} \frac{1}{(nz+m)^{2k}}$$

$$= 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \sum_{m \in \mathbf{Z}} \frac{1}{(nz+m)^{2k}}.$$

Applying (32) with z replaced by nz, we get

$$G_k(z) = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!} \sum_{d=1}^{\infty} \sum_{a=1}^{\infty} d^{2k-1} q^{ad}$$

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

Corollary.—*$G_k(z) = 2\zeta(2k) E_k(z)$ with*

$$E_k(z) = 1 + \gamma_k \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \tag{34}$$

and

(35)
$$\gamma_k = (-1)^k \frac{4k}{B_k}.$$

One defines $E_k(z)$ as the quotient of $G_k(z)$ by $2\zeta(2k)$; it is clear that $E_k(z)$ is given by (34). The coefficient γ_k is computed using prop. 7:

$$\gamma_k = \frac{(2i\pi)^{2k}}{(2k-1)!}\frac{1}{\zeta(2k)} = \frac{(2\pi)^{2k}(-1)^k}{(2k-1)!}\frac{(2k)!}{2^{2k-1}B_k\pi^{2k}} = (-1)^k\frac{4k}{B_k}.$$

Examples

$$E_2 = 1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n, \quad g_2 = (2\pi)^4\frac{1}{2^2.3}E_2$$

$$E_3 = 1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n, \quad g_3 = (2\pi)^6\frac{1}{2^3.3^3}E_3$$

$$E_4 = 1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n \qquad (480 = 2^5.3.5)$$

$$E_5 = 1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n \qquad (264 = 2^3.3.11)$$

$$E_6 = 1+\frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n \qquad (65520 = 2^4.3^2.5.7.13)$$

$$E_7 = 1-24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n.$$

Remark.—We have seen in n° 3.2 that the space of modular forms of weight 8 (resp. 10) is of dimension 1. Hence:

(36)
$$E_2^2 = E_4, \quad E_2E_3 = E_5.$$

This is equivalent to the identities:

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

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

More generally, every E_k can be expressed as a *polynomial* in E_2 and E_3.

4.3. *Estimates for the coefficients of modular forms*

Let

(37)
$$f(z) = \sum_{n=0}^{\infty}a_nq^n \quad (q = e^{2\pi iz})$$

be a modular form of weight $2k$, $k \geqq 2$. We are interested in the growth of the a_n:

Proposition 9.—*If $f = G_k$, the order of magnitude of a_n is n^{2k-1}. More precisely, there exist two constants A, $B > 0$ such that*

$$An^{2k-1} \leqq |a_n| \leqq Bn^{2k-1}. \tag{38}$$

Prop. 8 shows that there exists a constant $A > 0$ such that

$$a_n = (-1)^k A\sigma_{2k-1}(n), \qquad \text{hence } |a_n| = A\sigma_{2k-1}(n) \geqq An^{2k-1}.$$

On the other hand:

$$\frac{|a_n|}{n^{2k-1}} = A\sum_{d|n} \frac{1}{d^{2k-1}} \leqq A\sum_{d=1}^{\infty} \frac{1}{d^{2k-1}} = A\zeta(2k-1) < +\infty.$$

Theorem 5 (Hecke).—*If f is a cusp form of weight $2k$, then*

$$a_n = O(n^k). \tag{39}$$

(In other words, the quotient $\dfrac{|a_n|}{n^k}$ remains bounded when $n \to \infty$.)

Because f is a cusp form, we have $a_0 = 0$ and can factor q out of the expansion (37) of f. Hence:

$$|f(z)| = O(q) = O(e^{-2\pi y}) \qquad \text{with } y = Im(z), \qquad \text{when } q \text{ tends to } 0. \tag{40}$$

Let $\phi(z) = |f(z)|y^k$. Formulas (1) and (2) show that ϕ is *invariant* under the modular group G. In addition, ϕ is continuous on the fundamental domain D and formula (40) shows that ϕ tends to 0 for $y \to \infty$. This implies that ϕ is *bounded*, i.e. there exists a constant M such that

$$|f(z)| \leqq My^{-k} \qquad \text{for } z \in H. \tag{41}$$

Fix y and vary x between 0 and 1. The point $q = e^{2\pi i(x+iy)}$ runs along a circle C_y of center 0. By the residue formula,

$$a_n = \frac{1}{2\pi i}\int_{C_y} f(z)q^{-n-1}dq = \int_0^1 f(x+iy)q^{-n}dx.$$

(One could also deduce this formula from that giving the Fourier coefficients of a periodic function.)

Using (41), we get from this

$$|a_n| \leqq My^{-k}e^{2\pi ny}.$$

This inequality is valid for all $y > 0$. For $y = 1/n$, it gives $|a_n| \leqq e^{2\pi}Mn^k$. The theorem follows from this.

Corollary.—*If f is not a cusp form, then the order of magnitude of a_n is n^{2k-1}.*

We write f in the form $\lambda G_k + h$ with $\lambda \neq 0$ and a cusp form h and we apply prop. 9 and th. 5, taking into account the fact that n^k is "negligible" compared to n^{2k-1}.

Remark.—The exponent k of theorem 5 can be improved. Indeed, Deligne has shown (cf. 5.6.3 below) that

$$a_n = O(n^{k-1/2}\sigma_0(n)),$$

where $\sigma_0(n)$ is the number of positive divisors of n. This implies that

$$a_n = O(n^{k-1/2+\varepsilon}) \qquad \text{for every } \varepsilon > 0.$$

4.4. *Expansion of* Δ

Recall that

$$\begin{aligned}\Delta &= g_2^3 - 27g_3^2 = (2\pi)^{12}2^{-6}3^{-3}(E_2^3 - E_3^2) \\ &= (2\pi)^{12}(q - 24q^2 + 252q^3 - 1472q^4 + \dots).\end{aligned} \tag{42}$$

Theorem 6 (Jacobi).—$\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24}$.

[This formula is proved in the most natural way by using elliptic functions. Since this method would take us too far afield, we sketch below a different proof, which is "elementary" but somewhat artificial; for more details, the reader can look into A. HURWITZ, *Math. Werke*, Bd. I, pp. 578–595.]

We put:

$$F(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}. \tag{43}$$

To prove that F and Δ are proportional, it suffices to show that F is a modular form of weight 12; indeed, the fact that the expansion of G has constant term zero will show that F is a cusp form and we know (th. 4) that the space M_6^0 of cusp forms of weight 12 is of dimension 1. By prop. 1 of n° 2.1, all there is to do is to prove that:

$$F(-1/z) = z^{12}F(z). \tag{44}$$

We use for this the double series

$$G_1(z) = \sum_n \sum_m{}' \frac{1}{(m+nz)^2}, \quad G(z) = \sum_m \sum_n{}' \frac{1}{(m+nz)^2}$$

$$H_1(z) = \sum_n \sum_m{}' \frac{1}{(m-1+nz)\,(m+nz)}, \quad H(z) = \sum_m \sum_n{}' \frac{1}{(m-1+nz)\,(m+nz)}$$

where the sign Σ' indicates that (m,n) runs through all $m \in \mathbf{Z}$, $n \in \mathbf{Z}$ with $(m,n) \neq (0,0)$ for G and G_1 and $(m,n) \neq (0,0)$, $(1,0)$ for H and H_1. (Notice the order of the summations!)

The series H_1 and H are easy to calculate explicitly because of the formula:

$$\frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} - \frac{1}{m+nz}.$$

One finds that they converge, and that

$$H_1 = 2,\ H = 2 - 2\pi i/z.$$

Moreover, the double series with general term

$$\frac{1}{(m-1+nz)(m+nz)} - \frac{1}{(m+nz)^2} = \frac{1}{(m+nz)^2(m-1+nz)}$$

is absolutely summable. This shows that $G_1 - H_1$ and $G - H$ coincide, thus that the series G and G_1 converge (with order of summation indicated) and that

$$G_1(z) - G(z) = H_1(z) - H(z) = \frac{2\pi i}{z}.$$

It is clear moreover that $G_1(-1/z) = z^2 G(z)$. Hence:

(45) $$G_1(-1/z) = z^2 G_1(z) - 2\pi i z.$$

On the other hand, a computation similar to that of prop. 8 gives

(46) $$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Now, go back to the function F defined by (43). Its logarithmic differential is

(47) $$\frac{dF}{F} = \frac{dq}{q}\left(1 - 24 \sum_{n,m=1}^{\infty} n q^{nm}\right) = \frac{dq}{q}\left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n\right).$$

By comparing with (46), we get:

(48) $$\frac{dF}{F} = \frac{6i}{\pi} G_1(z) dz.$$

Combining (45) and (48), we have

(49) $$\begin{aligned}\frac{dF(-1/z)}{F(-1/z)} &= \frac{6i}{\pi} G_1(-1/z) \frac{dz}{z^2} = \frac{6i}{\pi} \frac{dz}{z^2} (z^2 G_1(z) - 2\pi i z) \\ &= \frac{dF(z)}{F(z)} + 12 \frac{dz}{z}.\end{aligned}$$

Thus the two functions $F(-1/z)$ and $z^{12}F(z)$ have the same logarithmic differential. Hence there exists a constant k such that $F(-1/z) = kz^{12}F(z)$ for all $z \in H$. For $z = i$, we have $z^{12} = 1$, $-1/z = z$ and $F(z) \neq 0$; this shows that $k = 1$, which proves (44), q.e.d.

Remark.—One finds another "elementary" proof of identity (44) in C. L. Siegel, *Gesamm. Abh.*, III, n° 62. See also *Seminar on complex multiplication*, III, §6.

4.5. *The Ramanujan function*

We denote by $\tau(n)$ the nth coefficient of the cusp form $F(z) = (2\pi)^{-12}\Delta(z)$. Thus

$$\sum_{n=1}^{\infty} \tau(n)q^n = q \prod_{n=1}^{\infty} (1-q^n)^{24}. \tag{50}$$

The function $n \mapsto \tau(n)$ is called the *Ramanujan function*.

Numerical table (1)

$\tau(1) = 1$, $\tau(2) = -24$, $\tau(3) = 252$, $\tau(4) = -1472$, $\tau(5) = 4830$,
$\tau(6) = -6048$, $\tau(7) = -16744$, $\tau(8) = 84480$, $\tau(9) = -113643$,
$\tau(10) = -115920$, $\tau(11) = 534612$, $\tau(12) = -370944$.

Properties of $\tau(n)$

$$\tau(n) = O(n^6), \tag{51}$$

because Δ is of weight 12, cf. n° 4.3, th. 5. (By Deligne's theorem, we even have $\tau(n) = O(n^{11/2+\varepsilon})$ for every $\varepsilon > 0$.)

$$\tau(nm) = \tau(n)\tau(m) \quad \text{if } (n, m) = 1 \tag{52}$$

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \quad \text{for } p \text{ prime, } n > 1 \text{, cf. n° 5.5. below.} \tag{53}$$

The identities (52) and (53) were conjectured by Ramanujan and first proved by Mordell. One can restate them by saying that the Dirichlet series $L_\tau(s) = \sum_{n=1}^{\infty} \tau(n)/n^s$ has the following eulerian expansion:

$$L_\tau(s) = \prod_{p\in P} \frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}, \quad \text{cf. n° 5.4.} \tag{54}$$

By a theorem of Hecke (cf. n° 5.4) the function L_τ extends to an entire function in the complex plane and the function

$$(2\pi)^{-s}\Gamma(s)L_\tau(s)$$

is invariant by $s \mapsto 12-s$.

The $\tau(n)$ enjoy various congruences modulo 2^{12}, 3^6, 5^3, 7, 23, 691. We quote some special cases (without proof):

$$\tau(n) \equiv n^2\sigma_7(n) \pmod{3^3} \tag{55}$$

$$\tau(n) \equiv n\sigma_3(n) \pmod{7} \tag{56}$$

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}. \tag{57}$$

For other examples, and their interpretation in terms of "l-adic representations" see *Sém. Delange-Pisot-Poitou* 1967/68, exposé 14, *Sém. Bourbaki* 1968/69, exposé 355 and Swinnerton–Dyer's lecture at Antwerp (*Lecture Notes*, n° 350, Springer, 1973).

---

(1) This table is taken from D. H. Lehmer, *Ramanujan's function* $\tau(n)$, *Duke Math. J.*, 10, 1943, which gives the values of $\tau(n)$ for $n \leqq 300$.

We end up with an *open question*, raised by D. H. Lehmer:
Is it true that $\tau(n) \neq 0$ for all $n \geq 1$?
It is so for $n \leq 10^{15}$.

§5. *Hecke operators*

5.1. *Definition of the* $T(n)$

Correspondences.—Let E be a set and let X_E be the free abelian group generated by E. A *correspondence* on E (with integer coefficients) is a homomorphism T of X_E into itself. We can give T by its values on the elements x of E:

$$T(x) = \sum_{y \in E} n_y(x) y, \quad n_y(x) \in \mathbf{Z}, \tag{58}$$

the $n_y(x)$ being zero for almost all y.

Let F be a numerical valued function on E. By $\mathbf{Z}$-linearity it extends to a function, again denoted F, on X_E. The transform of F by T, denoted TF, is the restriction to E of the function $F \circ T$. With the notations of (58),

$$TF(x) = F(T(x)) = \sum_{y \in E} n_y(x) F(y). \tag{59}$$

The $T(n)$.—Let $\mathcal{R}$ be the set of lattices of $\mathbf{C}$ (see n° 2.2). Let n be an integer $\geqq 1$. We denote by $T(n)$ the correspondence on $\mathcal{R}$ which transforms a lattice to the sum (in $X_{\mathcal{R}}$) of its sub-lattices of index n. Thus we have:

$$T(n)\Gamma = \sum_{(\Gamma:\Gamma') = n} \Gamma' \quad \text{if } \Gamma \in \mathcal{R}. \tag{60}$$

The sum on the right side is finite. Indeed, the lattices Γ' all contain $n\Gamma$ and their number is also the number of subgroups of order n of $\Gamma/n\Gamma = (\mathbf{Z}/n\mathbf{Z})^2$. If n is prime, one sees easily that this number is equal to $n+1$ (number of points of the projective line over a field with n elements).

We also use the homothety operators R_λ ($\lambda \in \mathbf{C}^*$) defined by

$$R_\lambda \Gamma = \lambda\Gamma \quad \text{if } \Gamma \in \mathcal{R}. \tag{61}$$

Formulas.—It makes sense to compose the correspondences $T(n)$ and R_λ, since they are endomorphisms of the abelian group $X_{\mathcal{R}}$.

Proposition 10.—*The correspondences* $T(n)$ *and* R_λ *verify the identities*

$$R_\lambda R_\mu = R_{\lambda\mu} \qquad (\lambda, \mu \in \mathbf{C}^*) \tag{62}$$

$$R_\lambda T(n) = T(n) R_\lambda \qquad (n \geqq 1, \lambda \in \mathbf{C}^*) \tag{63}$$

$$T(m)T(n) = T(mn) \qquad \textit{if } (m, n) = 1 \tag{64}$$

$$T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})R_p \qquad (p \textit{ prime}, n \geqq 1). \tag{65}$$

Formulas (62) and (63) are trivial.

Formula (64) is equivalent to the following assertion: Let m, n be two relatively prime integers $\geqq 1$, and let Γ'' be a sublattice of a lattice Γ of index mn; there exists a unique sublattice Γ' of Γ, containing Γ'', such that $(\Gamma:\Gamma') = n$ and $(\Gamma':\Gamma'') = m$. This assertion follows itself from the fact that the group Γ/Γ'', which is of order mn, decomposes uniquely into a direct sum of a group of order m and a group of order n (Bezout's theorem).

To prove (65), let Γ be a lattice. Then $T(p^n)T(p)\Gamma$, $T(p^{n+1})\Gamma$ and $T(p^{n-1})R_p\Gamma$ are linear combinations of lattices contained in Γ and of index p^{n+1} in Γ (note that $R_p\Gamma$ is of index p^2 in Γ). Let Γ'' be such a lattice; in the above linear combinations it appears with coefficients a, b, c, say; we have to show that $a = b+pc$, i.e. that $a = 1+pc$ since b is clearly equal to 1.

We have two cases:

i) Γ'' is not contained in $p\Gamma$. Then $c = 0$ and a is the number of lattices Γ', intermediate between Γ and Γ'', and of index p in Γ; such a lattice Γ' contains $p\Gamma$. In $\Gamma/p\Gamma$ the image of Γ' is of index p and it contains the image of Γ'' which is of order p (hence also of index p because $\Gamma/p\Gamma$ is of order p^2); hence there is only one Γ' which does the trick. This gives $a = 1$ and the formula $a = 1+pc$ is valid.

ii) $L'' \subset p\Gamma$. We have $c = 1$; any lattice Γ' of index p in Γ contains $p\Gamma$, thus *a fortiori* Γ''. This gives $a = p+1$ and $a = 1+pc$ is again valid.

Corollary 1.—*The $T(p^n)$, $n > 1$, are polynomials in $T(p)$ and R_p.*

This follows from (65) by induction on n.

Corollary 2.—*The algebra generated by the R_λ and the $T(p)$, p prime, is commutative; it contains all the $T(n)$.*

This follows from prop. 10 and cor. 1.

Action of $T(n)$ on the functions of weight $2k$.

Let F be a function on $\mathcal{R}$ of weight $2k$ (cf. n° 2.2). By definition

$$R_\lambda F = \lambda^{-2k}F \quad \text{for all } \lambda \in \mathbf{C}^*. \tag{66}$$

Let n be an integer $\geqq 1$. Formula (63) shows that

$$R_\lambda(T(n)F) = T(n)(R_\lambda F) = \lambda^{-2k}T(n)F,$$

in other words $T(n)F$ is also of weight $2k$. Formulas (64) and (65) give:

$$T(m)T(n)F = T(mn)F \qquad \text{if } (m, n) = 1, \tag{67}$$

$$T(p)T(p^n)F = T(p^{n+1})F + p^{1-2k}T(p^{n-1})F, \qquad p \text{ prime}, n \geqq 1. \tag{68}$$

5.2. *A matrix lemma*

Let Γ be a lattice with basis $\{\omega_1, \omega_2\}$ and let n be an integer $\geqq 1$. The following lemma gives all the sublattices of Γ of index n:

Lemma 2.—*Let S_n be the set of integer matrixes $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = n$, $a \geqq 1$, $0 \leqq b < d$. If $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is contained in S_n, let Γ_σ be the sublattice* *of Γ having for basis*

$$\omega_1' = a\omega_1 + b\omega_2,\ \omega_2' = d\omega_2.$$

The map $\sigma \mapsto \Gamma_\sigma$ is a bijection of S_n onto the set $\Gamma(n)$ of sublattices of index n in Γ.

The fact that Γ_σ belongs to $\Gamma(n)$ follows from the fact that $\det(\sigma) = n$. Conversely let $\Gamma' \in \Gamma(n)$. We put

$$Y_1 = \Gamma/(\Gamma' + \mathbf{Z}\omega_2) \quad \text{and} \quad Y_2 = \mathbf{Z}\omega_2/(\Gamma' \cap \mathbf{Z}\omega_2).$$

These are cyclic groups generated respectively by the images of ω_1 and ω_2. Let a and d be their orders. The exact sequence

$$0 \to Y_2 \to \Gamma/\Gamma' \to Y_1 \to 0$$

shows that $ad = n$. If $\omega_2' = d\omega_2$, then $\omega_2' \in \Gamma'$. On the other hand, there exists $\omega_1' \in \Gamma'$ such that

$$\omega_1' \equiv a\omega_1 \pmod{\mathbf{Z}\omega_2}.$$

It is clear that ω_1' and ω_2' form a basis of Γ'. Moreover, we can write ω_1' in the form

$$\omega_1' = a\omega_1 + b\omega_2 \qquad \text{with } b \in \mathbf{Z},$$

where b is uniquely determined modulo d. If we impose on b the inequality $0 \leqq b < d$, this fixes b, thus also ω_1'. Thus we have associated to every $\Gamma' \in \Gamma(n)$ a matrix $\sigma(\Gamma') \in S_n$, and one checks that the maps $\sigma \mapsto \Gamma_\sigma$ and $\Gamma' \mapsto \sigma(\Gamma')$ are inverses to each other; the lemma follows.

Example.—If p is a prime, the elements of S_p are the matrix $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and the p matrices $\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$ with $0 \leqq b < p$.

5.3. *Action of $T(n)$ on modular functions*

Let k be an integer, and let f be a weakly modular function of weight $2k$, cf. n° 2.1. As we saw in n° 2.2, f corresponds to a function F of weight $2k$ on $\mathcal{R}$ such that

$$F(\Gamma(\omega_1, \omega_2)) = \omega_2^{-2k} f(\omega_1/\omega_2). \tag{69}$$

We define $T(n)f$ as *the function on H associated to the function $n^{2k-1}T(n)F$ on $\mathcal{R}$*. (Note the numerical coefficient n^{2k-1} which gives formulas "without denominators" in what follows.) Thus by definition:

$$T(n)f(z) = n^{2k-1}T(n)F(\Gamma(z, 1)), \tag{70}$$

or else by lemma 2:

$$T(n)f(z) = n^{2k-1} \sum_{\substack{a \geqq 1,\, ad = n \\ 0 \leqq b < d}} d^{-2k} f\left(\frac{az+b}{d}\right). \tag{71}$$

Proposition 11.—*The function $T(n)f$ is weakly modular of weight $2k$. It is holomorphic on H if f is. We have:*

$$T(m)T(n)f = T(mn)f \quad \text{if} \quad (m, n) = 1, \tag{72}$$

$$T(p)T(p^n)f = T(p^{n+1})f + p^{2k-1}T(p^{n-1})f, \quad \text{if } p \text{ is prime, } n \geqq 1. \tag{73}$$

Formula (71) shows that $T(n)f$ is meromorphic on H, thus weakly modular; if in addition f is holomorphic, so is $T(n)f$. Formulas (72) and (73) follow from formulas (67) and (68) taking into account the numerical coefficient n^{2k-1} incorporated into the definition of $T(n)f$.

Behavior at infinity.—We suppose that f is a *modular function*, i.e. is meromorphic at infinity. Let

$$f(z) = \sum_{m \in \mathbf{Z}} c(m)q^m \tag{74}$$

be its Laurent expansion with respect to $q = e^{2\pi iz}$.

Proposition 12.—*The function $T(n)f$ is a modular function. We have*

$$T(n)f(z) = \sum_{m \in \mathbf{Z}} \gamma(m)q^m \tag{75}$$

with

$$\gamma(m) = \sum_{\substack{a|(n,m) \\ a \geqq 1}} a^{2k-1} c\left(\frac{mn}{a^2}\right). \tag{76}$$

By definition, we have:

$$T(n)f(z) = n^{2k-1} \sum_{\substack{ad=n,\, a \geqq 1 \\ 0 \leqq b < d}} d^{-2k} \sum_{m \in \mathbf{Z}} c(m)e^{2\pi im(az+b)/d}$$

Now the sum

$$\sum_{0 \leqq b < d} e^{2\pi i\, bm/d}$$

is equal to d if d divides m and to 0 otherwise. Thus we have, putting $m/d = m'$:

$$T(n)f(z) = n^{2k-1} \sum_{\substack{ad=n \\ a \geqq 1,\, m' \in \mathbf{Z}}} d^{-2k+1} c(m'd)q^{am'}.$$

Collecting powers of q, this gives:

$$T(n)f(z) = \sum_{\mu \in \mathbf{Z}} q^{\mu} \sum_{\substack{a|(n,\mu) \\ a \geqq 1}} \left(\frac{n}{d}\right)^{2k-1} c\left(\frac{\mu d}{a}\right).$$

Since f is meromorphic at infinity, there exists an integer $N \geqq 0$ such that $c(m) = 0$ if $m \leqq -N$. The $c\left(\frac{\mu d}{a}\right)$ are thus zero for $\mu \leqq -nN$, which shows that $T(n)f$ is also meromorphic at infinity. Since it is weakly modular, it is a modular function. The fact that its coefficients are given by formula (76) follows from the above computation.

Corollary 1.—$\gamma(0) = \sigma_{2k-1}(n)c(0)$ *and* $\gamma(1) = c(n)$.

Corollary 2.—*If* $n = p$ *with p prime, one has*

$$\gamma(m) = c(pm) \quad \text{if } m \not\equiv 0 \pmod p$$

$$\gamma(m) = c(pm)+p^{2k-1}c(m/p) \quad \text{if } m \equiv 0 \pmod p.$$

Corollary 3.—*If f is a modular form (resp. a cusp form), so is* $T(n)f$.
This is clear.

Thus, the $T(n)$ *act* on the spaces M_k and M_k^0 of n° 3.2. As we saw above, the operators thus defined *commute* with each other and satisfy the identities:

(72) $$T(m)T(n) = T(mn) \quad \text{if } (m, n) = 1$$

(73) $$T(p)T(p^n) = T(p^{n+1})+p^{2k-1}T(p^{n-1}) \quad \text{if } p \text{ is prime}, n \geqq 1.$$

5.4. *Eigenfunctions of the* $T(n)$

Let $f(z) = \sum_{n=0}^{\infty} c(n)q^n$ be a modular form of weight $2k$, $k > 0$, not identically zero. We assume that f is an *eigenfunction* of all the $T(n)$, i.e. that there exists a complex number $\lambda(n)$ such that

(77) $$T(n)f = \lambda(n)f \quad \text{for all } n \geqq 1.$$

Theorem 7.—a) *The coefficient* $c(1)$ *of q in f is* $\neq 0$.
b) *If f is normalized by the condition* $c(1) = 1$, *then*

(78) $$c(n) = \lambda(n) \quad \textit{for all } n > 1.$$

Cor. 1 to prop. 12 shows that the coefficient of q in $T(n)f$ is $c(n)$. On the other hand, by (77), it is also $\lambda(n)c(1)$. Thus we have $c(n) = \lambda(n)c(1)$. If $c(1)$ were zero, all the $c(n)$, $n > 0$, would be zero, and f would be a constant which is absurd. Hence a) and b).

Corollary 1.—*Two modular forms of weight* $2k$, $k > 0$, *which are eigenfunctions of the* $T(n)$ *with the same eigenvalues* $\lambda(n)$, *and which are normalized, coincide.*

This follows from a) applied to the difference of the two functions.

Corollary 2.—*Under the hypothesis of theorem* 7, b):

(79) $$c(m)c(n) = c(mn) \quad \text{if } (m, n) = 1$$

(80) $$c(p)c(p^n) = c(p^{n+1})+p^{2k-1}c(p^{n-1}).$$

Indeed the eigenvalues $\lambda(n) = c(n)$ satisfy the same identities (72) and (73) as the $T(n)$.

Formulas (79) and (80) can be translated analytically in the following manner:

Let

$$\Phi_f(s) = \sum_{n=1}^{\infty} c(n)/n^s \tag{81}$$

be the Dirichlet series defined by the $c(n)$; by the cor. of th. 5, this series converges absolutely for $R(s) > 2k$.

Corollary 3.—*We have:*

$$\Phi_f(s) = \prod_{p\in P} \frac{1}{1-c(p)p^{-s}+p^{2k-1-2s}} \tag{82}$$

By (79) the function $n \mapsto c(n)$ is multiplicative. Thus lemma 4 of chap. VII, n° 3.1 shows that $\Phi_f(s)$ is the product of the series $\sum_{n=0}^{\infty} c(p^n)p^{-ns}$. Putting $p^{-s} = T$, we are reduced to proving the identity

$$\sum_{n=0}^{\infty} c(p^n)T^n = \frac{1}{\Phi_{f,p}(T)} \quad \text{where} \quad \Phi_{f,p}(T) = 1-c(p)T+p^{2k-1}T^2. \tag{83}$$

Form the series

$$\psi(T) = \left(\sum_{n=0}^{\infty} c(p^n)T^n\right)(1-c(p)T+p^{2k-1}T^2).$$

The coefficient of T in ψ is $c(p)-c(p) = 0$. That of T^{n+1}, $n \geqq 1$, is

$$c(p^{n+1})-c(p)c(p^n)+p^{2k-1}c(p^{n-1}),$$

which is zero by (80). Thus the series ψ is reduced to its constant term $c(1) = 1$, and this proves (83).

Remarks.—1) Conversely, formulas (81) and (82) imply (79) and (80).

2) Hecke has proved that Φ_f extends analytically to a meromorphic function on the whole complex plane (it is even holomorphic if f is a cusp form) and that the function

$$X_f(s) = (2\pi)^{-s}\Gamma(s)\Phi_f(s) \tag{84}$$

satisfies *the functional equation*

$$X_f(s) = (-1)^k X_f(2k-s). \tag{85}$$

The proof uses *Mellin's formula*

$$X_f(s) = \int_0^{\infty} (f(iy)-f(\infty))y^s \frac{dy}{y}$$

combined with the identity $f(-1/z) = z^{2k}f(z)$. Hecke also proved a converse: every Dirichlet series Φ which satisfies a functional equation of this type, and some regularity and growth hypothesis, comes from a modular form f of weight $2k$; moreover, f is a normalized eigenfunction of the $T(n)$

if and only if ϕ is an Eulerian product of type (82). See for more details E. HECKE, *Math. Werke*, n° 33, and A. WEIL, *Math. Annalen*, 168, 1967.

5.5. *Examples*

a) *Eisenstein series.*—Let k be an integer $\geqq 2$.

Proposition 13.—*The Eisenstein series G_k is an eigenfunction of $T(n)$; the corresponding eigenvalue is $\sigma_{2k-1}(n)$ and the normalized eigenfunction is*

$$(-1)^k \frac{B_k}{4k} E_k = (-1)^k \frac{B_k}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n. \tag{86}$$

The corresponding Dirichlet series is $\zeta(s)\zeta(s-2k+1)$.

We prove first that G_k is an eigenfunction of $T(n)$; it suffices to do this for $T(p)$, p prime. Consider G_k as a function on the set $\mathscr{R}$ of lattices of $\mathbf{C}$; we have:

$$G_k(\Gamma) = \sum_{\gamma\in\Gamma}' 1/\gamma^{2k}, \quad \text{cf. n° 2.3,}$$

and

$$T(p)G_k(\Gamma) = \sum_{(\Gamma:\Gamma')=p} \sum_{\gamma\in\Gamma'}' 1/\gamma^{2k}.$$

Let $\gamma \in \Gamma$. If $\gamma \in p\Gamma$ then γ belongs to each of the $p+1$ sublattices of Γ of index p; its contribution in $T(p)G_k(\Gamma)$ is $(p+1)/\gamma^{2k}$. If $\gamma \in \Gamma - p\Gamma$, then γ belongs to only one sublattice of index p and its contribution is $1/\gamma^{2k}$. Thus

$$\begin{aligned} T(p)G_k(\Gamma) &= G_k(\Gamma) + p\sum_{\gamma\in p\Gamma} 1/\gamma^{2k} = G_k(\Gamma) + pG_k(p\Gamma) \\ &= (1+p^{1-2k})G_k(\Gamma), \end{aligned}$$

which proves that G_k (viewed as a *function on* $\mathscr{R}$) is an eigenfunction of $T(p)$ with eigenvalue $1+p^{1-2k}$; viewed as a modular form, G_k is thus an eigenfunction of $\Gamma(p)$ with eigenvalue $p^{2k-1}(1+p^{1-2k}) = \sigma_{2k-1}(p)$. Formulas (34) and (35) of n° 4.2 show that the *normalized* eigenfunction associated with G_k is

$$(-1)^k \frac{B_k}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n.$$

This also shows that the eigenvalues of $T(n)$ are $\sigma_{2k-1}(n)$. Finally

$$\begin{aligned} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)/n^s &= \sum_{a,d\geqq 1} a^{2k-1}/a^s d^s \\ &= \Big(\sum_{d\geqq 1} 1/d^s\Big)\Big(\sum_{a\geqq 1} 1/a^{s+1-2k}\Big) \\ &= \zeta(s)\zeta(s-2k+1). \end{aligned}$$

b) *The Δ function*

Proposition 14.—*The Δ function is an eigenfunction of $T(n)$. The corresponding eigenvalue is $\tau(n)$ and the normalized eigenfunction is*

$$(2\pi)^{-12}\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n)q^n.$$

This is clear, since the space of cusp forms of weight 12 is of dimension 1, and is stable by the $T(n)$.

Corollary.—*We have*

$$\tau(nm) = \tau(n)\tau(m) \qquad \text{if } (n, m) = 1, \tag{52}$$

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1}) \quad \text{if } p \text{ is a prime, } n \geqq 1. \tag{53}$$

This follows from cor. 2 of th. 7.

Remark.—There are similar results when the space M_k^0 of cusp forms of weight $2k$ has dimension 1; this happens for

$$k = 6, 8, 9, 10, 11, 13 \text{ with basis } \Delta, \Delta G_2, \Delta G_3, \Delta G_4, \Delta G_5, \text{ and } \Delta G_7.$$

5.6. *Complements*

5.6.1. *The Petersson scalar product.*

Let f, g be two cusp forms of weight $2k$ with $k > 0$. One proves easily that the measure

$$\mu(f,g) = f(z)\overline{g(z)}y^{2k}dxdy/y^2 \qquad (x = R(z), y = Im(z))$$

is *invariant* by G and that it is a *bounded* measure on the quotient space H/G. By putting

$$\langle f, g\rangle = \int_{H/G} \mu(f, g) = \int_D f(z)\overline{g(z)}y^{2k-2}dxdy, \tag{87}$$

we obtain a hermitian scalar product on M_k^0 which is *positive* and *non-degenerate.* One can check that

$$\langle T(n)f, g\rangle = \langle f, T(n)g\rangle, \tag{88}$$

which means that the $T(n)$ are *hermitian* operators with respect to $\langle f, g\rangle$. Since the $T(n)$ commute with each other, a well known argument shows that *there exists an orthogonal basis of M_k^0 made of eigenvectors of* $T(n)$ and that the eigenvalues of $T(n)$ are *real numbers.*

5.6.2. *Integrality properties.*

Let $M_k(\mathbf{Z})$ be the set of modular forms

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

of weight $2k$ whose coefficients $c(n)$ are *integers*. One can prove that there exists a $\mathbf{Z}$-basis of $M_k(\mathbf{Z})$ which is a $\mathbf{C}$-basis of M_k. [More precisely, one can check that $M_k(\mathbf{Z})$ has the following basis (recall that $F = q\,\Pi\,(1-q^n)^{24}$):

k even: One takes the monomials $E_2^{\alpha}F^{\beta}$ where $\alpha, \beta \in \mathbf{N}$, and $\alpha + 3\beta = k/2$;

k odd: One takes the monomials $E_3E_2^{\alpha}F^{\beta}$ where $\alpha, \beta \in \mathbf{N}$, and $\alpha + 3\beta =$

$(k-3)/2$.] Proposition 12 shows that $M_k(\mathbf{Z})$ is stable under $T(n)$, $n \geqq 1$. We conclude from this that *the coefficients of the characteristic polynomial of* $T(n)$, *acting on* M_k, *are integers*(1); in particular the eigenvalues of the $T(n)$ are *algebraic integers* ("totally real", by 5.6.1).

5.6.3. *The Ramanujan-Petersson conjecture.*

Let $f = \sum_{n \geqq 1} c(n)q^n$, $c(1) = 1$, be a cusp form of weight $2k$ which is a normalized eigenfunction of the $T(n)$.

Let $\Phi_{f,p}(T) = 1 - c(p)T + p^{2k-1}T^2$, p prime, be the polynomial defined in n° 5.4, formula (83). We can write

(89) $$\Phi_{f,p}(T) = (1-\alpha_p T)(1-\alpha'_p T)$$

with

(90) $$\alpha_p + \alpha'_p = c(p),\ \alpha_p\alpha'_p = p^{2k-1}.$$

The *Petersson conjecture* is that α_p and α'_p are *complex conjugate.* One can also express it by:

$$|\alpha_p| = |\alpha'_p| = p^{k-1/2},$$

or

$$|c(p)| \leqq 2p^{k-1/2},$$

or

$$|c(n)| \leqq n^{k-1/2}\sigma_0(n) \quad \text{for all } n \geqq 1.$$

For $k = 6$, this is the Ramanujan conjecture: $|\tau(p)| \leqq 2p^{11/2}$.

These conjectures have been proved in 1973 by P. Deligne (*Publ. Math. I.H.E.S.* n°43, p. 302), as consequences of the "Weil conjectures" about algebraic varieties over finite fields.

§6. *Theta functions*

6.1. *The Poisson formula*

Let V be a real vector space of finite dimension n endowed with an invariant measure μ. Let V' be the *dual* of V. Let f be a rapidly decreasing smooth function on V (see, L. Schwartz, Théorie des Distributions, chap. VII, §3). The *Fourier transform* f' of f is defined by the formula

(91) $$f'(y) = \int_V e^{-2i\pi\langle x,y\rangle} f(x)\mu(x).$$

This is a rapidly decreasing smooth function on V'.

Let now Γ be a *lattice* in V' (see n° 2.2). We denote by Γ' the lattice in V' *dual* to Γ; it is the set of $y \in V'$ such that $\langle x, y\rangle \in \mathbf{Z}$ for all $x \in \Gamma$. One

(1) We point out that there exists an *explicit formula* giving the trace of $T(n)$, cf. M. Eichler and A. Selberg, *Journ. Indian Math. Soc.*, 20, 1956.

checks easily that Γ' may be identified with the **Z**-dual of Γ (hence the terminology).

Proposition 15.—*Let $v = \mu(V/\Gamma)$. One has:*

$$\sum_{x\in\Gamma} f(x) = \frac{1}{v} \sum_{y\in\Gamma'} f'(y). \tag{92}$$

After replacing μ by $v^{-1}\mu$, we can assume that $\mu(V/\Gamma) = 1$. By taking a basis $e_1, \ldots, e_n$ of Γ, we identify V with $\mathbf{R}^n$, Γ with $\mathbf{Z}^n$, and μ with the product measure $dx_1 \ldots dx_n$. Thus we have $V' = \mathbf{R}^n$, $\Gamma' = \mathbf{Z}^n$ and we are reduced to the classical Poisson formula (SCHWARTZ, *loc. cit.*, formule (VII, 7:5)).

6.2. *Application to quadratic forms*

We suppose henceforth that V is endowed with a symmetric bilinear form $x.y$ which is *positive and nondegenerate* (i.e. $x.x > 0$ if $x \neq 0$). We identify V with V' by means of this bilinear form. The lattice Γ' becomes thus a *lattice* in V; one has $y \in \Gamma'$ if and only if $x.y \in \mathbf{Z}$ for all $x \in \Gamma$.

To a lattice Γ, we associate the following function defined on $\mathbf{R}^*_+$:

$$\Theta_\Gamma(t) = \sum_{x\in\Gamma} e^{-\pi t x.x}. \tag{93}$$

We choose the invariant measure μ on V such that, if $\varepsilon_1, \ldots \varepsilon_n$ is an orthonormal basis of V, the unit cube defined by the ε_i has volume 1. The volume v of the lattice Γ is then defined by $v = \mu(V/\Gamma)$, cf. n° 6.1.

Proposition 16.—*We have the identity*

$$\Theta_\Gamma(t) = t^{-n/2} v^{-1} \Theta_{\Gamma'}(t^{-1}). \tag{94}$$

Let $f = e^{-\pi x.x}$. It is a rapidly decreasing smooth function on V. The Fourier transform f' of f *is equal to* f. Indeed, choose an orthonormal basis of V and use this basis to identify V with $\mathbf{R}^n$; the measure μ becomes the measure $dx = dx_1 \ldots dx_n$ and the function f is

$$f = e^{-\pi(x_1^2 + \cdots + x_n^2)}.$$

We are thus reduced to showing that the Fourier transform of $e^{-\pi x^2}$ is $e^{-\pi x^2}$, which is well known.

We now apply prop. 15 to the function f and to the lattice $t^{1/2}\Gamma$; the volume of this lattice is $t^{n/2}v$ and its dual is $t^{-1/2}\Gamma'$; hence we get the formula to be proved.

6.3. *Matrix interpretation*

Let $e_1, \ldots, e_n$ be a basis of Γ. Put $a_{ij} = e_i.e_j$. The matrix $A = (a_{ij})$ is positive, nondegenerate and symmetric. If $x = \Sigma x_i e_i$ is an element of V, then

$$x.x = \Sigma a_{ij} x_i x_j.$$

The function Θ_Γ can be written

(95) $$\Theta_\Gamma(t) = \sum_{x_i \in \mathbf{Z}} e^{-\pi t \Sigma a_{ij} x_i x_j}.$$

The *volume* v of Γ is given by:

(96) $$v = \det(A)^{1/2}.$$

This can be seen as follows: Let $\varepsilon_1, \ldots, \varepsilon_n$ be an orthonormal basis of V and put

$$\varepsilon = \varepsilon_1 \wedge \ldots \wedge \varepsilon_n, \quad e = e_1 \wedge \ldots \wedge e_n.$$

We have $e = \lambda\varepsilon$ with $|\lambda| = v$. Moreover, $e.e = \det(A)\, \varepsilon.\varepsilon$, and by comparing, we obtain $v^2 = \det(A)$.

Let $B = (b_{ij})$ be the matrix inverse to A. One checks immediately that the dual basis (e'_i) to (e_i) is given by the formulas:

$$e'_i = \sum b_{ij} e_j.$$

The (e'_i) form a basis of Γ'. The matrix $(e'_i.e'_j)$ is equal to B. This shows in particular that if $v' = \mu(V/\Gamma')$, then we have $vv' = 1$.

6.4. *Special case*

We will be interested in pairs (V, Γ) which have the following two properties:

(i) *The dual* Γ' *of* Γ *is equal to* Γ.

This amounts to saying that one has $x.y \in \mathbf{Z}$ for $x, y \in \Gamma$ and that the form $x.y$ defines an *isomorphism* of Γ onto its dual. In matrix terms, it means that the matrix $A = (e_i.e_j)$ has *integer coefficients* and that *its determinant equals* 1. By (96) the last condition is equivalent to $v = 1$.

If $n = \dim V$, this condition implies that the quadratic module Γ belongs to the category S_n defined in n° 1.1 of chap. V. Conversely, if $\Gamma \in S_n$ is positive definite, and if one puts $V = \Gamma \otimes \mathbf{R}$, the pair (V, Γ) satisfies (i).

(ii) *We have* $x.x \equiv 0 \pmod 2$ *for all* $x \in \Gamma$.

This means that Γ is *of type* II, in the sense of chap. V, n° 1.3.5, or else that the diagonal terms $e_i.e_i$ of the matrix A are *even*.

We have given in chap. V some examples of such lattices Γ.

6.5. *Theta functions*

In this section and the next one, we assume that the pair (V, Γ) satisfies conditions (i) and (ii) of the preceding section.

Let m be an integer $\geqq 0$, and denote by $r_\Gamma(m)$ the number of elements x of Γ such that $x.x = 2m$. It is easy to see that $r_\Gamma(m)$ is bounded by a polynomial in m (a crude volume argument gives for instance $r_\Gamma(m) = O(m^{n/2})$). This shows that the series with integer coefficients

$$\sum_{m=0}^{\infty} r_\Gamma(m)q^m = 1+r_\Gamma(1)q+\ldots$$

converges for $|q| < 1$. Thus one can define a function θ_Γ on the half plane H by the formula

(97) $$\theta_\Gamma(z) = \sum_{m=0} r_\Gamma(m)q^m \quad (\text{where } q = e^{2\pi iz}).$$

We have:

(98) $$\theta_\Gamma(z) = \sum_{x\in\Gamma} q^{(x,x)/2} = \sum_{x\in\Gamma} e^{\pi iz(x,x)}.$$

The function θ_Γ is called the *theta function* of the quadratic module Γ. It is holomorphic on H.

Theorem 8.—(a) *The dimension n of V is divisible by 8.*
(b) *The function θ_Γ is a modular form of weight $n/2$.*

Assertion (a) has already been proved (chap. V, n° 2.1, cor. 2 to th. 2). We prove the identity

(99) $$\theta_\Gamma(-1/z) = (iz)^{n/2}\theta_\Gamma(z).$$

Since the two sides are analytic in z, it suffices to prove this formula when $z = it$ with t real >0. We have

$$\theta_\Gamma(it) = \sum_{x\in\Gamma} e^{-\pi t(x,x)} = \Theta_\Gamma(t).$$

Similarly, $\theta_\Gamma(-1/it) = \Theta_\Gamma(t^{-1})$. Formula (99) results thus from (94), taking into account that $v = 1$ and $\Gamma = \Gamma'$.

Since n is divisible by 8, we can rewrite (99) in the form

(100) $$\theta_\Gamma(-1/z) = z^{n/2}\theta_\Gamma(z)$$

which shows that θ_Γ is a modular form of weight $n/2$.

[We indicate briefly another proof of (a). Suppose that n is not divisible by 8; replacing Γ, if necessary, by $\Gamma\oplus\Gamma$ or $\Gamma\oplus\Gamma\oplus\Gamma\oplus\Gamma$, we may suppose that $n \equiv 4 \pmod 8$. Formula (99) can then be written

$$\theta_\Gamma(-1/z) = (-1)^{n/4}z^{m/2}\theta_\Gamma(z) = -z^{n/2}\theta_\Gamma(z).$$

If we put $\omega(z) = \theta_\Gamma(z)dz^{n/4}$, we see that the differential form ω is transformed into $-\omega$ by $S:z\mapsto -1/z$. Since ω is invariant by $T:z\mapsto z+1$, we see that ST transforms ω into $-\omega$, which is absurd because $(ST)^3 = 1$.]

Corollary 1.—*There exists a cusp form f_Γ of weight $n/2$ such that*

(101) $$\theta_\Gamma = E_k+f_\Gamma \quad \textit{where } k = n/4.$$

This follows from the fact that $\theta_\Gamma(\infty) = 1$, hence that $\theta_\Gamma - E_k$ is a cusp form.

Corollary 2.—*We have* $r_\Gamma(m) = \dfrac{4k}{B_k}\sigma_{2k-1}(m)+O(m^k)$ *where* $k = n/4$.

This follows from cor. 1, formula (34) and th. 5.

Remark.—The "error term" f_Γ is in general not zero. However Siegel has proved that the *weighted mean of the* f_Γ *is zero*. More precisely, let C_n be the set of classes (up to isomorphism) of lattices Γ verifying (i) and (ii) and denote by g_Γ the order of the automorphism group of $\Gamma \in C_n$ (cf. chap. V, n° 2.3). One has:

$$\sum_{\Gamma \in C_n} \frac{1}{g_\Gamma} \cdot f_\Gamma = 0 \tag{102}$$

or equivalently

$$\sum_{\Gamma \in C_n} \frac{1}{g_\Gamma} \theta_\Gamma = M_n E_k \quad \text{where } M_n = \sum_{\Gamma \in C_n} \frac{1}{g_\Gamma}. \tag{103}$$

Note that this is also equivalent to saying that the weighted mean of the θ_Γ is an *eigenfunction* of the $T(n)$.

For a proof of formulas (102) and (103), see C. L. SIEGEL, *Gesam. Abh.*, n° 20.

6.6. *Examples*

i) *The case* $n = 8$.

Every cusp form of weight $n/2 = 4$ is zero. Cor. 1 of th. 8 then shows that $\theta_\Gamma = E_2$, in other words:

$$r_\Gamma(m) = 240\sigma_3(m) \quad \text{for all integers } m \geqq 1. \tag{104}$$

This applies to the lattice Γ_8 constructed in chap. V, n° 1.4.3 (note that this lattice is the only element of C_8).

ii) *The case* $n = 16$.

For the same reason as above, we have:

$$\theta_\Gamma = E_4 = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m. \tag{105}$$

Here one may take $\Gamma = \Gamma_8 \oplus \Gamma_8$ or $\Gamma = \Gamma_{16}$ (with the notations of chap. V, n° 1.4.3); even though these two lattices are not isomorphic, they have the same theta function, i.e. they represent each integer the same number of times.

Note that the function θ attached to the lattice $\Gamma_8 \oplus \Gamma_8$ is the *square* of the function θ of Γ_8; we recover thus the identity:

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

iii) *The case* $n = 24$.

The space of modular forms of weight 12 is of dimension 2. It has for basis the two functions:

$$E_6 = 1 + \frac{65520}{691} \sum_{m=1}^{\infty} \sigma_{11}(m) q^m,$$

$$F = (2\pi)^{-12}\Delta = q \prod_{m=1}^{\infty} (1-q^m)^{24} = \sum_{m=1}^{\infty} \tau(m)q^m.$$

The theta function associated with the lattice Γ can thus be written

(106) $$\theta_\Gamma = E_6 + c_\Gamma F \quad \text{with } c_\Gamma \in \mathbf{Q}.$$

We have

(107) $$r_\Gamma(m) = \frac{65520}{691}\sigma_{11}(m) + c_\Gamma \tau(m) \quad \text{for } m \geqq 1.$$

The coefficient c_Γ is determined by putting $m = 1$:

(108) $$c_\Gamma = r_\Gamma(1) - \frac{65520}{691}.$$

Note that it is $\neq 0$ since 65520/691 is not an integer.

Examples.

a) The lattice Γ constructed by J. Leech (*Canad. J. Math.*, 16, 1964) is such that $r_\Gamma(1) = 0$. Hence:

$$c_\Gamma = -\frac{65520}{691} = -2^4.3^2.5.7.13/691.$$

b) For $\Gamma = \Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8$, we have $r_\Gamma(1) = 3.240$, hence:

$$c_\Gamma = \frac{432000}{691} = 2^7 3^3 5^3/691.$$

c) For $\Gamma = \Gamma_{24}$, we have $r_\Gamma(1) = 2.24.23$, hence:

$$c_\Gamma = \frac{697344}{691} = 2^{10}3.227/691.$$

6.7. *Complements*

The fact that we consider only the full modular group $G = \mathbf{PSL}_2(\mathbf{Z})$, forced us to limit ourselves to lattices verifying the very restrictive conditions of n° 6.4. In particular, we have not treated the most natural case, that of the quadratic forms

$$x_1^2 + \ldots + x_n^2,$$

which verify (i) but not (ii). The corresponding theta functions are "modular forms of weight $n/2$" (note that $n/2$ is not necessarily an integer) with respect to the subgroup of G generated by S and T^2. This group has index 3 in G, and its fundamental domain has two "cusps" to which correspond two types of "Eisenstein series"; using them, one obtains formulas giving the number of representations of an integer as a sum of n squares; for more details, see the books and papers quoted in the bibliography.

Bibliography

Some classics

C. F. GAUSS—*Disquisitiones arithmeticae*, 1801, *Werke*, Bd. I. (English translation: Yale Univ. Press—French translation: Blanchard.)
C. JACOBI—*Fundamenta nova theoriae functionum ellipticarum*, 1829, *Gesammelte Werke*, Bd. I., pp. 49–239.
G. LEJEUNE DIRICHLET—*Démonstration d'un théorème sur la progression arithmétique*, 1834, *Werke*, Bd. I, p. 307.
G. EISENSTEIN, *Mathematische Werke*, Chelsea, 1975.
B. RIEMANN—*Gesammelte mathematische Werke*, Teubner, 1892 (English translation: Dover—partial French translation: Gauthier-Villars, 1898).
D. HILBERT—*Die Theorie der algebraischer Zahlkörper*, *Gesam. Abh.*, Bd. I, pp. 63–363 (French translation: *Ann. Fac. Sci. Toulouse*, 1909 and 1910).
H. MINKOWSKI—*Gesammelte Abhandlungen*, Teubner, 1911; Chelsea, 1967.
A. HURWITZ—*Mathematische Werke*, Birkhäuser Verlag, 1932.
E. HECKE—*Mathematische Werke*, Göttingen, 1959.
C. L. SIEGEL—*Gesammelte Abhandlungen*, Springer-Verlag, 1966–1979.
A. WEIL—*Collected Papers*, Springer-Verlag, 1980.

Number fields and local fields

E. HECKE—*Algebraische Zahlen*, Leipzig, 1923.
Z. I. BOREVICH and I. R. SHAFAREVICH—*Number Theory* (translated from Russian) Academic Press, 1966. (There exist also translations into French and German.)
M. EICHLER—*Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser Verlag, 1963 (English translation: Academic Press, 1966).
J-P. SERRE—*Corps Locaux*, Hermann, 1962.
P. SAMUEL—*Théorie algébrique des nombres*, Hermann, 1967.
E. ARTIN and J. TATE—*Class Field Theory*, Benjamin, 1968.
J. CASSELS and A. FRÖHLICH (edit.)—*Algebraic Number Theory*, Academic Press, 1967.
A. WEIL—*Basic Number Theory*, Springer-Verlag, 1967.
S. LANG—*Algebraic Number Theory*, Addison-Wesley, 1970.
(The four last works contain an exposition of the so-called "class field theory".)

Quadratic forms

a) *Generalities, Witt's theorem*

E. WITT—*Theorie der quadratischen Formen in beliebigen Körpern*, J. Crelle, 176, 1937, pp. 31–44.
N. BOURBAKI—*Algèbre*, chap. IX, Hermann, 1959.
E. ARTIN—*Geometric Algebra*, Interscience Publ., 1957 (French translation: Gauthier-Villars, 1962).

b) *Arithmetic properties*

B. JONES—*The arithmetic theory of quadratic forms*, Carus Mon., n° 10, John Wiley and Sons, 1950.
M. EICHLER—*Quadratische Formen und orthogonale Gruppen*, Springer-Verlag, 1952.
G. L. WATSON—*Integral quadratic forms*, Cambridge Tracts, n° 51. Cambridge, 1960.
O. T. O'MEARA—*Introduction to quadratic forms*. Springer-Verlag, 1963.
J. MILNOR and D. HUSEMOLLER—*Symmetric Bilinear Forms*, Springer-Verlag, 1973.
T. Y. LAM—*The algebraic theory of quadratic forms*, New York, Benjamin, 1973.
J. W. S. CASSELS—*Rational Quadratic Forms*, Academic Press, 1978.

c) *Integral quadratic forms with discriminant* ± 1

E. Witt—*Eine Identität zwischen Modulformen zweiten Grades*, Abh. math. Sem. Univ. Hamburg, 14, 1941, pp. 323–337.
M. Kneser—*Klassenzahlen definiter quadratischer Formen*, Arch. der Math. 8, 1957, pp. 241–250.
J. Milnor—*On simply connected manifolds*, Symp. Mexico, 1958, pp. 122–128.
J. Milnor—*A procedure for killing homotopy groups of differentiable manifolds*, Symp. Amer. Math. Soc., n° 3, 1961, pp. 39–55.
J. H. Conway and N. J. A. Sloane—*Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

Dirichlet theorem, zeta function and L-functions

J. Hadamard—*Sur la distribution des zéros de la fonction* $\zeta(s)$ *et ses conséquences arithmétiques*, 1896, Oeuvres, CNRS, t. 1, pp. 189–210.
E. Landau—*Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, 1909; Chelsea, 1953.
A. Selberg—*An elementary proof of the prime number theorem for arithmetic progressions*, Canad. J. Math., 2, 1950, pp. 66–78.
E. C. Titchmarsh—*The Theory of the Riemann zeta-function*, Oxford, 1951.
K. Prachar—*Primzahlverteilung*, Springer-Verlag, 1957.
H. Davenport—*Multiplicative number theory*, second edition, Springer-Verlag, 1980.
K. Chandrasekharan—*Introduction to analytic number theory*, Springer-Verlag, 1968.
A. Blanchard—*Initiation à la théorie analytique des nombres premiers*, Dunod, 1969.
H. M. Edwards—*Riemann's zeta function*, New York, Acad. Press, 1974.
W. Narkiewicz—*Elementary and analytic theory of algebraic numbers*, Warsaw, Mon. Mat. 57, 1974.
W. Ellison—*Les Nombres Premiers*, Paris, Hermann, 1975.

Modular functions

F. Klein—*Vorlesungen über die Theorie der elliptischen Modulfunktionen*, Leipzig, 1890.
S. Ramanujan—*On certain arithmetical functions*, Trans. Cambridge Phil. Soc., 22, 1916, pp. 159–184 (= *Collected Papers*, pp. 136–162).
G. Hardy—*Ramanujan*, Cambridge Univ. Press, 1940.
R. Godement—*Travaux de Hecke*, Sém. Bourbaki, 1952–53, exposés 74, 80.
R. C. Gunning—*Lectures on modular forms* (notes by A. Brumer), Ann. of Math. Studies, Princeton, 1962.
A. Borel et al.—*Seminar on complex multiplication*, Lecture Notes in Maths., n° 21, Springer-Verlag, 1966.
A. Ogg—*Modular forms and Dirichlet series*, Benjamin, 1969.
G. Shimura—*Introduction to the arithmetic theory of automorphic functions*, Tokyo-Princeton, 1971.
H. Rademacher—*Topics in Analytic Number Theory*, Springer-Verlag, 1973.
W. Kuyk et al. (edit.)—*Modular Functions of One Variable*, I, . . . , VI, *Lecture Notes in Math.*, 320, 349, 350, 476, 601, 627, Springer-Verlag, 1973–1977.
P. Deligne—*La conjecture de Weil* I, Publ. Math. I.H.E.S., 43, 1974, p. 273–307.
A. Weil—*Elliptic Functions according to Eisenstein and Kronecker*, Springer-Verlag, 1976.
S. Lang—*Introduction to Modular Forms*, Springer-Verlag, 1976.
R. Rankin—*Modular Forms and Functions*, Cambridge Univ. Press, 1977.

(See also the works of Hecke, Siegel and Weil quoted above.)

Index of Definitions

Index of Notations