SIEGEL MODULAR FORMS AND RADIAL DIRICLET SERIES

Anatoli Andrianov and Fedor Andrianov

Contents

1991 *Mathematics Subject Classification.* 11F46, 11F60, 11F66.

Key words and phrases. Hecke operators, Hecke-Shimura rings, Siegel modular forms, zeta functions of modular forms.

Introduction: On arithmetical zeta functions

A zeta function in Arithmetic is generally speaking a generating function for an arithmetical problem written in the form of Dirichlet series. A right zeta function must have at least two principal features: *an Euler product factorization* and *an analytic continuation* over whole complex plane satisfying *functional equations*. The first reflects relations between the global arithmetical problem and its localizations, while the second provides a kind of reciprocity between the localizations.

Let us illustrate it on examples:

1. *The Riemann zeta function*,

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\qquad (\Re s>1),$$

is the generating function for the numbers of ideals of given norm in the ring $\mathbb{Z}$ of rational integers. It has Euler product factorization of the form

$$\zeta(s)=\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1},\qquad (\Re s>1),$$

the product being over all rational prime numbers p.

It was B.Riemann, who proved in the middle of nineteenth century that $\zeta(s)$ has analytic continuation over whole complex s-plane, is holomorphic, except for a simple pole of residue 1 at $s=1$, and satisfies the functional equation that the function $\pi^{-s/2}\Gamma(s/2)\zeta(s)$, where Γ is the gamma function, is invariant under $s\mapsto 1-s$. He also discovered that the problem of *distribution of prime numbers* closely connected with *location of complex zeroes* of the zeta function in the vertical strip $0\le\Re s\le 1$. At the end of the century J.Hadamard and Ch.de la Vallee Poussin have proved that $\zeta(s)$ has no zeroes on the line $\Re s=1$, which implied the famous asymptotic formula for the number $\pi(x)$ of prime numbers not exceeding x,

$$\pi(x)\sim\frac{x}{\log x},\qquad (x\to\infty).$$

2. *A global zeta function of a nonsingular algebraic variety* V over the field $\mathbb{Q}$ of rational numbers is defined by an Euler product

$$\zeta^{*}(V,\,s)=\prod_{p}\zeta\left(V_p,\,p^{-s}\right)$$

of *local zeta functions* $\zeta(V_p,\,p^{-s})$, where p runs over all prime numbers such that V has a good *reduction* V_p *modulo* p, i.e. the good and, in particular, nonsingular variety V_p over the finite field $\mathbb{F}(p)$ of p elements obtained by replacing of equations defining V by corresponding congruences modulo p; the local zeta function is the zeta function of V_p defined by

$$\zeta\,(V_p,\,t) = \exp\left(\sum_{\delta=1}^{\infty} N(p^\delta)t^\delta/\delta\right)$$

where $N(p^\delta)$ is the number of points of V_p with coordinates in the finite field $\mathbb{F}(p^\delta)$ of p^δ elements. According to B.Dwork, the local zeta functions $\zeta\,(V_p,\,t)$ of nonsingular varieties V_p are rational fractions in t. It follows that the global zeta function $\zeta^*\,(V,\,s)$ can be written as a Dirichlet series convergent in a right half-plane of the complex variable s. It is generally believed that the zeta function can be analytically continued over whole s–plane as a meromorphic function and satisfies a functional equation, but it is doubtful that a human being living now will see a complete proof.

Nevertheless even particular cases present considerable interest. Let us consider a (*projective*) *elliptic curve*

$$E: \quad y^2z = x^3 + axz^2 + bz^3, \qquad (a,\,b \in \mathbb{Z}).$$

The points on E with coordinates in $\mathbb{Q}$ form an Abelian group, which we denote by $E_{\mathbb{Q}}$; the theorem of Mordell tells us that the group $E_{\mathbb{Q}}$ is finitely generated, i.e. is a product of a finite group by a lattice of a finite rank g. A principal problem of the theory is to determine the group $E_{\mathbb{Q}}$, and, in particular, to determine the rank g. In the mid-sixtieth B.J.Birch and H.P.F.Swinnerton-Dyer had put forward revolutionary conjectures connecting the group $E_{\mathbb{Q}}$ with the zeta function $\zeta^*\,(E,\,s)$ of the curve. Let us recall some details.

A prime number p is said to be good, if it does not divide $6(27b^2 + 4a^3)$. For such a prime p, the reduction

$$E_p: \quad y^2z \equiv x^3 + axz^2 + bz^3 \pmod p$$

of E modulo p, is an elliptic curve over $\mathbb{F}(p)$. It is well known that the zeta function of E_p over $\mathbb{F}(p)$ has the form

$$\zeta\,(E_p,\,t) = \frac{1-(1+p-N(p))t+pt^2}{(1-t)(1-pt)}.$$

Then we may define an L–function of E by

$$L^*(E,\,s) = \prod_p \bigl(1-(1+p-N(p))p^{-s}+p^{1-2s}\bigr)^{-1},$$

where the product is taken over all good primes. It converges for $\Re s > 3/2$. Then the main *Birch–Swinnerton-Dyer conjecture* says that $L^*(E, s)$ has a zero of order g at $s = 1$. Generally it is still open.

3. Despite clear importance of zeta functions of algebraic varieties, algebraic geometry provides no means for their investigation. The only hope is to relate them with techniques coming from an analytical background, probably, with *zeta functions of automorphic forms*, which, on the contrary, have usually vast means for analytical investigation, but often lack clear arithmetical motivation.

Let us consider the simplest case of zeta functions of modular forms of integral weights for congruence subgroups K of the modular group $SL_2(\mathbb{Z})$. Let us recall the corresponding definitions.

A function F on the upper half-plane $\mathbb{H} = \{x + iy \in \mathbb{C} \bigm| y > 0\}$ is said to be *a modular cusp form* of weight k for the group K, if it is holomorphic on $\mathbb{H}$, equals zero at all cusps of K, and satisfies

$$(cz+d)^{-k} F\left(\frac{az+b}{ac+d}\right) = F(z) \quad \text{for each} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K.$$

All such functions form a finite dimensional space $\mathfrak{N} = \mathfrak{N}_k(K)$ over the field $\mathbb{C}$ of complex numbers. If the group K contains the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then every $F \in \mathfrak{N}$ can be presented by an absolutely convergent on $\mathbb{H}$ *Fourier series* of the form

$$F(z) = \sum_{m=1}^{\infty} \phi(m) \exp(2\pi i m z)$$

with constant Fourier coefficients $\phi(m)$. *A zeta function* of F can be defined then by the Dirichlet series

$$Z(F, s) = \sum_{m=1}^{\infty} \frac{\phi(m)}{n^s}.$$

The series absolutely converges in a right half-plane of the variable s, and can be presented there by means of a Mellin integral

$$\Phi(s) = \Phi(F, s) = \int_0^{\infty} F(iy) y^{s-1} dy = (2\pi)^{-s} \Gamma(s) Z(F, s).$$

Suppose that the group K satisfies

$$\begin{pmatrix} 0 & -1 \\ q & 0 \end{pmatrix}^{-1} K \begin{pmatrix} 0 & -1 \\ q & 0 \end{pmatrix} = K$$

for an positive integer q. Then it is easy to check that, for each cusp form $F \in \mathfrak{N}$, the function

$$(F \mid \omega)(z) = q^{-k/2} z^{-k} F(-1/qz)$$

again belongs to $\mathfrak{N}$ and satisfies $F \mid \omega \mid \omega = (-1)^k F$. It follows that we can write a direct sum decomposition

$$\mathfrak{N} = \mathfrak{N}^+ + \mathfrak{N}^-, \quad \text{where, for} \quad F \in \mathfrak{N}^\pm, \quad F \mid \omega = \pm i^k F.$$

Exercise. *Prove the above assertions.*

If $F \in \mathfrak{N}^\pm$, then

$$F(i/qy) = \pm(-1)^k q^{k/2} y^k F(iy), \qquad (y > 0),$$

and we can write, for $\Re s$ sufficiently large,

$$\Phi(s) = \int_0^{q^{-1/2}} F(iy) y^{s-1} dy + \int_{q^{-1/2}}^\infty F(iy) y^{s-1} dy$$

$$= \int_{q^{-1/2}}^\infty F(i/qy)(1/qy)^{s-1}(1/qy^2) dy + \int_{q^{-1/2}}^\infty F(iy) y^{s-1} dy$$

$$= \pm(-1)^k q^{k/2-s} \int_{q^{-1/2}}^\infty F(iy) y^{k-s-1} dy + \int_{q^{-1/2}}^\infty F(iy) y^{s-1} dy.$$

The both of the last integrals are holomorphic for all s, and so is the function $\phi(s)$. Besides, the last expression implies that

$$\Phi(k-s) = \pm(-1)^k q^{s-k/2} \Phi(s),$$

which is the functional equation for the zeta function $Z(F, s)$.

Note that the simplest of the groups K satisfying the cited conditions is the group

$$\Gamma_0(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{q} \right\}.$$

The problem of Euler product factorization of zeta functions corresponding to modular forms of integral weights for the groups of type $\Gamma_0(q)$ was essentially solved by E.Hecke in 1937 and completed by A.O.L.Atkin and J.Lehner in 1970. In particular, it was found that, although the zeta function of a cusp form not necessarily have an Euler product factorization, but the space of cusp forms has a basis consisting of forms with zeta functions decomposable into Euler products. Such forms can be characterized as eigenfunctions of certain rings of linear operators, the Hecke operators, acting on the space.

Since the nineteenth century the main arithmetical application of modular forms was the analytical theory of integral quadratic forms. The reason is that the generating Fourier series with coefficients equal to numbers of integral representations of positive integers by a positive definite integral quadratic form is a modular (not cusp) form. But in the middle of the twentieth century G.Shimura and Y.Taniyama proposed famous conjectures relating modular forms and elliptic curves over $\mathbb{Q}$. The *Shimura–Taniyama conjecture* includes conjecture that the L–function $L^*(E, s)$ of any elliptic curve E over $\mathbb{Q}$ completed by appropriate p-factors for bad primes is, in fact, the zeta function of a cusp form of weight 2 for the group $\Gamma_0(q)$, where q is the product of some degrees of bad primes. In 1985 G.Frey made the remarkable observation that this conjecture would imply Fermat's Last Theorem. The precise relation of the two was established by K.A.Ribet in 1986, which allowed A.Wiles in 1995 to prove the Fermat's Last Theorem, one of the brightest achievements of mathematics of the twentieth century.

One can hardly doubt that the relation between zeta functions of elliptic curves and zeta functions of modular forms in one variable described by Shimura–Taniyama conjecture is only a particular case of some general links of global zeta functions of algebraic varieties and zeta functions of automorphic forms. Speaking on Abelian varieties in place of elliptic curves, one can expect that modular forms in one variable should be replaced by Siegel modular forms for congruence subgroups of the symplectic modular group $\Gamma^n = Sp_n(\mathbb{Z})$, which expectation is supported by numerical evidences.

Contents. The main objective of this course is to give an introduction to arithmetical theory of Siegel modular forms, Hecke operators, and zeta functions. In the case of several variables we are trying to be so precise but short as was Andrew Ogg in his excellent course *Modular Forms and Dirichlet series*, published in 1969 by W.A.Benjamin, INC.

In Chapter 1 we give a compressed exposition of essential features of the theory of Siegel modular forms of integral weights for congruence subgroups of the symplectic modular group $Sp_n(\mathbb{Z})$. Chapter 2 treats analytical properties of radial Dirichlet series corresponding to modular forms of genuses 1 and 2. Chapter 3 is devoted to the theory of Hecke–Shimura rings and Hecke operators on Siegel modular forms of arbitrary genus. In Chapter 4 we consider applications of Hecke operators to Euler product factorization of the radial Dirichlet series, which leads us to Andrianov zeta functions of Siegel modular forms. The course contains a number of exercises which usually indicate some interesting points not included into the main text, partly for the reasons of volume and partly because of their incompleteness.

Sources. We try to expose the proofs in full, whenever it is reasonable and possible. The omitted details can be mainly found in the books Andrianov,A.N.:

Quadratic forms and Hecke operators, Springer-Verlag, Berlin, Heidelberg, ..., 1987, 374 p. (Grundlehren Math. Wiss., Bd. 286), cited below as the *Source*, or Andrianov,A.N.; Zhuravlev,V.G.: Modular forms and Hecke operators, Nauka, Moskow, 1990, 447 p. (in Russian). The English edition: AMS, Providence, Rhode Island, Transl. of Math. Monographs, vol.145, 1995, 334 p.. The Notes at the end of the book contain essential references. The main text contains no references exept for general references on the *Source*.

Notation. We reserve the letters $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ for the set of positive rational integers, the ring of rational integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively.

$\mathbb{A}_n^m$ is the set of all $m \times n$-matrices with entries in a set $\mathbb{A}$, $\mathbb{A}^n = \mathbb{A}_1^n$, and $\mathbb{A}_n = \mathbb{A}_n^1$.

If M is a matrix, ${}^tM$ always denotes the transpose of M. If M is a square matrix, $\sigma(M)$ usually stands for the trace of M. For a matrix M over $\mathbb{C}$, $\overline{M}$ is the matrix with complex conjugate entries. If Y is a real symmetric matrix, $Y > 0$ (resp., $Y \geqq 0$) means that Y is positive definite (resp., positive semidefinite). For two matrices A and B we write

$$A[B] = {}^tABA$$

if the product on the right is defined.

Chapter 1. Modular form

§1.1. Symplectic group and upper half-plane.

A matrix $M \in \mathbb{C}_{2n}^{2n}$ is said to be *symplectic* if it satisfies the relation

$$ {}^tMJM = \mu(M)J, \quad \text{with} \quad J = J_n = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}, \tag{1.0}$$

with a nonzero scalar $\mu(M)$ called the *multiplier* of M. It is clear that product of two symplectic matrices of the same order is again a symplectic matrix, and the multiplier of the product is the product of multipliers of factors.

Lemma 1.1. *Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where the blocks A, B, C, and D are complex square matrices of order n, and let μ be a nonzero complex number. Then the following conditions are equivalent:*

(1) *M is symplectic with the multiplier $\mu(M) = \mu$;*
(2) *${}^tM$ is symplectic with the multiplier $\mu({}^tM) = \mu$;*
(3) *M is invertible, and*

$$\mu M^{-1} = \begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix}; \tag{1.1}$$

(4) *The blocks A, B, C, and D satisfy the conditions*

$$ {}^tAC = {}^tCA, \quad {}^tBD = {}^tDB, \quad \text{and} \quad {}^tAD -{}^tCB = \mu E \tag{1.2}$$

or the conditions

$$ A\,{}^tB = B\,{}^tA, \quad C\,{}^tD = D\,{}^tC, \quad \text{and} \quad A\,{}^tD - B\,{}^tC = \mu E. \tag{1.3}$$

Proof. It is an easy exercise on multiplication of block-matrices.△

Exercise 1.2. *Prove the lemma.*

In the course of our arithmetical considerations we shall be interested in discrete subgroups and subsemigroups of the *general real positive symplectic group of genus n* consisting of all real symplectic matrices of order $2n$ with positive multipliers:

$$\mathbb{G} = \mathbb{G}^n = GSp_n^+(\mathbb{R}) = \left\{ M \in \mathbb{R}_{2n}^{2n} \;\middle|\; {}^tMJM = \mu(M)J,\, \mu(M) > 0 \right\}. \tag{1.4}$$

The group $\mathbb{G}$ is a real Lie group acting as a group of analytic automorphisms on the $n(n+1)/2$-dimensional open complex variety

$$\mathbb{H} = \mathbb{H}^n = \left\{ Z = X + iY \in \mathbb{C}_n^n \;\middle|\; {}^tZ = Z, \quad Y > 0 \right\}, \tag{1.5}$$

the *upper half-plane of genus* n, by the rule

$$\mathbb{G} \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} : Z \mapsto M\langle Z\rangle = (AZ+B)(CZ+D)^{-1}, \quad (Z \in \mathbb{H}). \tag{1.6}$$

In order to verify it, we have to check that the mapping (1.6) is always defined, maps the upper half-plane into itself, and satisfies

$$(MM')\langle Z\rangle = M\langle M'\langle Z\rangle\rangle, \quad (M,\, M' \in \mathbb{G},\, Z \in \mathbb{H}). \tag{1.7}$$

The relations (1.7) follow from definition by the formal comparison of both parts, provided that the both parts are defined. So it would be sufficient to prove the following two lemmas.

Lemma 1.3. *For every matrices* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{G}$ *and* $Z \in \mathbb{H}$*, the matrices*

$$J(M,\, Z) = CZ + D \tag{1.8}$$

are nonsingular and satisfy the rule

$$J(MM',\, Z) = J(M,\, M'\langle Z\rangle)J(M',\, Z), \quad (M, M' \in \mathbb{G},\, Z \in \mathbb{H}). \tag{1.9}$$

Proof. The relation (1.9) formally follows from definitions, if the matrix $J(M',\, Z)$ is nonsingular.

First, note that the matrix (1.8) is nonsingular for every $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{G}$ and $Z = iE$. Otherwise the matrix

$$(Ci+D)\,{}^t\overline{(Ci+D)} = C\,{}^tC + D\,{}^tD + i(C\,{}^tD - D\,{}^tC) = C\,{}^tC + D\,{}^tD$$

(see (1.3)) is singular, and so, since it is symmetric and semi-definite, there is a nonzero real n-column T such that ${}^tT(C\,{}^tC + D\,{}^tD)T = 0$, whence ${}^tTC\,{}^tCT = 0$ and ${}^tTD\,{}^tDT = 0$, and so ${}^tTC ={}^t TD = 0$. The last relations imply that the rank of the matrix $(C,\, D)$ is less than n, which is impossible, since the matrix M is nonsingular.

Then, note that each matrix $Z = X + iY \in \mathbb{H}$ can be written in the form $Z = M'\langle iE\rangle$ with a matrix $M' \in \mathbb{G}$. It is sufficient to take $M' = \begin{pmatrix} A_1 & X\,{}^tA_1^{-1} \\ 0 & {}^tA_1^{-1} \end{pmatrix}$, if $Y = A_1\,{}^tA_1$.

Finally, by (1.9) with $Z = iE$, we get

$$J(MM',\, iE) = J(M,\, M'\langle iE\rangle)J(M',\, iE) = J(M,\, Z)J(M',\, iE),$$

which implies that $J(M,\, Z)$ is nonsingular. $\triangle$

Lemma 1.4. *Let* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{G}$ *and* $Z = X + iY \in \mathbb{H}$, *then the matrix* $Z' = X' + iY' = M\langle Z\rangle$ *is symmetric, and*

$$Y' = \mu(M)\, {}^t(C\overline{Z} + D)^{-1} Y (CZ + D)^{-1}. \tag{1.10}$$

In particular, $Z' \in \mathbb{H}$.

Proof. As it easily follows from the relations (1.2), the matrix

$${}^t(CZ+D)M\langle Z\rangle(CZ+D) = (Z\,{}^tC + {}^tD)(AZ+B) = Z\,{}^tCAZ + {}^tDAZ + Z\,{}^tCB + {}^tDB$$

is symmetric and so the matrix $Z' = M\langle Z\rangle$ is symmetric too.

Further, by (1.2), we have

$${}^t(C\overline{Z} + D)(Z' - \overline{Z}')(CZ + D) = (\overline{Z}\,{}^tC + {}^tD)(AZ + B) - (\overline{Z}\,{}^tA + {}^tB)(CZ + D)$$

$$= \overline{Z}({}^tCA - {}^tAC)Z + ({}^tDA - {}^tBC)Z + \overline{Z}({}^tCB - {}^tAD) = \mu(M)(Z - \overline{Z}).$$

The formula (1.10) and the lemma follow.△

Finally, we shall find an $\mathbb{G}$-invariant element of volume on $\mathbb{H}$. The upper half-plane $\mathbb{H}$ is clearly an open subset of the $n(n+1)$-dimensional real affine space, and we can consider the Euclidean element of volume on $\mathbb{H}$,

$$dZ = \prod_{1\le\alpha\le\beta\le n} dx_{\alpha\beta}dy_{\alpha\beta} \qquad (Z = (x_{\alpha\beta} + iy_{\alpha\beta}) \in \mathbb{H}). \tag{1.11}$$

Lemma 1.5. *For each matrix* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{G}$, *the element of volume* (1.11) *satisfies the relation*

$$dM\langle Z\rangle = \mu(M)^{n(n+1)}|\det(CZ + D)|^{-2n-2}dZ.$$

Proof. For $Z = (z_{\alpha\beta}) = (x_{\alpha\beta}+iy_{\alpha\beta}) \in \mathbb{H}$, we set $Z' = (z'_{\gamma\delta}) = (x'_{\gamma\delta}+iy'_{\gamma\delta}) = M\langle Z\rangle$. We have to compute the absolute value of the Jacobian of the variables $x'_{\gamma\delta}$, $y'_{\gamma\delta}$ with respect to the variables $x_{\alpha\beta}$, $y_{\alpha\beta}$. First, we shall consider the transformation of the differentials of the complex variables $z_{\alpha\beta}$. For $Z_1, Z_2 \in \mathbb{H}$, since Z'_2 is symmetric, we get

$$Z'_2 - Z'_1 = (Z_2\,{}^tC + {}^tD)^{-1}(Z_2\,{}^tA + {}^tB) - (AZ_1 + B)(CZ_1 + D)^{-1}$$

$$= \mu(M)(Z_2\,{}^tC + {}^tD)^{-1}(Z_2 - Z_1)(CZ_1 + D)^{-1},$$

where we have also used the relations (1.2). It follows that

$$\boldsymbol{D}Z' = \mu(M)(Z\,{}^tC + {}^tD)^{-1}\boldsymbol{D}Z(CZ+D)^{-1},$$

where $\boldsymbol{D}Z = (dz_{\alpha\beta})$ and $\boldsymbol{D}Z' = (dz'_{\gamma\delta})$ are the matrix of differentials of the variables $z_{\alpha\beta}$ and $z'_{\gamma\delta}$, respectively. Note that if $\rho(U)$ with $U \in GL_n(\mathbb{C})$ is the transformation $(v_{\alpha\beta}) \mapsto U(v_{\alpha\beta})\,{}^tU$ of variables $v_{\alpha\beta} = v_{\beta\alpha}$ with $1 \le \alpha, \beta \le n$, then $\det\rho(U) = (\det U)^{n+1}$. This can be easily checked by ordering the variables $v_{\alpha\beta}$ lexicographically and replacing U by an upper triangular matrix of the form $W^{-1}UW$. Let $\boldsymbol{d}Z$ and $\boldsymbol{d}Z'$ be the columns with entries $dz_{\alpha\beta}$ $(1 \le \alpha, \beta \le n)$ and $dz'_{\gamma\delta}$ $(1 \le \gamma, \le \delta \le n)$ arranged in a fixed order. Then the above considerations imply the relation

$$\boldsymbol{d}Z' = \rho(\sqrt{\mu(M)}\,{}^t(CZ+D)^{-1})\boldsymbol{d}Z.$$

Taking $\boldsymbol{d}Z = \boldsymbol{d}X + i\boldsymbol{d}Y$, $\boldsymbol{d}Z' = \boldsymbol{d}X' + i\boldsymbol{d}Y'$, and $\rho(\sqrt{\mu(M)}\,{}^t(CZ+D)^{-1}) = R + iS$, we obtain that

$$\boldsymbol{d}X' = R\boldsymbol{d}X - S\boldsymbol{d}Y, \quad \boldsymbol{d}Y' = S\boldsymbol{d}X + R\boldsymbol{d}Y.$$

Thus, the Jacobian equals

$$\det\begin{pmatrix} R & -S \\ S & R \end{pmatrix} = \det\left(\begin{pmatrix} E & iE \\ 0 & E \end{pmatrix}\begin{pmatrix} R & -S \\ S & R \end{pmatrix}\begin{pmatrix} E & -iE \\ 0 & E \end{pmatrix}\right)$$

$$= \det\begin{pmatrix} R+iS & 0 \\ 0 & R-iS \end{pmatrix} = \mu(M)^{n(n+1)}|\det(CZ+D)|^{-2n-2}.$$

$\triangle$

By combining the above lemma and formula (1.10), we get

Proposition 1.6. *The element of volume on* $\mathbb{H}$ *given by*

$$d^*Z = \det Y^{-(n+1)}dZ, \quad (Z = X + iY \in \mathbb{H}), \tag{1.12}$$

where $dZ = dXdY$ *is the Euclidean element of volume* (1.11)*, is invariant under all transformations of the group* $\mathbb{G}$*:*

$$d^*M\langle Z\rangle = d^*Z, \qquad (M \in \mathbb{G}).$$

It is easy to see that two matrices M, M' of $\mathbb{G}$ have the same action (1.6) on an open subset of $\mathbb{H}$ if and only if $M' = \lambda M$ with λ in the set $\mathbb{R}^\times$ of nonzero real numbers. It follows that the group of all transformations of the upper half-plane of the form (1.6) is isomorphic to the factor groups

$$\mathbb{G}/\{\mathbb{R}^\times 1_{2n}\} \simeq \mathbb{S}/\{\pm 1_{2n}\},$$

where

$$\mathbb{S} = \mathbb{S}^n = Sp_n(\mathbb{R}) = \left\{ M \in \mathbb{G}^n \;\middle|\; \mu(M) = 1 \right\} \tag{1.13}$$

is the (*real*) *symplectic group of genus* n. We have already seen in the proof of Lemma 1.3 that each matrix $Z \in \mathbb{H}$ can be written in the form $Z = M\langle iE\rangle$ with a matrix $M \in \mathbb{S}$. Therefore, the upper half-plane can be identified with the homogeneous space of the symplectic group by the stabilizer $\mathbb{U}$ of the point iE in $\mathbb{S}$. More precisely, we have the following lemma:

Lemma 1.7. *The map $M \mapsto M\langle iE\rangle$ defines one-to-one correspondence $\mathbb{S}/\mathbb{U} \leftrightarrow \mathbb{H}$, which is compatible with the actions of the group $\mathbb{S}$, where on the left side it acts by multiplication from the left; the stabilizer $\mathbb{U}$ has the form*

$$\mathbb{U} = \mathbb{U}^n = \left\{ \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \in \mathbb{S}^n \right\};$$

the map $\begin{pmatrix} A & B \\ -B & A \end{pmatrix} \mapsto A + iB$ is an isomorphism of $\mathbb{U}$ onto the unitary group of order n; in particular, the group $\mathbb{U}$ is compact.

Exercise 1.8. *Prove the lemma and preceding assertions.*

Exercise 1.9. *Show that the Cayley mapping*

$$Z \mapsto W = (Z - iE)(Z + iE)^{-1}, \qquad (Z \in \mathbb{H}),$$

is an analytical isomorphism of $\mathbb{H}$ onto the bounded domain

$$\left\{ W \in \mathbb{C}_n^n \;\middle|\; {}^tW = W, \quad \overline{W}W < E \right\},$$

where the inequality is understood in the sense of Hermitian matrices. Show that the inverse mapping is given by

$$W \mapsto Z = i(E + W)(E - W)^{-1}.$$

§1.2 Fundamental domains for modular group and related groups.

The *modular* (*symplectic*) *group* or the *Siegel modular group of genus* n, i.e. the group of all integral symplectic matrices of order $2n$ with unit multiplier,

$$\Gamma = \Gamma^n = Sp_n(\mathbb{Z}) = \mathbb{S}^n \bigcap \mathbb{Z}_{2n}^{2n}, \tag{1.14}$$

is clearly a discrete subgroup of the symplectic group $\mathbb{S}$. The same is true for each subgroup S of $\mathbb{S}$ *commensurable with the group* Γ, i.e. such that the intersection $S \cap \Gamma$ is of finite index both in S and Γ. The lemma 1.7 implies then that each such group S discretely acts on the upper half-plane.

Automorphic forms for subgroups S of the symplectic group, which we are going to consider in this chapter, are functions on the upper half-plane with certain analytical properties satisfying functional equations, which connect its values at points of each S-*orbit*

$$S\langle Z\rangle = \left\{ M\langle Z\rangle \;\middle|\; M \in S \right\}, \qquad (Z \in \mathbb{H})$$

on $\mathbb{H}$, so that such a function is uniquely determined by its restriction to any subset of $\mathbb{H}$, which meets each S-orbit.

We shall remind that a closed subset $\mathbf{D}$ of a topological space $\mathbf{X}$ is called a *fundamental domain* for a discrete transformation group G acting on $\mathbf{X}$, if it meets each of the G-orbits $G(x) = \{g(x) | g \in G\}$ with $x \in \mathbf{X}$ and has no distinct inner points belonging to the same orbit. It follows from the definition that the decomposition

$$\mathbf{X} = \bigcup_{g \in G/G'} g(\mathbf{D}) \quad \text{with } G' = \{g \in G | g(x) = x, \forall x \in X\} \tag{1.15}$$

holds, and its components have pairwise no common inner points. Fundamenal domains are not necessarily exist.

The construction of fundamental domains for modular symplectic group is essentially based on the *Minkowski reduction theory of positive definite quadratic forms*. In the matrix language the problem of reduction of positive definite quadratic forms relative to unimodular equivalence is that of construction of a fundamental domain for the *unimodular group*

$$\Lambda = \Lambda^n = GL_n(\mathbb{Z}) \tag{1.16}$$

acting on the cone

$$\boldsymbol{P} = \boldsymbol{P}_n = \left\{ Y \in \mathbb{R}^n_n \;\middle|\; {}^tY = Y,\, Y > 0 \right\}, \tag{1.17}$$

of real positive definite matrices of order n by

$$\Lambda \ni V \;:\quad Y \mapsto Y[V] = {}^tVYV.$$

The columns of a matrix $U \in \Lambda$ will be denoted by $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$, so that $U = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$. In order to choose a special representative $Y[U]$ of the *orbit*

$$\Lambda(Y) = \left\{ Y[V] \;\middle|\; V \in \Lambda \right\}$$

of a point $Y \in \boldsymbol{P}$, we determine the matrix U column by column with help of some minimal conditions. Let

$$\Lambda_r = \Lambda_r^n = \left\{ (\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) \in \mathbb{Z}_r^n \;\middle|\; (\boldsymbol{u}_1, \dots, \boldsymbol{u}_r, *, \dots, *) \in \Lambda \right\}$$

be the set of all integral $n \times r$-matrices composed of the first r columns of matrices in Λ. For a given $Y \in \boldsymbol{P}$, we choose $\boldsymbol{u}_1 \in \Lambda_1$ so that the value $Y[\boldsymbol{u}_1] = {}^t\boldsymbol{u}_1 Y \boldsymbol{u}_1$ of the quadratic form with the matrix Y on the column $\boldsymbol{u}_1$ is minimal; this can be done, since the form is positive definite. Next, we determine $\boldsymbol{u}_2$ so that $(\boldsymbol{u}_1, \boldsymbol{u}_2) \in \Lambda_2$ and the value $Y[\boldsymbol{u}_2]$ is minimal. On replacing $\boldsymbol{u}_2$ by $-\boldsymbol{u}_2$, if necessary, one may assume that ${}^t\boldsymbol{u}_1 Y \boldsymbol{u}_2 \geq 0$. Proceeding in the same way, at the r-th step we choose $\boldsymbol{u}_r$ so that $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) \in \Lambda_r$, $Y[\boldsymbol{u}_r]$ is minimal, and ${}^t\boldsymbol{u}_{r-1} Y \boldsymbol{u}_r \geq 0$. Finally, when $r = n$, we get an unimodular matrix $U = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) \in \Lambda$ and a matrix $T = (t_{\alpha\beta}) = Y[U] \in \Lambda(Y)$, which is called *Minkowski reduced*, or just *reduced*.

Let us determine the conditions for a positive definite matrix to be reduced in the terms of its entries. First of all, by induction on n based on Euclidean algorithm, one can easily prove the following

Lemma 1.10. *An integral n-column $\boldsymbol{u}$ belongs to Λ_1 if and only if its entries are coprime.*

Also, as an easy exercise on multiplication of block matrices, we get

Lemma 1.11. *Two matrices U, U' of Λ^n have the same first r columns if and only if*

$$U' = U \begin{pmatrix} E_r & B \\ 0 & D \end{pmatrix} \qquad \text{with } D \in \Lambda^{n-r} \text{ and } b \in \mathbb{Z}_r^{n-r}.$$

Let $U = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) \in \Lambda^n$. By Lemma 1.11, the set of all r-th columns of all matrices $U' \in \Lambda^n$ with the first columns $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{r-1}$ coincides with the set of the columns of the form $U\boldsymbol{v}$, where $\boldsymbol{v}$ is an integral n-column, whose last $n - r + 1$ entries $v_r, \dots, v_n$ form the first column of a matrix $D \in \Lambda^{n-r+1}$. By Lemma 1.10, the last condition means that the numbers $v_r, \dots, v_n$ are coprime. Thus, if $U = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) \in \Lambda^n$ and $1 \leq r \leq n$, then

$$\left\{ \boldsymbol{u} \in \mathbb{Z}^n \;\middle|\; (\boldsymbol{u}_1, \dots, \boldsymbol{u}_{r-1}, \boldsymbol{u}) \in \Lambda_r^n \right\} = U\boldsymbol{V}_{r,n}, \tag{1.18}$$

where

$$\boldsymbol{V}_{r,n} = \left\{ \boldsymbol{v} =^t (v_1, \dots, v_n) \in \mathbb{Z}^n \;\middle|\; \gcd(v_r, \dots, v_n) = 1 \right\}.$$

By the definition and (1.18), we conclude that a matrix $T = (t_{\alpha\beta}) = Y[U]$ is reduced if and only if it satisfies the conditions

$$Y[U\boldsymbol{v}] \geq Y[\boldsymbol{u}_r], \quad \text{for all } \boldsymbol{v} \in \boldsymbol{V}_{r,n} \text{ and } 1 \leq r \leq n,$$

and

$$ {}^t\boldsymbol{u}_{r-1} Y \boldsymbol{u}_r \geq 0, \quad \text{for } 1 < r \leq n, $$

where $U = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$. Since $Y[U] = T = (t_{\alpha\beta})$, we have $Y[\boldsymbol{u}_r] = t_{rr}$ and ${}^t\boldsymbol{u}_{r-1} Y \boldsymbol{u}_r = t_{r-1,r}$. Hence, the above conditions means exactly that T belongs to the set

$$ (1.19) \quad \boldsymbol{M} = \boldsymbol{M}_n = \{T = (t_{\alpha\beta}) \in \boldsymbol{P}_n \;\Big|\; t_{rr} \leq T[\boldsymbol{v}] \,\forall \boldsymbol{v} \in \boldsymbol{V}_{r,n}\, (1 \leq r \leq n); \quad t_{r-1,r} \geq 0\, (1 < r \leq n)\}, $$

called the *Minkowski reduction domain.*

Theorem 1.12. *Every orbit $\Lambda(Y)$ of the group Λ on $\boldsymbol{P}$ contains at least one and not more than finitely many points of the Minkowski domain $\boldsymbol{M}$. If T, T' are two inner points of $\boldsymbol{M}$, and $T' = T[U]$ with $U \in \Lambda$, then $U = \pm E$; in particular, no different inner points of $\boldsymbol{M}$ belong to the same orbit. In other words, $\boldsymbol{M}$ is a fundamental domain of Λ on $\boldsymbol{P}$.*

Proof. The above consideration shows that, for a given $Y \in \boldsymbol{P}$, there exists $U \in \Lambda$ such that $Y[U] \in \boldsymbol{M}$, and every column of such U can be chosen in finitely many ways.

Let us set

$$ \boldsymbol{M}' = \boldsymbol{M}'_n = \{T \in \boldsymbol{P}_n \;\Big|\; t_{rr} < T[\boldsymbol{v}],\, \boldsymbol{v} \in \boldsymbol{V}_{r,n},\, \boldsymbol{v} \neq \pm \boldsymbol{e}_r\, (1 \leq r \leq n); \quad t_{r-1,r} > 0\, (1 < r \leq n)\}, $$

where $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ are the columns of the unit matrix $E = E_n$. It is clear that $\boldsymbol{M}' \in \boldsymbol{M}$ and each inner point of $\boldsymbol{M}$ is contained in $\boldsymbol{M}'$. If $T = (t_{\alpha\beta})$ and $T' = (t'_{\alpha\beta})$ belong to $\boldsymbol{M}'$ and $T' = T[U]$ with $U = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) \in \Lambda$, then $\boldsymbol{u}_1 \in \boldsymbol{V}_{1,\,n}$, whence $t'_{11} = T[\boldsymbol{u}_1] \geq t_{11}$ and, similarly, $t_{11} \geq t'_{11}$. It follows that $t_{11} = t'_{11} = T[\boldsymbol{u}_1]$ and so $\boldsymbol{u}_1 = \pm \boldsymbol{e}_1$. Then $\boldsymbol{u}_2 \in \boldsymbol{V}_{2,\,n}$, and in the same way we conclude that $\boldsymbol{u}_2 = \pm \boldsymbol{e}_2$. By repeating the same arguments, we see that $\boldsymbol{u}_r = \pm \boldsymbol{e}_r$ for all $r = 1, \ldots, n$. Now the conditions

$$ t_{r-1,\,r} > 0, \quad t'_{r-1,\,r} = {}^t\boldsymbol{u}_{r-1} T \boldsymbol{u}_r > 0 \quad (1 < r \leq n) $$

imply that $\boldsymbol{u}_r = \boldsymbol{e}_r$ or $\boldsymbol{u}_r = -\boldsymbol{e}_r$ for $r = 1, \ldots, n$, and $T = T'$. △

The entries of reduced matrices $T = (t_{\alpha\beta})$ satisfy some useful inequalities. First of all, since $t_{rr} \leq T[\boldsymbol{e}_{r+1}] = t_{r+1,r+1}$, it follows that

$$ (1.20) \qquad t_{11} \leq t_{22} \leq \ldots \leq t_{nn}. $$

Then, by $t_{ll} \leq T[\boldsymbol{e}_r \pm \boldsymbol{e}_l] = t_{rr} \pm 2t_{rl} + t_{ll}$, where $1 \leq r < l \leq n$, we obtain

$$ (1.21) \qquad |2t_{rl}| \leq t_{rr}, \qquad \text{if } r \neq l. $$

Finally, Minkowski have proved a deeper inequality for reduced matrices, which we cite without proof (for the proof see, for example, *Sources*):

$$t_{11}t_{22}\dots t_{nn} \le c_n \det T, \qquad (T = (t_{\alpha\beta}) \in \boldsymbol{M}_n), \tag{1.22}$$

where c_n is a positive constant depending only on n. The Minkowski inequality imply that every $T = (t_{\alpha\beta}) \in \boldsymbol{M}_n$ satisfies the inequality

$$T \ge \frac{1}{n^{n-1}c_n} diag(t_{11}, t_{22}, \dots, t_{nn}). \tag{1.23}$$

Really, let $\rho_1, \dots, \rho_n$ be the characteristic values of the matrix

$$T' = T[diag(t_{11}^{-1/2}, t_{22}^{-1/2}, \dots, t_{nn}^{-1/2})],$$

then $\rho_1 + \ldots + \rho_n = n$ and, by (1.22),

$$\rho_1 \dots \rho_n = (t_{11}t_{22}\dots t_{nn})^{-1} \det T \ge 1/c_n;$$

it follows that $\rho_\alpha \le n$ and $\rho_\alpha \ge 1/n^{n-1}c_n$ for $\alpha = 1, \dots, n$, which implies (1.23).

Exercise 1.13. *Show that*

$$\boldsymbol{M}_2 = \left\{ \begin{pmatrix} t_{11} & t_{12} \\ t_{12} & t_{22} \end{pmatrix} \in \boldsymbol{P}_2 \;\middle|\; 0 \le 2t_{12} \le t_{11} \le t_{22} \right\};$$

Show that in the inequalities (1.22) *one can take* $c_1 = 1$ *and* $c_2 = 4/3$, *and the values are minimal.*

[Hint: For minimality of c_2, consider $T = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}$].

Exercise 1.14. *Two binary quadratic forms* $f(x, y)$ *and* $f‘(x, y)$ *are said to be equivalent if* $f'(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$ *with* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Lambda^2$. *Show that the number of classes of equivalent positive definite quadratic forms* $f(x, y) = ax^2 + bxy + cy^2$ *with integral coefficients* a, b, c *and a fixed discriminant* $d = b^2 - 4ac$ *is finite.*

Let us come back to the action of the modular group (1.14) on the upper half-plane. We consider orbits $\Gamma\langle Z\rangle$ of the modular group on $\mathbb{H}$. For $Z = X + iY \in \mathbb{H} = \mathbb{H}^n$, we shall call the positive real number $\det Y$ the *height* of the point Z and denote it by $h(Z)$. By (1.10), we have

$$h(M\langle Z\rangle) = |\det(CZ + D)|^{-2} h(Z), \qquad \left(Z \in \mathbb{H},\, M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma\right). \tag{1.24}$$

Lemma 1.15. *Each orbit of the group Γ on $\mathbb{H}$ contains points Z of maximal height. The points can be characterized by the inequalities*

$$|\det(CZ+D)| \geq 1 \qquad \textit{for every } \begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \Gamma.$$

Proof. In view of (1.24) we have to show that $|\det(CZ+D)|$ assumes a minimum on each orbit. Note that, for any $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma$ and $V \in \Lambda = \Lambda^n$, the product

$$\begin{pmatrix} {}^tV^{-1} & 0 \\ 0 & V \end{pmatrix} M = \begin{pmatrix} {}^tV^{-1}A & {}^tV^{-1}B \\ VC & VD \end{pmatrix}$$

also belongs to Γ. It follows that if $(C,\,D)$ is the "second row" of a matrix of Λ, then so is $(VC,\,VD)$. Replacing of M in

$$M\langle X+iY\rangle = X'+iY'$$

by the above product does not change the value $|\det(CZ+B)|$ and replaces the matrix $(Y')^{-1}$ by the matrix ${}^tV(Y')^{-1}V$. Therefore, we may assume that the positive definite matrix $(Y')^{-1}$ is Minkowski reduced.

Let us denote by $\boldsymbol{c}_r$ and $\boldsymbol{d}_r$ $(r=1,\dots,n)$ the columns of the matrices ${}^tC$ and $X\,{}^tC + {}^tD$, respectively, and by $t_1,\dots,t_n$ the diagonal elements of $(Y')^{-1}$. Then, by (1.10), we can write

$$(Y')^{-1} = (CZ+D)Y^{-1}(\overline{Z}\,{}^tC + {}^tD) = (CX+D)Y^{-1}(X\,{}^tC + {}^tD) + CY\,{}^tC,$$

whence, for $r=1,\dots,n$, we get

$$t_r = Y^{-1}[\boldsymbol{d}_r] + Y[\boldsymbol{c}_r] \geq \begin{cases} Y[\boldsymbol{c}_r] \\ Y^{-1}[\boldsymbol{d}_r]. \end{cases} \tag{1.25}$$

If, for some r, the columns $\boldsymbol{c}_r$ and $\boldsymbol{d}_r$ are both zero, then the r-th column of the matrix $(C\,D)$ is also zero, which is impossible, since M is nonsingular. Since $Y>0$, the value $Y[\boldsymbol{c}_r]$ assumes a positive minimum when Z is fixed and $\boldsymbol{c}_r$ is arbitrary nonzero integral column. On the other hand, if $\boldsymbol{c}_r = 0$, then $\boldsymbol{d}_r$ is the r-th column of ${}^tD$ and so is a nonzero integral column. Since $Y^{-1}>0$, the value $Y^{-1}[\boldsymbol{d}_r]$ also assumes a positive minimum. It follows then from (1.25) that the numbers $u_1,\dots,u_n$ have a positive lower bound independent of M. The relations (1.22) and (1.24) imply the inequality

$$t_1t_2\dots t_n \leq c_n(\det Y')^{-1} = c_n(\det Y)^{-1}|\det(CZ+D)|^2.$$

If we now assume that a condition $|\det(CZ+D)| \leq h$ is satisfied for an arbitrary large number h, then it implies upper bounds for $t_1,t_2,\dots,t_n$. Then from (1.25) we obtain upper bounds for entries of the columns $\boldsymbol{c}_r$ and $\boldsymbol{d}_r$ and hence for the entries of the matrices C and D. Therefore, the condition is satisfied only for finitely many pairs $(C,\,D)$ if Z is fixed and h is a given large number. This proves the lemma.$\triangle$

Theorem 1.16. *Let $\boldsymbol{D} = \boldsymbol{D}_n$ be the subset of matrices $Z = X + iY \in \mathbb{H}_n$ satisfying the following conditions:*

(1). $|\det(CZ + D)| \geq 1$ for every $\begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \Gamma = \Gamma^n$;

(2). $Y \in \boldsymbol{M}_n$, where $\boldsymbol{M}_n$ is the Minkowski reduction domain (1.19);

(3). $X \in \boldsymbol{X}_n = \left\{ X = (x_{\alpha\beta}) \in \mathbb{R}^n_n) \;\middle|\; {}^tX = X, \quad |x_{\alpha\beta}| \leq 1/2\,(1 \leq \alpha, \beta \leq n) \right\}$.

Then $\boldsymbol{D}$ meets each Λ-orbit on $\mathbb{H}$, and $Z' = M\langle Z\rangle$ for two inner points Z, $Z' \in \boldsymbol{D}$ with $M \in \Gamma$ if and only if $M = \pm E$, i.e. $\boldsymbol{D}$ is a fundamental domain of Γ on $\mathbb{H}$.

If $Z = X = iY \in \boldsymbol{D}$, then

$$Y \geq b_n E \quad \text{and} \quad \sigma(Y^{-1}) \leq n/b_n, \tag{1.26}$$

where b_n is a positive constant depending only on n.

The volume of $\boldsymbol{D}$ with respect to the invariant element of volume (1.12) is finite.

Proof. Let us consider the orbit $\Gamma\langle Z''\rangle$ of a point $Z'' \in \mathbb{H}$. By Lemma 1.15, the orbit contains a point $Z' = X' + iY'$ of maximal height, and the point satisfies the condition (1). Every transformation of the form

$$Z' \mapsto \begin{pmatrix} {}^tV & SV^{-1} \\ 0 & V^{-1} \end{pmatrix} = {}^tV Z' V + S = X'[V] + S + iY'[V]$$

with $V \in \Lambda = \Lambda^n$ and $S \in \boldsymbol{S}^n(\mathbb{Z})$ corresponds to a matrix of Γ and does not change the height of Z'. By Theorem 1.12, there is a matrix $V \in \Lambda$ such that the matrix $Y = Y'[V]$ belongs to $\boldsymbol{M}_n$. Also, clearly, there is $S \in \boldsymbol{S}^n(\mathbb{Z})$ such that $X'[V] + S \in \boldsymbol{X}_n$. Then

$$Z = X + iY \in \Gamma\langle Z'\rangle \bigcap \boldsymbol{D}.$$

Suppose now that $Z' = M\langle Z\rangle$ for two points Z, $Z' \in \boldsymbol{D}$ with $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma$. Then $h(Z') = h(Z)$, by Lemma 1.15. It follows from (1.24) that $|\det(CZ+D)| = 1$. On the other hand, since $Z = M^{-1}\langle Z'\rangle$, we conclude that $|\det(-{}^tCZ' + {}^tA)| = 1$ (see (1.1)). If $C \neq 0$, then the equations are nontrivial, and so the points Z, Z' belong to the boundary of D. If $C = 0$, then M has the form

$$M = \begin{pmatrix} {}^tV & SV^{-1} \\ 0 & V^{-1} \end{pmatrix} \qquad \text{with } V \in \Lambda \text{ and } S = {}^tS \in \mathbb{Z}^n_n.$$

So we have

$$Z' = X' + iY' = X[V] + S + iY[V], \qquad \text{where} \quad X + iY = Z,$$

in particular, $Y' = Y[V]$. Since Y and Y' are both in $\boldsymbol{M}_n$, it follows from Theorem 1.12 that Y and Y' are boundary points of $\boldsymbol{M}_n$ or $V = \pm E$. In the last case we have $X' = X + S$, whence $S = 0$, unless X and X' belong to the boundary of $\boldsymbol{X}_n$. We conclude that $M = \pm 1_{2n}$, unless Z and Z' are boundary points of $\boldsymbol{D}$.

Let $Z = (z_{\alpha\beta}) = (x_{\alpha\beta} + iy_{\alpha\beta}) \in \boldsymbol{D}$. the inequality $|\det(CZ + D)| \geq 1$ for the pair

$$(C,\, D) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1_{n-1} \end{pmatrix} \right)$$

implies the inequality $|z_{11}| = \sqrt{x_{11}^2 + y_{11}^2} \geq 1$. Since $|x_{11}| \leq 1/2$, it follows that $y_{11}^2 \geq 3/4$, i.e. $y_{11} \geq \sqrt{3}/2$. The last inequality and the inequalities (1.20) imply that $y_{\alpha\alpha} \geq \sqrt{3}/2$ for $\alpha = 1, \ldots, n$. The first inequality of (1.26) follows then from (1.23) with $b_n = \sqrt{3}/2n^{n-1}c_n$. The inequality implies that each characteristic value of Y^{-1} not greater than $1/b$, which proves the second inequality.

Finally, by (1.12), Theorem 1.16, and (1.26) we have

$$v(\boldsymbol{D}_n) = \int_{\boldsymbol{D}_n} (\det Y)^{-n-1} d(\det Y)^{-n-1} dY x dY \leq \int_{Y \in \boldsymbol{M}_n, Y \geq b_n E} (\det Y)^{-n-1} dY,$$

which, by (1.20), (1.21), and (1.22), can be estimated as

$$\leq \int_{\substack{b_n \leq y_{11} \leq y_{22} \leq \ldots \leq y_{nn}; \\ |2y_{\alpha\beta}| \leq y_{\alpha\alpha}\ (\alpha \neq \beta)}} (c_n^{-1} y_{11} y_{22} \ldots y_{nn})^{-n-1} dY$$

$$\leq \int_{y_{11}, y_{22}, \ldots, y_{nn} \geq b_n} (c_n^{-1} y_{11} y_{22} \ldots y_{nn})^{-n-1} \left(\prod_{\alpha=1}^{n} y_{\alpha\alpha}^{n-\alpha} \right) dy_{11} dy_{22} \ldots dy_{nn}$$

$$= c' \prod_{\alpha=1}^{n} \int_{c_n}^{\infty} y^{-\alpha-1} dy_{\alpha\alpha} < \infty.$$

△

Exercise 1.17. *Prove that $\boldsymbol{D}_1$ is the so-called modular triangle,*

$$\boldsymbol{D}_1 = \left\{ z = x + iy \in \mathbb{H} \;\middle|\; |x| \leq \frac{1}{2},\, |z| = x^2 + y^2 \geq 1 \right\},$$

and one can take $b_1 = \frac{\sqrt{3}}{2}$. Draw the modular triangle.

Exercise 1.18. *Two binary quadratic forms*

$$Q(x,y) = q_{11}x^2 + q_{12}xy + q_{22}y^2 \text{ and } Q'(x,y) = q'_{11}x^2 + q'_{12}xy + q'_{22}y^2$$

are said to be properly equivalent (over $\mathbb{Z}$) if

$$Q'(x,y) = Q(ax+by,\, cx+dy) \qquad \text{with} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^1 = SL_2(\mathbb{Z}). \tag{1.27}$$

Show that any real positive definite quadratic form Q is properly equivalent to a form Q', whose coefficients satisfy the inequalities $|q'_{12}| \le q'_{11} \le q'_{22}$. Show that the cone given by the inequalities in the space of the coefficients of the form contains no distinct inner points corresponding to properly equivalent forms

[Hint: Let ω and ω' are the roots belonging to $\mathbb{H}$ of the equations $Q(x,\,1) = 0$ and $Q'(x,\,1) = 0$, respectively. Show that (1.26) is equivalent with the conditions

$$(q'_{12})^2 - 4q'_{11}q'_{22} = (q_{12})^2 - 4q_{11}q_{22} \quad \text{and} \quad \omega' = M^{-1}\langle\omega\rangle \quad \text{with} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda;$$

then use Theorem 1.16 and Exercise 1.17.]

Theorem 1.19. *Each subgroup of the symplectic group $\mathbb{S} = \mathbb{S}^n$ of the form $S_M = M^{-1}SM$, where S is a subgroup of finite index in the modular group $\Gamma = \Gamma^n$, and M belongs to the general symplectic group $\mathbb{G} = \mathbb{G}^n$, has a fundamental domain $\boldsymbol{D}(S_M)$ on $\mathbb{H} = \mathbb{H}^n$, and one can take*

$$\boldsymbol{D}(S_M) = \bigcup_{M_\alpha \in (-1_{2n})S \cup S \backslash \Gamma} (M^{-1}M_\alpha)\langle \boldsymbol{D}\rangle, \tag{1.28}$$

where $\boldsymbol{D} = \boldsymbol{D}(\Gamma)$ is a fundamental domain of Γ, and M_α ranges over a system of representatives of different left cosets of Γ modulo the subgroup $(-1_{2n})S \cup S$.

The invariant volume of the fundamental domain is finite.

Proof. First of all, the set (1.28) is closed, as a finite union of closed subsets. Next, if $M^{-1}M_\alpha\langle Z\rangle$ and $M^{-1}M_\alpha\langle Z'\rangle$ are two inner points of the set belonging to the same orbit of S_M, i.e.

$$(M^{-1}M_\alpha)\langle Z\rangle = (M^{-1}NM)\langle (M^{-1}M_\beta)\langle Z'\rangle\rangle = (M^{-1}NM_\beta)\langle Z'\rangle \quad (N \in S),$$

one can assume that Z, and Z' are inner points of $\boldsymbol{D}$. Then, by (1.7), $M_\alpha\langle Z\rangle = (NM_\beta)\langle Z'\rangle$, and so $Z = Z'$, and $M_\alpha = \pm NM_\beta$, by the definition of $\boldsymbol{D}$, which implies that $\alpha = \beta$ and $N = \pm 1_{2n}$. Finally, since $\boldsymbol{D}$ meets each Γ-orbit, we have

$$\mathbb{H} = \bigcup_{N \in \Gamma/\{\pm 1_{2n}\}} N\langle \boldsymbol{D}\rangle = \bigcup_{N \in (-1_{2n}S)\cup S/\{\pm 1_{2n}\}} \; \bigcup_{M_\alpha \in (-1_{2n}S)\cup S\backslash\Gamma} (NM_\alpha)\langle \boldsymbol{D}\rangle,$$

whence

$$\mathbb{H} = M^{-1}\langle\mathbb{H}\rangle = \bigcup_{N\in(-1_{2n}S)\cup S/\{\pm 1_{2n}\}} \bigcup_{M_\alpha\in(-1_{2n}S)\cup S\backslash\Gamma} ((M^{-1}NM)M^{-1}M_\alpha)\langle\boldsymbol{D}\rangle.$$

The decomposition (1.14) follows, whence the set $\boldsymbol{D}(S_M)$ meets each S_M-orbit.

Let us take $\boldsymbol{D}(S')$ in the form (1.17) . Then we get

$$\begin{aligned} v(\boldsymbol{D}(S_M)) = \int_{\boldsymbol{D}(S_M)} d^*Z &= \sum_{M_\alpha\in(-1_{2n})S\cup S\backslash\Gamma} \int_{(M^{-1}M_\alpha)\langle\boldsymbol{D}\rangle} d^*Z \\ &= \sum_{M_\alpha\in(-1_{2n})S\cup S\backslash\Gamma} \int_{\boldsymbol{D}} d^*Z = [\Gamma : (-1_{2n})S\cup S]\; v(\boldsymbol{D}) < \infty, \end{aligned}$$

by the last part of Theorem 1.16. $\triangle$

§1.3. Modular forms.

Acting on the upper half-plane $\mathbb{H} = \mathbb{H}^n$, the general symplectic group $\mathbb{G} = \mathbb{G}^n$ operates also on complex-valued functions F on $\mathbb{H}$ by *Petersson operators of integral weights* k,

$$\mathbb{G} \ni M : F \mapsto F|_k M = \mu(M)^{nk-\frac{n(n+1)}{2}} j(M,\, Z)^{-k} F(M\,\langle Z\rangle), \tag{1.29}$$

where

$$j(M,\, Z) = \det J(M,\, Z), \tag{1.30}$$

and the matrix $J(M,\, Z)$ was defined by (1.8). It follows from (1.7) and (1.9) that the Petersson operators satisfy the rules

$$\begin{aligned} F|_k MM' &= (\mu(M)\mu(M'))^{nk-\frac{n(n+1)}{2}} (j(M,\, M'\langle Z\rangle)j(M',\, Z))^{-k} F(M\langle M'\langle Z\rangle\rangle) \\ &= \mu(M')^{nk-\frac{n(n+1)}{2}} j(M',\, Z)^{-k} (F|_k M)(M'\langle Z\rangle) \\ &= (F|_k M)|_k M' \qquad (M, M' \in G^n). \end{aligned} \tag{1.31}$$

Let S be a subgroup of $\mathbb{G}$ commensurable with the modular group $\Gamma = \Gamma^n$, χ a *character* of S, that is a multiplicative homomorphism of S into nonzero complex numbers with the kernel of finite index in S, and k an integral number. A complex-valued function F on $\mathbb{H}$ is called a (*Siegel*) *modular form of weight* k *and character* χ *for the group* S, if the following conditions are satisfied:

(i) F is a holomorphic function in $n(n+1)/2$ complex variables on $\mathbb{H}$;

(ii) For every matrix $M \in S$, the function F satisfies the functional equation

$$F|_k M = \chi(M)F, \tag{1.32}$$

where $|_k$ is the Petersson operator of weight k;

(iii) If $n = 1$, then every function $F|_k M$ with $M \in \Gamma^1$ is bounded on each subset of $\mathbb{H}^1$ of the form $\mathbb{H}^1_\varepsilon = \{x + iy \in \mathbb{H}^1 | y \geq \varepsilon\}$ with $\varepsilon > 0$.

The set $\mathfrak{M}_k(S, \chi)$ of all modular forms of weight k and character χ for the group S is clearly a linear space over the field $\mathbb{C}$.

For $q \in \mathbb{N}$, we shall denote by

$$\Gamma(q) = \Gamma^n(q) = \left\{ M \in \Gamma^n \;\middle|\; M \equiv 1_{2n} \pmod{q} \right\} \tag{1.33}$$

the *principal congruence subgroup of level* q of the modular group. Considering matrices of Γ modulo q, we get a homomorphism of the modular group into the finite group of symplectic matrices of order $2n$ over the residue ring $\mathbb{Z}/q\mathbb{Z}$. It follows that $\Gamma(q)$ is a normal subgroup of finite index of the modular group.

A subgroup S of the symplectic group $\mathbb{S}$, defined by (1.13), is called a *congruence subgroup* if it contains a principal congruence subgroup as a subgroup of finite index. A character of such S is said to be a *congruence character* if it is trivial on a principal congruence subgroup contained in S. The following lemma is an easy consequence of the definitions.

Lemma 1.20. *Let S be a congruence subgroup of $\mathbb{S}$, χ a congruence character of S, and $M \in \mathbb{G} \cap \mathbb{Q}^{2n}_{2n}$ a matrix of $\mathbb{G}$ with rational entries, then the group $M^{-1}SM$ is again a congruence subgroup of $\mathbb{S}$, and the character*

$$M^{-1}SM \ni M' \mapsto \chi_M(M') = \chi(MM'M^{-1}) \tag{1.34}$$

is a congruence character of the group.

Theorem 1.21. *Let S be a congruence subgroup of $\mathbb{S}$, and χ a congruence character of S. Then each modular form $F \in \mathfrak{M}_k(S, \chi)$ has an expansion of the form*

$$F(Z) = \sum_{A \in \mathbb{E}^n,\, A \geq 0} f(A) e^{\frac{\pi i}{q}\sigma(AZ)}, \tag{1.35}$$

with constant coefficients $f(A)$, where

$$\mathbb{E}^n = \left\{ A = (a_{\alpha\beta}) \in \mathbb{Z}^n_n \;\middle|\; {}^tA = A, \quad a_{11}, a_{22}, \ldots, a_{nn} \in 2\mathbb{Z} \right\}$$

is the set of "even" matrices of order n, σ *denotes the trace, and where* $q = q(S, \chi)$ *is such positive integer that the group* S *contains a subgroup of the form*

$$T_q = \left\{ \begin{pmatrix} E & qB \\ 0 & E \end{pmatrix} \,\middle|\, B = {}^tB \in \mathbb{Z}_n^n \right\}. \tag{1.36}$$

The series (1.35) *converges absolutely on* $\mathbb{H}$ *and uniformly on each subset of* $\mathbb{H}$ *of the form*

$$\mathbb{H}_\varepsilon = \mathbb{H}_\varepsilon^n = \left\{ X + iY \in \mathbb{H}^n \,\middle|\, Y \geq \varepsilon 1_{2n} \right\} \qquad \textit{with} \quad \varepsilon > 0; \tag{1.37}$$

in particular, F *is bounded on each of the subset.*

The coefficients $f(A)$ *satisfy the relations*

$$f({}^tVAV) = (\det V)^k \chi(M) e^{-\frac{\pi i}{q}\sigma(AVU)} f(A), \qquad (\forall\, A \in \mathbb{E}^n), \tag{1.38}$$

for every matrix M *of the group* S *of the form*

$$M = M(U, V) = \begin{pmatrix} V^{-1} & U \\ 0 & {}^tV \end{pmatrix} \tag{1.39}$$

The expansion (1.35) is called the *Fourier expansion of* F, and the numbers $f(A)$ with $A \in \mathbb{E}^n$, $A \geq 0$ are the *Fourier coefficients* of F.

Proof. The functional equations (1.32) for matrices of the subgroup $T_q \subset S$ turns into

$$F(Z + qB) = F(Z), \qquad (Z = (z_{\alpha\beta}) \in \mathbb{H},\, B = {}^tB \in \mathbb{Z}_n^n).$$

This means that F is periodic of period q in each of the variables $z_{\alpha\beta} = z_{\beta\alpha}$. Since F is also holomorphic, it can be expanded in a Fourier series of the form

$$F(Z) = \sum_{\widetilde{A}} f'(\widetilde{A};\, Y) \exp\left(\frac{2\pi i}{q} \sum_{1 \leq \alpha < \beta \leq n} a_{\alpha\beta} x_{\alpha\beta} \right),$$

where $Z = X + iY$ with $X = (x_{\alpha\beta})$, and $\widetilde{A}$ ranges over the set of all upper triangular matrices of order n with integral entries $a_{\alpha\beta}$, and the series can be differentiated with respect to all variables. The expansion can be rewritten in the form

$$F(Z) = \sum_{A \in \mathbb{E}} f(A;\, Y) e^{\frac{\pi i}{q}\sigma(AZ)},$$

where $A = \widetilde{A} + {}^t\widetilde{A}$ runs through the set $\mathbb{E} = \mathbb{E}^n$ of all even matrices of order n, and where $f(A; Y) = f'(\widetilde{A}; Y) \exp\left(-\frac{\pi}{q}\sigma(AY)\right)$. Since $F(Z)$ is holomorphic in each of the variables $z_{\alpha\beta}$, it satisfies the Cauchy-Riemann equations with respect to $z_{\alpha\beta}$, that is

$$\frac{\partial F}{\partial \bar{z}_{\alpha\beta}} = 0, \quad \text{where } \frac{\partial}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right).$$

Since the last sum can be differentiated term by term, it follows that

$$\frac{\partial f(A, Y)}{\partial \bar{z}_{\alpha\beta}} = \frac{i}{2}\frac{\partial f(A, Y)}{\partial y_{\alpha\beta}} = 0, \quad \text{for } 1 \le \alpha \le \beta \le n.$$

Hence, the coefficients $f(A, Y) = f(A)$ are independent of Y, and we get the expansion

$$F(Z) = \sum_{A \in \mathbb{E}} f(A) e^{\frac{\pi i}{q}\sigma(AZ)} \tag{1.40}$$

with constant coefficients.

The last expression can be considered as a Laurent expansion of the holomorphic function F in the variables $t_{\alpha\beta} = \exp(2\pi i z_{\alpha\beta}/q)$, and so converges absolutely on $\mathbb{H}$.

The functional equations (1.32) for a matrix M of the form (1.39) give the relation

$$(\det V)^{-k} \sum_{A \in \mathbb{E}} f(A) e^{\frac{\pi i}{q}\sigma(AV^{-1}Z\,{}^tV^{-1} + AU\,{}^tV^{-1})} = \chi(M) \sum_{A \in \mathbb{E}} f(A) e^{\frac{\pi i}{q}\sigma(AZ)}.$$

On replacing A by ${}^tVAV$ on the left, and comparing the coefficients, we get the relations (1.38).

In order to complete the proof, we only have to show that $f(A) = 0$, unless $A \ge 0$, and that the series converges uniformly on subsets (1.37).

If $n = 1$, the expansion (1.40) turns into the expansion

$$F(z) = \sum_{a \in 2\mathbb{Z}} f(a) e^{\frac{\pi i a z}{q}} = \sum_{a \in 2\mathbb{Z}} f(a) t^{a/2}, \qquad \left(t = e^{\frac{2\pi i z}{q}}\right),$$

which can be considered as a Laurent expansion of a function in t holomorphic for $|t| < 1$, except, possibly, at $t = 0$. The condition (iii) of the definition of modular forms for $n = 1$ implies that F is bounded in the circle and so is holomorphic at $t = 0$. Hence, $f(a) = 0$ if $a < 0$, and the series converges uniformly on $\mathbb{H}^1_\varepsilon$ with $\varepsilon > 0$.

Now let $n \geq 2$. Let Λ' be the group of all matrices $V \in \Lambda = SL_n(\mathbb{Z})$ such that the matrix $M(0, V)$ of the form (1.39) with $U = 0$ belongs to the kernel of the character χ. Since χ is a congruence character, the group Λ' has finite index in Λ. By (1.38), we have $f({}^tVAV) = f(A)$, for all $A \in \mathbb{E}^n$ and $V \in \Lambda'$. Hence, the expansion (1.40) can be rewritten in the form

$$F(Z) = \sum_{A \in \mathbb{E}/\Lambda'} f(A)\eta(Z, \{A\}),$$

where the sum is extended over a system of representatives for the *classes* $\{A\} = \{{}^tVAV \mid V \in \Lambda'\}$ of the set $\mathbb{E}$ modulo the equivalence $A \sim {}^tVAV$ with $V \in \Lambda'$, and where

$$\eta(Z, \{A\}) = \sum_{A' \in \{A\}} e^{\frac{\pi i}{q}\sigma(A'Z)}.$$

If $f(A) \neq 0$, then the series $f(A)\eta(Z, \{A\})$ converges absolutely for every $Z \in \mathbb{H}$, because it is a partial sum of an absolutely convergent series; in particular, the series

$$\eta(iE, \{A\}) = \sum_{A' \in \{A\}} e^{\frac{-\pi}{q}\sigma(A')}$$

is convergent. Since the trace $\sigma(A')$ of every $A' \in \{A\}$ is a rational integer, it follows that the class $\{A\}$ cannot contain more than a finite number of matrices A' with $\sigma(A') < 0$. On the other hand, we shall show that the trace $\sigma(A')$ takes infinitely many negative values on the class $\{A\}$ of any integral symmetric matrix A of order $n \geq 2$, unless $A \geq 0$. If A is not semi-definite, then there is an integral n-column $\boldsymbol{h}$ such that ${}^t\boldsymbol{h}A\boldsymbol{h} < 0$. For $r \in \mathbb{Z}$ we set

$$V_r = E + rH \qquad \text{with} \quad H = (t_1\boldsymbol{h}, \dots, t_n\boldsymbol{h}) \in \mathbb{Z}_n^n,$$

where $t_1, \dots, t_n$ are some integers. Since the rank of rH is equal to 1 or 0, it follows that

$$\det V_r = 1 + \sigma(rH) = 1 + r(t_1h_1 + \dots + t_nh_n),$$

where h_α are entries of $\boldsymbol{h}$. Since $n \geq 2$, there are integers $t_1, \dots, t_n$ not all equal 0 and such that $t_1h_1 + \dots + t_nh_n = 0$. Then we have

$$V_r \in \Lambda, \quad H^2 = ((t_1h_1 + \dots + t_nh_n)h_\alpha t_\beta) = 0, \quad \text{and } \ V_r = V_1^r.$$

Since the index of Λ' in Λ is finite, it follows that matrix $V_a = V_1^a$ belongs to Λ' for some $a \in \mathbb{N}$, and so does the matrices $V_{ab} = V_a^b$ for every integer b. Whence, the matrices ${}^tV_{ab}AV_{ab}$ belong to the class $\{A\}$, and

$$\sigma\left({}^tV_{ab}AV_{ab}\right) = \sigma(A) + 2ab\sigma(AH) + a^2b^2\sigma({}^tVAV)$$

$$= \sigma(A) + 2ab\sigma(AH) + a^2b^2({}^t\boldsymbol{h}A\boldsymbol{h})(t_1^2 + \cdots + t_n^2).$$

The last expression is a polynomial in b of degree 2 with negative leading coefficient. Hence, it takes infinitely many negative values on $\mathbb{Z}$.

The above consideration show that a coefficient $f(A)$ in (1.30) equals zero, unless $A \geq 0$, which proves the expansion (1.35).

Finally, it is easy to see that the series (1.35) is majorized on each set (1.37) by a convergent series with nonnegative constant coefficients, and so converges there uniformly.$\triangle$

Lemma 1.22. *Let F be a modular form of weight k and congruence character χ for a subgroup S of $\mathbb{S}$ commensurable with the modular group Γ, and let M be a matrix from Γ. Then*

$$F'(Z) = F|_kM \in \mathfrak{M}_k\left(M^{-1}SM,\, \chi_M\right), \tag{1.41}$$

where $|_k$ is the Petersson operator (1.29) *and χ_M is the character* (1.34).

Proof. The function F' is clearly holomorphic on $\mathbb{H}$, satisfies, by (1.31) and (1.32), the functional equations

$$F'|_k(M^{-1}M'M) = F|_k(MM^{-1}M'M) = \chi(M')F|_kM = \chi_M(M^{-1}M'M)F|_kM$$

for all $M' \in S$, and, if $n = 1$, satisfies, together with F, the condition (iii) of the definition of modular forms. $\triangle$

If S is a congruence subgroup and χ is a congruence character of S, then, by Lemma 1.20 and Theorem 1.21, the function $F|_kM$ has a Fourier expansion of the form

$$(F|_kM)(Z) = \sum_{A\in\mathbb{E}^n,\, A\geq 0} f_M(A)e^{\frac{\pi i}{q}\sigma(AZ)} \tag{1.42}$$

with a positive integer q depending on S, χ, and M, which converges absolutely on $\mathbb{H}$ and uniformly on the subsets (1.37). The modular form F is called a *cusp form*, if coefficients $f_M(A)$ of the decomposition (1.42) satisfy the conditions

$$f_M(A) = 0 \qquad \text{for all } M \in \Gamma \quad \text{and } A \in \mathbb{E} \quad \text{with } \det A = 0. \tag{1.43}$$

The subspace of cusp forms of $\mathfrak{M}_k(S,\, \chi)$ will be denoted by $\mathfrak{N}_k(S,\, \chi)$.

Proposition 1.23. *Let S be a congruence subgroup of $\mathbb{S} = \mathbb{S}^n$ and χ a congruence character of S. Then, for each cusp form $F \in \mathfrak{N}_k(S,\, \chi)$ and each matrix $M \in \Gamma$,* *the function* $F|_kM \in \mathfrak{M}_k\left(M^{-1}SM, \chi_M\right)$*, where* χ_M *is the character* (1.34)*, is a cusp form with the Fourier expansion of the shape*

$$(F|_kM)(Z) = \sum_{A\in\mathbb{E}^n,\, A>0} f_M(A)e^{\frac{\pi i}{q}\sigma(AZ)}. \tag{1.44}$$

where q *is a positive integer. If* $k \geq 0$*, then each of the forms* $F|_kM$ *satisfies*

$$|(F|_kM)(X+iY)| \leq \delta(\det Y)^{k/2}, \qquad (X+iY \in \mathbb{H}), \tag{1.45}$$

and its Fourier coefficients satisfy

$$|f_M(A)| \leq \delta'(\det A)^{k/2} \qquad \textit{for all } A \in \mathbb{E} \quad \textit{with } A > 0, \tag{1.46}$$

where δ *and* δ' *are constant depending only on* F*.*

First we shall prove the following simple lemma.

Lemma 1.24. *Let*

$$\phi(Y) = \sum_{A\in\mathbb{E}^n,\, A>0} \varphi(A)e^{-\eta\sigma(AY)},$$

where Y *belongs to the cone* $\boldsymbol{P} = \boldsymbol{P}_n$ *of positive definite matrices of order* n *and* $\eta > 0$*, be a series with nonnegative coefficients* $\eta(A)$ *convergent for all* $Y \in \boldsymbol{P}$*. Then, for every Minkowski reduced matrix* Y *satisfying* $Y \geq dE$ *with* $d > 0$*, the following estimate holds*

$$\phi(Y) \leq d'e^{-d''\sigma(Y)},$$

with positive constants d' *and* d''*.*

Proof of the lemma. If $Y = (y_{\alpha\beta}) \in \boldsymbol{P}$ and $A = (a_{\alpha\beta}) \in \mathbb{E}$ satisfies $A > 0$ then, by (1.23),

$$\sigma(AY) \geq b\sigma(A\, diag(y_{11}, y_{22}, \ldots, y_{nn})) = b\sum_{\alpha=1}^{n} a_{\alpha\alpha}y_{\alpha\alpha} \geq 2b\sigma(Y),$$

where b is a positive constant depending only on n. On the other hand, if $Y > dE$, then for $A = (a_{\alpha\beta}) \in \mathbb{E}$ with $A > 0$, we obtain $\sigma(AY) \geq d\sigma(A)$. (Note that we have used twice the obvious inequality $\sigma(AR) \geq \sigma(BR)$ valid if matrices $A-B$ and R are positive semi-definite.) It follows then from the above inequalities that

$$\sigma(AY) \geq b\sigma(Y) + \frac{1}{2}d\sigma(A),$$

whence

$$\phi(Y) \leq \sum_{A \in \mathbb{E},\, A>0} \varphi(A) e^{-\eta(b\sigma(Y)+\frac{1}{2}d\sigma(A))} = e^{-\eta b\sigma(Y)}\phi(\frac{1}{2}dE),$$

which proves the estimate. △

Proof of Proposition 1.23. The fact that $F|_k M$ is a cusp form with the Fourier expansion (1.44) follows from the definition of cusp forms and Lemma 1.22.

By our assumption, χ is trivial on a principal congruence subgroup $\Gamma(q)$ of Γ. Let us consider the function

$$G = \sum_{M_\alpha \in \Gamma(q)\backslash\Gamma} |F|_k M_\alpha|. \tag{1.47}$$

It follows from (1.31) and (1.32) that G is independent of the choice of representatives in the cosets $\Gamma(q)\backslash\Gamma$ and satisfies

$$|G|_k M| = \sum_{M_\alpha \in \Gamma(q)\backslash\Gamma} |F|_k M_\alpha M| = G \qquad \text{for all } M \in \Gamma, \tag{1.48}$$

because $M_\alpha M$ runs through a system of representatives for $\Gamma(q)\backslash\Gamma$, when M_α does. Hence, by (1.10), we see that the function

$$H(Z) = H(X+iY) = (\det Y)^{k/2} \sum_{M_\alpha \in \Gamma(q)\backslash\Gamma} |F|_k M_\alpha| \tag{1.49}$$

satisfies

$$H(M\langle Z\rangle) = H(Z) \qquad \text{for all } Z \in \mathbb{H} \quad \text{and } M \in \Gamma. \tag{1.50}$$

Since, by Theorem 1.21, each of the functions $F|_k M_\alpha$ is bounded on the sets $\mathbb{H}_\varepsilon$ with $\varepsilon > 0$, it follows from (1.26) that the functions are bounded on the fundamental domain $\boldsymbol{D}$ of Γ, defined in Theorem 1.16. Besides,

$$|F|_k M| \leq \sum_{A \in \mathbb{E},\, A>0} |f_M(A)| e^{-\frac{\pi}{q}\sigma(AY)},$$

and the last series converges on the cone $\boldsymbol{P} = \boldsymbol{P}_n$. If $Z \in \boldsymbol{D}$, then Y is Minkowski reduced and satisfies $Y \geq b_n E$, hence, by Lemma 1.24, each of the series is dominated by a function of the form $d' \exp(-d''\sigma(Y))$ with constant d' and d'' depending on F and M. Therefore, since $k \geq 0$, we obtain

$$\begin{aligned} H(X+iY) &\leq d'[\Gamma : \Gamma(q)](\det Y)^{k/2} \exp(-d''\sigma(Y)) \\ &\leq \delta \prod_{\alpha=1}^{n} y_{\alpha\alpha}^{k/2} \exp(-d'' y_{\alpha\alpha}), \end{aligned}$$

where $y_{\alpha\alpha}$ are the diagonal entries of Y, and we have also used the following consequence of the Hadamard's determinant theorem

$$\det Y \le y_{11}y_{22}\cdots y_{nn} \qquad (Y \in \boldsymbol{P}_n). \tag{1.51}$$

Since the last expression is clearly bounded on $\boldsymbol{P}$, it follows that H is bounded on $\boldsymbol{D}$. Thus, by (1.50), H is bounded on $\mathbb{H}$, which imply the estimate (1.45). Finally, for the Fourier coefficients we obtain

$$q^{\frac{n(n+1)}{2}}|f_M(A)| \\ = |\int_{-q/2\le x_{\alpha\beta}\le q/2}(F|_kM)((x_{\alpha\beta})+iA^{-1})e^{-\frac{\pi i}{q}\sigma((x_{\alpha\beta})+iA^{-1})}\prod_{1\le\alpha\le\beta\le n}dx_{\alpha\beta}|,$$

and the estimate (1.46) follows from (1.45). $\triangle$

One can prove that the coefficients of the Fourier expansion (1.35) of an arbitrary modular form of nonnegative weight k and congruence character for a congruence subgroup of $\mathbb{S}^n$ satisfy

$$|f(A)| \le c(\det A)^k, \qquad (A \in \mathbb{E}^n,\ A \ge 0), \tag{1.52}$$

where c depends only on the form (see *Sources*).

The general philosophy of modular forms believes that consideration of arbitrary modular forms can usually be reduced to the case of cusp forms and the cases of modular forms of smaller genuses. The reduction is ensured by the *Siegel operator* and its iterations. Let $F = F(Z)$ be a modular form of weight k and character χ for a congruence subgroup S of the symplectic group $\mathbb{S} = \mathbb{S}^n$ and a congruence character χ of S. Since the Fourier series (1.25) for F converges uniformly on subsets of $\mathbb{H}^n$ of the form (1.27), the limit

$$(F|\Phi)(Z') = \lim_{\lambda\to+\infty} F\left(\begin{pmatrix} Z' & 0 \\ 0 & i\lambda\end{pmatrix}\right) = \sum_{A\in\mathbb{E}^n,\, A\ge O} f(A)\lim_{\lambda\to+\infty} e^{\frac{\pi i}{q}\sigma\left(AZ'_\lambda\right)}, \tag{1.53}$$

where $Z'_\lambda = \begin{pmatrix} Z' & 0 \\ 0 & i\lambda\end{pmatrix}$, exists for every $Z' \in \mathbb{H}^{n-1}$. If $A = \begin{pmatrix} A' & * \\ * & a_{nn}\end{pmatrix}$, then $\sigma(AZ'_\lambda) = \sigma(A'Z') + i\lambda a_{nn}$, whence

$$\lim_{\lambda\to+\infty} e^{\frac{\pi i}{q}\sigma(AZ'_\lambda)} = \lim_{\lambda\to+\infty} e^{-\frac{\pi}{q}\lambda a_{nn}}e^{\frac{\pi i}{q}\sigma(A'Z')} = \begin{cases} e^{\frac{\pi i}{q}\sigma(A'Z')}, & \text{if } a_{nn} = 0 \\ 0, & \text{if } a_{nn} > 0.\end{cases}$$

Since $A \geq 0$, the equality $a_{nn} = 0$ implies that A has the form $\begin{pmatrix} A' & 0 \\ 0 & 0 \end{pmatrix}$. Thus, we have

$$(F|\Phi)(Z') = \sum_{A' \in \mathbb{E}^{(n-1)},\, A' \geq 0} f\left(\begin{pmatrix} A' & 0 \\ 0 & 0 \end{pmatrix}\right) e^{\frac{\pi i}{q}\sigma\left(A'Z'\right)}, \tag{1.54}$$

for all $Z' \in \mathbb{H}^{(n-1)}$. The last series is a partial series for the Fourier expansion of F, and so it converges absolutely on $\mathbb{H}^{(n-1)}$ and uniformly on $\mathbb{H}^{(n-1)}_{\varepsilon}$ with $\varepsilon > 0$. If $n = 1$, we set

$$F|\Phi = \lim_{\lambda \to +\infty} F(i\lambda) \in \mathbb{C}. \tag{1.55}$$

As above, the limit exists and is equal to the constant term of the Fourier expansion of F. The linear operator

$$\Phi : F \mapsto F|\Phi, \qquad (F \in \mathfrak{M}_k(S, \chi)), \tag{1.56}$$

is called the *Siegel operator*.

In order to show that the function $F|\Phi$ is a modular form on $\mathbb{H}^{(n-1)}$, we shall need new notation. Let $n > 1$. For a matrix $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ with square blocks A', B', C', and D' of order $n - 1$, we set

$$\overrightarrow{M'} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \qquad \text{and} \qquad \phi(\overrightarrow{M'}) = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix},$$

where

$$A = \begin{pmatrix} A' & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} B' & 0 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} C' & 0 \\ 0 & 0 \end{pmatrix}, D = \begin{pmatrix} D' & 0 \\ 0 & 1 \end{pmatrix}.$$

If S is a subgroup of $\mathbb{G}^n$, we denote by $\overleftarrow{S}$ the set of all matrices $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ such that the matrix $\overrightarrow{M'}$ belongs to S:

$$\overleftarrow{S} = \left\{ M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \in \mathbb{R}^{2n-2}_{2n-2} \;\middle|\; \overrightarrow{M'} \in S \right\}. \tag{1.57}$$

Then it is clear that $\overleftarrow{S}$ is a subgroup of $\mathbb{S}^{(n-1)}$, and the map ψ given by

$$\overleftarrow{S} \ni M' \mapsto \psi(M') = \overrightarrow{M'} \in S \tag{1.58}$$

is a homomorphic embedding of the group $\overleftarrow{S}$ into S.

Lemma 1.25. *Let S be a congruence subgroup of $\mathbb{S}^n$ with $n > 1$, and χ a congruence character of S. Then the group $\overleftarrow{S}$ is a congruence subgroup of $\mathbb{G}^{(n-1)}$, and the map $\overleftarrow{\chi}$ given by*

$$\overleftarrow{S} \ni M' \mapsto \overleftarrow{\chi}(M') = \chi(\overrightarrow{M'}) \tag{1.59}$$

is a congruence character of $\overleftarrow{S}$.

Proof. By the assumptions, S contains a principal congruence subgroup $\Gamma(q) = \Gamma^n(q)$ of finite index belonging to the kernel of χ. Then the group $\overleftarrow{\Gamma(q)}$ of the form (1.57) is clearly a principal congruence subgroup of $\overleftarrow{S}$ belonging to the kernel of the character $\overleftarrow{\chi}$. It remains to prove that $\overleftarrow{\Gamma(q)}$ has finite index in $\overleftarrow{S}$. Really, if $\overleftarrow{\Gamma(q)}M'_\alpha \neq \overleftarrow{\Gamma(q)}M'_\beta$, where M'_α, M'_β belong to $\overleftarrow{S}$, then $\Gamma(q)\overrightarrow{M'_\alpha} \neq \Gamma(q)\overrightarrow{M'_\beta}$, since otherwise we would have $\overrightarrow{M'_\alpha}(\overrightarrow{M'_\beta})^{-1} \in \Gamma(q)$, and so $M'_\alpha(M'_\beta)^{-1} \in \overleftarrow{\Gamma}(q)$.△

Now we can prove

Theorem 1.26. *Let S be a congruence subgroup of $\mathbb{S}^n$, and χ a congruence character of S. Then the Siegel operator Φ maps the space $\mathfrak{M}_k(S, \chi)$ into the space $\mathfrak{M}_k(\overleftarrow{S}, \overleftarrow{\chi})$:*

$$\Phi : \mathfrak{M}_k(S, \chi) \mapsto \mathfrak{M}_k(\overleftarrow{S}, \overleftarrow{\chi}), \tag{1.60}$$

where, for $n = 1$, we set

$$\mathfrak{M}_k(\overleftarrow{S}, \overleftarrow{\chi}) = \mathbb{C}.$$

Proof. One can assume that $n > 1$. Let $F \in \mathfrak{M}_k(S, \chi)$, $Z' \in \mathbb{H}^{n-1}$, $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \in \overleftarrow{\mathbb{S}}$, $Z'_\lambda = \begin{pmatrix} Z' & 0 \\ 0 & i\lambda \end{pmatrix}$, and $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \psi(M') \in \mathbb{S}$, where ψ is the embedding (1.58). Then we have

$$M\langle Z'_\lambda\rangle = \begin{pmatrix} A'Z' + B' & 0 \\ 0 & i\lambda \end{pmatrix} \begin{pmatrix} C'Z' + D' & 0 \\ 0 & 1 \end{pmatrix}^{-1} = M'\langle Z'\rangle_\lambda,$$

$$\det(CZ'_\lambda + D) = \det(C'Z' + D'), \quad \text{and} \quad \chi(M) = \overleftarrow{\chi}(M').$$

It follows that

$$\begin{aligned}(F|\Phi|_k M')(Z') &= \det(C'Z' + D')^{-k} \lim_{\lambda\to+\infty} F(M'\langle Z'\rangle_\lambda) \\ &= \lim_{\lambda\to+\infty} \det(CZ_\lambda + D)^{-k} F(M\langle Z'_\lambda\rangle) = (F|_k M|\Phi)(Z').\end{aligned} \tag{1.61}$$

In particular, if $M' \in \overleftarrow{S}$, then we have

$$F|\Phi|_k M' = \chi(M) F\Phi = \overleftarrow{\chi}(M') F|\Phi.$$

Besides, it follows from (1.54) and (1.61) that the function $(F|\Phi|_k M')(Z')$ is holomorphic on $\mathbb{H}^{n-1}$, and is bounded on each subset $\mathbb{H}^{n-1}_\varepsilon$ with $\varepsilon > 0$.△

¿From (1.54) and the definition of cusp forms we obtain

Lemma 1.27. *Let S be a congruence subgroup of $\mathbb{S}^n$, and χ a congruence character of S. Then a function $F \in \mathfrak{M}_k(S, \chi)$ is a cusp form if and only if it satisfies*

$$(F|_k M)|\Phi = 0 \qquad \text{for all } M \in \Gamma,$$

where Φ is the Siegel operator.

We can prove now the following important theorem.

Theorem 1.28. *Let S be a congruence subgroup of $\mathbb{S}^n$, χ a congruence character of S, and k a nonnegative integer. Then the space $\mathfrak{M}_k(S, \chi)$ of modular forms of weight k and character χ for the group S is finite-dimensional over the field $\mathbb{C}$.*

The proof of the theorem is based on the next key lemma.

Lemma 1.29. *Let*

$$F(Z) = \sum_{A \in \mathbb{E},\, A > 0} f(A) e^{\pi i \sigma(AZ)}$$

be a cusp form of a nonnegative integral weight k and the unit character χ for the full modular group $\Gamma = \Gamma^n$. Suppose that the Fourier coefficient satisfy the conditions

$$f(A) = 0, \qquad \text{if} \quad \sigma(A) \le \frac{kn}{2\pi b_n}, \tag{1.62}$$

where b_n is the constant of Theorem 1.16. Then F is identically equal to zero.

Proof of the lemma. Similarly to the proof Proposition 1.23, let us consider the function

$$H(Z) = H(X + iY) = (\det Y)^{k/2} |F(Z)|.$$

As we have seen, it satisfies $H(M\langle Z\rangle) = H(Z)$ for all $Z \in \mathbb{H}$ and $M \in \Gamma$ and is bounded on the fundamental domain $\boldsymbol{D}_n$ of Γ described in Theorem 1.16. Besides, it follows from the estimates (1.51) and (1.52) that $H(X+iY) \to 0$, when $\det Y \to +\infty$ remaining in $\boldsymbol{D}_n$. It follows from Theorem 1.16 that any subset of $\boldsymbol{D}_n$ of the form $\{X + iY \in \boldsymbol{D}_n | \det Y \le c\}$ with $c > 0$ is bounded and closed, and therefore is compact. Hence, the function $H(Z)$ attains its maximum μ at some point $Z_0 = X_0 + iY_0$ of $\boldsymbol{D}_n$. Since H is Γ-invariant, we conclude that μ is the maximum of H on $\mathbb{H}$, that is $H(Z) \leq H(Z_0) = \mu$ for all $Z \in \mathbb{H}$. Let us set $Z_t = Z_0 + tE$, where $t = u + iv$ is a complex parameter, and consider the function

$$\begin{aligned} h(t) &= F(Z_t)e^{-\pi i\lambda\sigma(Z_t)} \\ &= \sum_{A\in\mathbb{E},\, A>0} f(A)e^{\pi i(\sigma(AZ_0+t\sigma(A))-\lambda\sigma(Z_0+tE))} \\ &= \sum_{A\in\mathbb{E},\, A>0} f(A)e^{\pi i(\sigma(AZ_0-\lambda Z_0))}e^{\pi it(\sigma(A)-\lambda n)} \\ &= h'(w), \end{aligned}$$

where $w = e^{\pi it}$, and λ satisfies $\lambda n = 1 + [kn/2\pi b_n]$. By the assumption of the lemma, $f(A) = 0$ if $\sigma(A) - \lambda n < 0$, and so the expansion of the function $h'(w)$ does not contain negative powers of w. If $\varepsilon > 0$ is so small that $Z_t \in \mathbb{H}$ for $v \geq -\varepsilon$, then the expansion converges absolutely and uniformly on the half-plane $v \geq -\varepsilon$, and so the function $h'(w)$ is holomorphic in the disk $|w| \leq e^{\pi\varepsilon} = \tau$. Since $\tau > 1$, it follows, by the maximum-modulus principle, that there is a point $w_0 = e^{\pi it_0}$ satisfying $|w_0| = \tau$ and $h'(1) \leq h'(w_0)$. Coming back to the function h, we can rewrite the last inequality in the form

$$|F(Z_0)e^{\pi\lambda\sigma(Y_0)}| \leq |F_{t_0}|e^{\pi\lambda\sigma(Y_0)}e^{\pi\lambda nv_0},$$

where $t_0 = u_0 + v_0$, whence

$$(\det Y_0)^{-k/2}H(Z_0) \leq (\det Y_{t_0})^{-k/2}H(Z_{t_0})e^{\pi\lambda nv_0}.$$

Since $H(Z_0) = \mu$ and $H(Z_{t_0}) \leq \mu$, the last inequality implies the inequality

$$\mu \leq \mu(\det Y_0)^{k/2}(\det Y_{t_0})^{-k/2}e^{\pi\lambda nv_0} = \mu\psi(v_0),$$

where $\psi(v) = \det(E + vY_0^{-1})^{-k/2}e^{\pi\lambda nv}$. We have $\psi(0) = 1$. Let us show that the derivative of ψ is positive at $v = 0$. We can write

$$\psi(v) = e^{\pi\lambda nv}\prod_{j=1}^{n}(1 + v\lambda_j)^{-k/2},$$

where $\lambda_1, \ldots, \lambda_n$ are the characteristic values of Y_0^{-1}, whence the value of the derivative at $v = 0$ is

$$\begin{aligned} \pi\lambda n - \frac{k}{2}(\lambda_1 + \cdots + \lambda_n) &= \pi\lambda n - \frac{k}{2}\sigma(Y_0^{-1}) \\ &\geq \pi\lambda n - \frac{kn}{2b_n} = \pi\left(1 + \left[\frac{kn}{2\pi b_n}\right]\right) - \frac{kn}{2b_n} > 0, \end{aligned}$$

by (1.26), since $X_0 + iY_0 \in \boldsymbol{D}_n$. It follows that, for small $\varepsilon > 0$, we have $\psi(v_0) = \psi(-\varepsilon) < 1$ (we remind that $e^{\pi\varepsilon} = \tau = |e^{\pi i(u_0+iv_0)}| = e^{-\pi v_0}$). Then the above inequality shows that $\mu = 0$, and so F is identically equal to zero. $\triangle$

Proof of Theorem 1.28. Note, first of all, that if the character χ is trivial on a principal congruence subgroup $\Gamma(q) = \Gamma^n(q)$ contained in the group S, then the space $\mathfrak{M}_k(S, \chi)$ is contained into the space $\mathfrak{M} = \mathfrak{M}_k(\Gamma(q))$ of modular forms of weight k and the unit character for the group $\Gamma(q)$. Therefore, it will sufficient to prove that each of the spaces is finite-dimensional. We remind that $\Gamma(q)$ is a normal subgroup of finite index $\nu = [\Gamma : \Gamma(q)]$ in Γ. Let $M_1, \dots, M_\nu$ be a system of representatives for cosets of Γ modulo $\Gamma(q)$. For a function $F \in \mathfrak{M}$, let us consider the functions

$$F_1 = F|_k M_1, \dots, F_\nu = F|_k M_\nu. \tag{1.63}$$

By (1.31) and (1.32), the functions does not depend on the choice of the representatives M_α. Since, for any $M \in \Gamma$, the set $M_1 M, \dots, M_\nu M$ is again a set of representatives for the cosets, it follows that the functions $F_1|_k M, \dots, F_\nu|_k M$ coincide up to a permutation with the functions (1.63). By Lemma 1.22, each of the functions (1.63) belongs to $\mathfrak{M}$ and, by Proposition 1.23, is a cusp form, if F is a cusp form.

Now, let us derive from Lemma 1.29 its generalization to the subspace $\mathfrak{N} = \mathfrak{N}_k(\Gamma(q))$ of cusp forms of $\mathfrak{M}$: If

$$F(Z) = \sum_{A \in \mathbb{E},\, A > 0} f(A) e^{\pi i \sigma(AZ)} \in \mathfrak{N},$$

and the Fourier coefficients $f(A)$ satisfy

$$f(A) = 0, \qquad \text{if} \quad \sigma(A) \le \frac{knq\nu}{2\pi b_n}, \tag{1.64}$$

then F is identically equal to zero. For that we shall consider the product

$$G(Z) = \prod_{\alpha=1}^{\nu} F_\alpha(Z)$$

of the functions (1.63). By (1.29) and the above consideration, we have, for every $M \in \Gamma$,

$$\begin{aligned} G|_{k\nu} M = j(M, Z)^{-k\nu} G(M\langle Z\rangle) &= \prod_{\alpha=1}^{\nu} (j(M, Z)^{-k} F_\alpha(\langle Z\rangle)) \\ = \prod_{\alpha=1}^{\nu} F_\alpha|_k M = \prod_{\alpha=1}^{\nu} F_\alpha = G. \end{aligned}$$

Since G, obviously, satisfies analytical conditions of the definition of cusp forms, we conclude that G is a cusp forms of weight $k\nu$ for the group Γ. Let $f_\alpha(A)$ be the Fourier coefficients of the function F_α, so that

$$F_\alpha = \sum_{A\in\mathbb{E},\, A>0} f_\alpha(A)e^{\frac{\pi i}{q}\sigma(AZ)}.$$

Then the Fourier coefficients $g(A)$ of G can be written in the form

$$g(A) = \sum_{A_1+\ldots+A_\nu=qA} f_1(A_1)\cdots f_\nu(A_\nu).$$

Let A be a positive definite matrix of $\mathbb{E}$ satisfying $\sigma(A) \leq kn\nu/2\pi b$, where $b = b_n$. Then the inequality

$$\sigma(A) = \frac{1}{q}(\sigma(A_1) + \cdots + \sigma(A_\nu)) \leq \frac{k\nu n}{2\pi b}$$

for positive definite even matrices $A_1, \ldots, A_\nu$ implies that $\sigma(A_\alpha) < knq\nu/2\pi b$ for each $\alpha = 1, \ldots, \nu$, since the trace of any positive definite matrix is positive. If, for example, $F_1 = F$ and so $f_1 = f$, then the condition (1.64) implies that each of the terms of the sum for $g(A)$ has a factor of the form $f_1(A_1) = f(A_1)$ with $\sigma(A_1) < knq\nu/2\pi b$, which is zero. Then, by Lemma 1.29, $G = 0$, and so $F = 0$.

Now, we can prove that the subspace $\mathfrak{N}$ of cusp forms of $\mathfrak{M}$ is finite-dimensional. Since entries of positive semi-definite matrices $A = (a_{\alpha\beta})$ satisfy the inequalities $a_{\alpha\alpha} \pm 2a_{\alpha\beta} + a_{\beta\beta} \geq 0$, it follows that the number of even positive semi-definite even matrices A of order n with $\sigma(A) \leq 2N$ does not exceed the bound

$$(N+1)^n(2N+1)^{n(n-1)/2}. \tag{1.65}$$

Therefore, the number of positive definite even matrices A satisfying the inequality in (1.64)is bounded by a number of the form $d_n(kq\nu)^{n(n+1)/2}$, where d_n depends only on n. Taking d_n to be integral number, we see that arbitrary $d+1$ functions $F_1, \ldots, F_{d+1}$ of $\mathfrak{N}$ are linearly dependent, since one can always find complex numbers $c_1, \ldots, c_{d+1}$ not all equal zero and such that the function $F = c_1F_1 + \ldots + c_{d+1}F_{d+1}$ satisfies the condition (1.64) and therefore is identically equal to zero.

Finally, we use induction on n to prove the theorem for the spaces $\mathfrak{M}^n = \mathfrak{M}_k(\Gamma^n(q))$. Let us define for $n \geq 1$ the linear map

$$\Phi = \Phi_n : \quad \mathfrak{M}^n \mapsto \underbrace{\mathfrak{M}^{n-1} \times \cdots \times \mathfrak{M}^{n-1}}_{\nu_n \text{ times}}$$

by
$$F|\varPhi = (F_1|\Phi, \dots, F_{\nu_n}|\Phi)\,, \qquad (F \in \mathfrak{M}^n),$$
where ν_n is the index of $\Gamma^n(q)$ in Γ^n, Φ the Siegel operator (1.56), F_α are the functions (1.63), and where we set $\mathfrak{M}^0 = \mathbb{C}$. By Lemma 1.27, the kernel of $\varPhi_n$ coincides with the subspace $\mathfrak{N}^n$ of cusp forms of $\mathfrak{M}^n$ and so is finite-dimensional. The image of $\varPhi_1$ is finite-dimensional, since it is contained in $\mathbb{C}^{\nu_1}$, which proves the theorem for $n = 1$. If it is already proved for $n-1 \geq 1$, then the image of $\varPhi_n$ is finite-dimensional and so is the space $\mathfrak{M}^n$. $\triangle$

One can show that $\mathfrak{M}(S, \chi) = \{0\}$ if k is a negative integer, but we shall not need the result.

Exercise 1.30. *Show that* $\mathfrak{M}_k(\Gamma^n) = \{0\}$ *if* nk *is odd.*

Exercise 1.31. *Show that the spaces* $\mathfrak{M}_k(\Gamma^1)$ *for* $k = 0, 2, 4, 6, 8, 10$ *contain no cusp forms, and there is not more than one linearly independent cusp forms of weight* 12 *for* Γ^1.

[Hint: Use Lemma 1.29 for $n = 1$ with b_1 given in Exercise 1.17.]

Exercise 1.32. *Let* $k > 2$ *be an integer. Show that the Eisenstein series*
$$E_k(z) = \sum_{\substack{c,d\in\mathbb{Z};\\ (c,d)\neq(0,0)}} \frac{1}{(cz+d)^k}, \qquad (z \in \mathbb{H}^1)$$
converges absolutely and defines a modular form of weight k *for* Γ^1.

[Hint: If $\boldsymbol{S}$ is a compact subset of $\mathbb{H}^1$, then $|\alpha z+\beta| \geq b(|\alpha|+|\beta|)$ for all α, $\beta \in \mathbb{R}$ and $z \in \boldsymbol{S}$ with a positive constant b. Since there are only $4r$ pairs of integers (c, d) with $|c| + |d| = r$, it follows $E_k(z)$ is dominated term by term by
$$b^{-k}\sum_{r=1}^{\infty}\frac{4r}{r^k}.]$$

Exercise 1.33. *Show that, if* $k > 2$ *is even, then the Fourier expansion of* $E_k(z)$ *has the form*
$$E_k(z) = 2\sum_{n=1}^{\infty}\frac{1}{n^k} + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\left(\sum_{d|n} d^{k-1}\right) e^{2\pi i n z}.$$

[Hint: Show first that
$$\sum_{d\in\mathbb{Z}}\frac{1}{(z+d)^k} = \frac{\pi^2}{\sin^2 \pi z} = \frac{(2\pi)^2 t}{(1-t)^2} = (2\pi i)^2\sum_{d=1}^{\infty} d t^d,$$
where $t = e^{2\pi i z}$. Then differentiate the both parts $k-2$ times.]

Exercise 1.34. *let k be a positive even integer. Show that the Fourier coefficients of any modular form*

$$F(z) = \sum_{a=0}^{\infty} f(2a)e^{2\pi iaz} \in \mathfrak{M}_k(\Gamma^1)$$

satisfy

$$f(2a) = f(0)\zeta(k)^{-1}\frac{(2\pi i)^k}{(k-1)!}\sum_{d|n} d^{k-1} + f'(a), \quad \textit{where } |f'(a)| \le \delta_F a^{k/2},$$

where $\zeta(s)$ is the Riemann zeta.

[Hint: Show first that the function $F(z) - f(0)(2\zeta(k))^{-1}E_k(z)$ is a cusp form. Then use Exercise 1.33 and (1.46).]

Exercise 1.35. *Show that the spaces $\mathfrak{M}_k(\Gamma^1)$ for $k = 0, 4, 6, 8, 10$ are spanned respectively by 1, E_4, E_6, E_8, and E_{10}.*

Exercise 1.36. *Show that the function*

$$\Delta'(z) = ((2\zeta(4))^{-1}E_4(z))^3 - ((2\zeta(6))^{-1}E_6(z))^2$$

is a nonzero cusp form of space $\mathfrak{M}_{12}(\Gamma^1)$ and together with $E_{12}(z)$ span the space.

§1.4. Petersson scalar product.

Every space $\mathfrak{N}_k(S, \chi)$ of cusp forms of an integral weight k and a congruence character χ for a congruence subgroup S of the symplectic group can be endowed with structure of a Hilbert space by means of the Petersson scalar product. For two functions F and F' on $\mathbb{H} = \mathbb{H}^n$, we consider the differential form on $\mathbb{H}$ defined by

$$\omega_k(F, F') = F(Z)\overline{F'(Z)}h(Z)^k d^*Z, \tag{1.66}$$

where $h(Z) = h(X + iY) = \det Y$ is the height of Z, d^*Z is the invariant element of volume (1.12), and, us usual, bar means the complex conjugation. It follows from Lemma 1.4 and Proposition 1.6 that, for each matrix $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{G} = \mathbb{G}^n$, the form satisfies the relation

$$\omega_k(F, F')(M\langle Z\rangle) = F(M\langle Z\rangle)\overline{\det F'(M\langle Z\rangle)}h(M\langle Z\rangle)^k d^*M\langle Z\rangle$$

$$= \mu(M)^{nk} \det(CZ+D)^{-k} F(M\langle Z\rangle)\overline{\det(CZ+D)}^{-k}\overline{F'(M\langle Z\rangle)}h(Z)^k d^*Z$$
$$= \mu(M)^{-nk+n(n+1)} \left(F|_k M\right)(Z)\overline{\left(F'|_k M\right)(Z)}h(Z)^k d^*Z$$

$$= \mu(M)^{n(n+1-k)}\omega_k\left(F|_k M,\, F'|_k M\right)(Z), \tag{1.67}$$

where $|_k M$ is the Petersson operator (1.29) of weight k. In particular, if $F, F' \in \mathfrak{M}_k(S, \chi)$ and $M \in S$, then, by (1.32), we have

$$\omega_k(F, F')(M\langle Z\rangle) = \omega_k(\chi(M)F, \chi(M)F')(Z) = \omega_k(F, F')(Z). \tag{1.68}$$

It follows that the integral

$$\int_{D(S)} \omega_k(F, F')(Z) \tag{1.69}$$

on a fundamental domain $D(S)$ of S on $\mathbb{H}$ does not depend on the choice of the fundamental domain, provided that it converges absolutely.

Lemma 1.37. *Let S be a congruence subgroup of $\mathbb{S} = \mathbb{S}^n$, χ a congruence character of S, and k an integer. Suppose that at least one of the forms $F, F' \in \mathfrak{M}_k(S, \chi)$ is a cusp form. Then the integral* (1.69) *converges absolutely.*

Proof. By increasing the space $\mathfrak{M}_k(S, \chi)$, one may assume that S is a subgroup of finite index in Γ and the character χ is trivial on S. Let us take then as $D(S)$ a fundamental domain of the form (1.28) with $M = 1_{2n}$, that is a finite union of the sets $M_\alpha\langle \boldsymbol{D}\rangle$ with $M_\alpha \in \Gamma$, where $\boldsymbol{D} = \boldsymbol{D}_n$ is the fundamental domain of Γ described in Theorem 1.16. Then, by (1.67), it is sufficient to show that each integral

$$\int_{M\langle \boldsymbol{D}\rangle} \omega_k(F, F')(Z) = \int_{\boldsymbol{D}} \omega_k\left(F|_k M,\, F'|_k M\right)(Z) \text{ with } M \in \Gamma$$

converges absolutely. Assuming that F' is a cusp form, by (1.42) and (1.43), we can write absolutely convergent Fourier expansions

$$F|_k M = \sum_{A \in \mathbb{E}, A \geq 0} f_M(A) e^{\frac{\pi i}{q}\sigma(AZ)},$$

$$F'|_k M = \sum_{A \in \mathbb{E}, A > .0} f'_M(A) e^{\frac{\pi i}{q}\sigma(AZ)},$$

where $\mathbb{E} = \mathbb{E}^n$ and q is such that $\Gamma^n(q) \subset S$. It follows that

$$|(F|_k)(Z)\overline{(F'|_k M)}(Z)| \leq \sum_{A \in \mathbb{E}, A > 0} c(A) e^{-\frac{\pi}{q}\sigma(AZ)},$$

where $Z = X + iY$, with nonnegative coefficients $c(A)$, and the last series converges on $\mathbb{H}$. Then, by Theorem 1.16 and Lemma 1.24, we get the inequality

$$|(F|_k)(Z)\overline{(F'|_k M)}(Z)| \leq d' e^{-d''\sigma(Y)}, \quad (Z = X + iY \in \boldsymbol{D}),$$

with positive constants d' and d''. Thus, to prove the lemma it suffices to show that the integral

$$\int_{\boldsymbol{D}} e^{-d\sigma(Y)} (\det Y)^{k-n-1} \prod_{1 \leq \alpha \leq \beta \leq n} dx_{\alpha\beta} dy_{\alpha\beta}$$

with $d > 0$ converges. If $(x_{\alpha\beta}) + i(y_{\alpha\beta}) \in \boldsymbol{D}$, then it follows from the definition of $\boldsymbol{D}$ and (1.22) that $|x_{\alpha\beta}| \leq 1/2$ for $1 \leq \alpha, \beta \leq n$ and $y_{\alpha\beta} \leq y_{\alpha\alpha}/2$ for $\alpha \neq \beta$. In the proof of Theorem 1.16 we have seen that $y_{\alpha\alpha} \geq \sqrt{3}/2$ for $\alpha = 1, \ldots, n$. Then the inequality (1.22), if $k < n$, and the inequality (1.51), if $k \geq n + 1$, imply that the last integral is majorized by

$$c \int_{\substack{|x_{\alpha\beta}| \leq 1/2, y_{\alpha\alpha} \geq \sqrt{3}/2, \\ |y_{\alpha\beta}| \leq y_{\alpha\alpha}/2 (\alpha \neq \beta)}} \prod_{\alpha=1}^{n} y_{\alpha\alpha}^{k-n-1} e^{-\delta y_{\alpha\alpha}} \prod_{1 \leq \alpha \leq \beta \leq n} dx_{\alpha\beta} dy_{\alpha\beta}$$

$$= c \prod_{\alpha=1}^{\infty} \int_{\sqrt{3}/2}^{\infty} y_{\alpha\alpha}^{k-n-1+n-\alpha} e^{-\delta y_{\alpha\alpha}} dy_{\alpha\alpha} < \infty.$$

△

The above lemma justifies the following definition. For two modular forms $F, F' \in \mathfrak{M}(S, \chi)$ of an integral weight k and a congruence character χ for a congruence subgroup $S \subset \mathbb{S}$, such that at least one of the forms is a cusp form, the integral

$$(F, F') = \nu(K')^{-1} \int_{D(K)} \omega_k(F, F')(Z), \tag{1.70}$$

where K is a congruence subgroup of Γ contained in S, $K' = K \cup (-1_{2n})K$, $\nu(K')$ the index of K' in Γ, and $D(K)$ a fundamental domain of K on $\mathbb{H}$, is called the *(Petersson) scalar product of these forms.*

Theorem 1.38. *Under the assumptions of the definition, the scalar product has the following properties:*

(1) *It converges absolutely and does not depend on the choice of fundamental domain $D(K)$;*

(2) *The scalar product is independent of the choice of the subgroup K of Γ contained in S;*
(3) *It is linear in F and conjugate linear in F';*
(4) $\overline{(F,\, F')} = (F',\, F)$;
(5) *If F is a cusp form, then $(F,\, F) \geq 0$, and $(F,\, F) = 0$ only if $F = 0$;*
(6) *If $M \in \mathbb{G}^n \cap \mathbb{Q}^{2n}_{2n}$ is a symplectic matrix with positive multiplier and entries in the field $\mathbb{Q}$ of rational numbers, then*

$$(F|_k M,\, F'|_k M) = \mu(M)^{n(k-n-1)}(F,\, F'), \tag{1.71}$$

where the functions $F|_k M$ and $F'|_k M$ are considered as elements of the space $\mathfrak{M}_k\left(M^{-1}SM,\, \chi_M\right)$ with the character χ_M defined by (1.34).

Proof. The first property follows from (1.68) and Lemma 1.37.

In order to prove the second property, let us assume that K_1 is another congruence subgroup of Γ contained in S. Then on replacing K_1 by $K_1 \cap K$, one can assume that $K_1 \subset K$. Let

$$\Gamma = \bigcup_{\alpha} K' M_\alpha \quad \text{and} \quad K' = \bigcup_{\beta} K'_1 N_\beta \text{with} \quad K'_1 = K_1 \cup (-1_{2n})K_1$$

be decompositions into different left cosets. Then we have

$$\Gamma = \bigcup_{\alpha,\beta} K'_1 N_\beta M_\alpha,$$

and the left cosets are pairwise distinct. It follows from Theorem 1.19 that one can take

$$D(K_1) = \bigcup_{\alpha,\beta} N_\beta M_\alpha \langle \boldsymbol{D}_n \rangle,$$

whence we obtain

$$\nu(K'_1)^{-1} \int_{D(K_1)} \omega_k(F,\, F')(Z) = \nu(K'_1)^{-1} \sum_{\alpha} \sum_{\beta} \int_{N_\beta \langle M_\alpha \langle \boldsymbol{D}_n \rangle\rangle} \omega_k(F,\, F')(Z)$$

$$= \nu(K'_1)^{-1} [K' : K'_1] \sum_{\alpha} \int_{M_\alpha \langle \boldsymbol{D}_n \rangle} \omega_k(F,\, F')(Z),$$

where we have also used relations (1.68). Again by Theorem 1.19, the last expression is equal to

$$\nu(K'_1)^{-1} \int_{D(K)} \omega_k(F,\, F')(Z),$$

that proves the property (2).

The properties (3), (4), and (5) follow directly from the definition.

In order to prove (1.71), we note that, since all entries of M are rational, the group $M^{-1}SM$ is again a congruence subgroup of $\mathbb{S}$, and so the groups

$$K_M = \Gamma \bigcap M^{-1}KM \quad \text{and} \quad K_{(M)} = K \bigcap K_M = K \bigcap M^{-1}KM$$

are both congruence subgroups of Γ and therefore are both of finite index in Γ. It follows from Lemma 1.20, the part (2), and (1.67) that

$$(F|_k M,\, F'|_k M) = \nu\left(K'_{(M)}\right)^{-1} \int_{D(K_(M))} \omega_k\left(F|_k M,\, F'|_k M\right)(Z)$$

$$= \mu(M)^{n(k-n-1)} \nu\left(K'_{(M)}\right)^{-1} \int_{D(K_{(M)})} \omega_k(F,\, F')\left(M\langle Z\rangle\right)$$

$$= \mu(M)^{n(k-n-1)} \nu\left(K'_{(M)}\right)^{-1} \int_{M\langle D(K_{(M)})\rangle} \omega_k(F,\, F')(Z),$$

where $K'_{(M)} = K_{(M)} \cup (-1_{2n})K_{(M)}$ and $D\left(K_{(M)}\right)$ is a fundamental domain for $K_{(M)}$. It is clear that the set $M\langle D\left(K_{(M)}\right)\rangle$ is a fundamental domain for the group $MK_{(M)}M^{-1} = MKM^{-1} \cap K = K_{(M)^{-1}}$. Hence, again by property (2), we can rewrite the last expression in the form

$$\mu(M)^{n(k-n-1)} \nu\left(K'_{(M)}\right)^{-1} \nu\left(K'_{(M^{-1})}\right) \nu\left(K'_{(M^{-1})}\right)^{-1} \int_{D\langle\left(K_{(M)^{-1}}\right)\rangle} \omega_k(F,\, F')(Z)$$

$$= \mu(M)^{n(k-n-1)} \nu\left(K'_{(M)}\right)^{-1} \nu\left(K'_{(M^{-1})}\right)(F,\, F'),$$

where $K'_{(M^{-1})} = K_{(M^{-1})} \cup (-1_{2n})K_{(M^{-1})}$. In order to prove the relation (1.71), it is sufficient to prove that $\nu\left(K'_{(M)}\right) = \nu\left(K'_{(M^{-1})}\right)$, or that

$$\left[K : K_{(M)}\right] = \left[K : K_{(M^{-1})}\right] \tag{1.72}$$

for every matrix M of $\mathbb{G}$ with rational entries. Let D be a fundamental domain for the group $K_{(M)}$. Since $K_{(M^{-1})} = MK_{(M)}M^{-1}$, it follows that one can take the set $M\langle D\rangle$ as a fundamental domain for $K_{(M^{-1})}$. Then Theorem 1.19 implies the following relations for the invariant volumes of the domains D and $M\langle D\rangle$:

$$v(D) = \left[K : K_{(M)}\right] v(D(K)), \quad v(M\langle D\rangle) = \left[K : K_{(M^{-1})}\right] v(D(K)),$$

which inplies (1.72), since $v(D) = v(M\langle D\rangle)$. $\triangle$

Exercise 1.39. *Show that the Eisenstein series* $E_k(z)$ *defined in Exercise* 1.32 *is orthogonal to the space* $\mathfrak{N}_k(\Gamma^1)$ *of cusp forms of weight* k *for* Γ^1*.*

[Hint: Note that

$$E_k(z) = (1 + (-1)^k)\zeta(k) \sum_{M \in \Gamma_0^1 \backslash \Gamma^1} j(M,\, z)^{-k},$$

where $j(M,\, z)$ is defined by (1.30) and $\Gamma_0^1 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma^1 \right\}$, which allows one to rewrite the scalar product of $E_k(z)$ on a cusp form as integral over a fundamental domain for the group Γ_0^1, say, $\{z = x + iy \in \mathbb{H}^1 \,\big|\, -1/2 \le x \le 1/2\}$.]