수 학 강 의 록 제 9 권

Topics in Algebra, Algebraic Geometry and Number Theory II

Edited by
JAE MOON KIM

서 울 대 학 교
수학연구소 · 대역해석학연구센터

Notes of the Series of Lecture
held at the Seoul National University

Jae. Moon Kim(ed), Inha University

펴낸날 : 1993년 2월 20일
편집인 : 김 재 문
펴낸곳 : 서울대학교 수학연구소 · 대역해석학연구센터 〔TEL : 02-880-6530〕
인 쇄 : 도서출판 풍남〔TEL : 274-7800(대), 1128〕

Preface

This lecture note is based on the seminars in 1991 at Seoul National University and Ewha Womans University. Since the seminars were aimed to facilitate communications among the members of the seminar group on various areas in number theory, most topics in this book are introductory. Thus we hope this book along with the first volume of our lecture note series could give opportunities for graduate students interested in number theory to take several branches of number theory.

We thank the Research Institute of Mathematics at Seoul National University, especially professor O.K. Yoon, the director of RIM. for financial support. We also want to express special thanks to those algebraists at Seoul National University and Ewha Womans University who showed great concern to our seminar group by encouraging and participating seminars. Our thanks also go to S.M. Kim for his TEXing our manuscript.

Authors.

Contents

Heights

Sung Sik Woo

Department of Mathematics
Ewha Woman's University
Seoul 120 – 750, Korea

Contents

1 . Basic Properties of Heights.

Let K be a field. An absolute value v on K is said to be *proper* if

(i) for any finite extension E of K, we have

$$[E : K] = \sum_{w|v} [E_w : K_v]$$

where the sum is taken over all extension of w of v,

(ii) if $\mathrm{char} K = 0$, then the restriction to $\mathbb{Q}$ is either trivial, ordinary absolute value or p–adic absolute value.

A set M_K of absolute values on K is said to be *proper* if

(i) every absolute value in M_K are proper,

(ii) two distinct absolute values are indenpendent, *i.e,* they define different topology,

(iii) for any nonzero element x of K, there are only finitely many v in M_K such that $|x|_v \neq 1$,

(iv) satisfies the product formula, *i.e,* for $x \in K$ we have

$$\prod_{v \in M_K} |x|_v = 1.$$

Let E/K be a finite extension. We will denote M_E the set of all extensions of M_K. If M_K is a proper set of absolute values of K, then so is M_E. We will be interested in the following two cases.

Case 1. Let $K = \mathbb{Q}$. For primes p, ℓ, we define

$$|\ell|_p = \begin{cases} 1 & \text{if } p \neq \ell, \\ 1/\ell & \text{if } p = \ell. \end{cases}$$

Then $M_{\mathbb{Q}}$ which consists of all $|\ |_p$ together with the ordinary absolute value is a proper set of absolute values.

If K is a number field, then M_K consists of all extensions of $M_{\mathbb{Q}}$; for $x \in K$, and for a finite prime $\wp$,

$$\|x\|_\wp = \left(\frac{1}{\mathrm{N}(\wp)}\right)^{ord_\wp(x)}$$

where $\mathrm{N}(\wp) = [\mathcal{O}_{K/\wp} : \mathbb{Z}/p]$. If $v = \infty$,

$$\|x\|_v = |x|_{\sigma_v}^{\varepsilon_v}$$

where $\varepsilon_v = 1, 2$ depending on whether σ_v is a real or complex emmbeding.

Case 2. Let K be a perfect field, W be a projective variety in $\mathbb{P}^n$ nonsingular in codimension one *i.e*, for any irreducible subvariety $\wp$ of W, $\mathcal{O}_{W,\wp}$ is a discrete valuation ring. Let c be a real with $0 < c < 1$. Let $K = k(W)$, the function field of W, and M_K be the set of absolute values defined by

$$|x|_\wp = c^{ord_\wp(x)\deg(\wp)}, \quad x \in K$$

for each prime (=irreducible) divisors $\wp$ of W which is defined over k. Here we remark that $\deg(\wp)$ depends on the projective emmbeding of W in $\mathbb{P}^n$. The set of absolute values M_K is proper.

For a divisor $D = \sum n_\wp \wp$, we will use the notation

$$\mathrm{Deg}_\wp(D) = n_\wp \cdot \deg(\wp) = \mathrm{ord}_\wp(D) \cdot \deg(\wp).$$

Let K be a field with a proper set of absolute values M_K. The projective space $\mathbb{P}_K^n$ consists of the points

$$(x_0, \ldots, x_n), \ x_i \in K, \ \text{ not all } x_i \text{ are zero},$$

with the identification $(x_0, \ldots, x_n) = (\alpha x_0, \ldots, \alpha x_n)$ for nonzero α in K. For $P = (x_0, \ldots, x_n) \in \mathbb{P}_K^n$, we define the (multiplicative) *height* of P relative to M_K by

$$H_K(P) = \prod_{v \in M_K} \sup_i \|x_i\|_v.$$

Note that $H_K(P)$ does not depend on the choice of coordinates by the product formula. When K is a number field (respectively, function field) the *logarithmic height* is defined by

$$h_K(P) = \log H_K(P)$$

where log is the usual logarithm (respectively, log with base $1/c$).

Proposition 1. Let $K \subset F \subset E$ be finite extensions with their proper set of absolute values. For $P \in \mathbb{P}^n_K$, we have

$$H_E(P) = H_F(P)^{[E:F]}.$$

Proof. For $w \in M_E$, $v \in M_F$, let $N_w = [E_w : K_w]$, and $N_v = [F_v : K_v]$. Since $N_w = [E_w : F_w]N_v$, we have

$$\sum_{w|v} N_w = N_v \sum_{w} [E_w : F_w] = N_v[E : F].$$

Therefore we have,

$$\begin{aligned} H_E(P) &= \prod_{v \in M_F} \prod_{w|v} \sup_i |x_i|_w^{N_w} = \prod_{v \in M_F} \sup_i |x_i|^{\left(\sum N_w\right) N_v} \\ &= \Big(\prod_{v \in M_F} \sup_i |x_i|^{N_v} \Big)^{[E:F]} = H_F(P)^{[E:F]}. \end{aligned}$$

■

Proposition 2. Let $K = k(W)$ where W is a projective variety in $\mathbb{P}^n$ nonsingular in codimension 1. Let $(y_0, \ldots, y_n) \in \mathbb{P}^n_K$ and let

$$H_K(P) = \left(\frac{1}{c}\right)^d.$$

Proof. We may assume that one of the y_i is equal to 1. In the product defining the height, we will have a nontrivial contribution if $\wp$ is a pole of one of y_i. For such a pole $\wp$, we have

$$\begin{aligned} \sup_i c^{(ord_\wp y_i)\deg(\wp)} &= \sup_i \left(\frac{1}{c}\right)^{-(ord_\wp y_i)(\deg \wp)} \\ &= \left(\frac{1}{c}\right)^{\sup_i(-\mathrm{ord}_\wp y_i)(\deg \wp)}. \end{aligned}$$

Now our assertion is obvious. ■

If $P \in \mathbb{P}^n_{\bar{K}}$ and $P \in \mathbb{P}^n_F$ for some finite extension F of K, then we define the *absolute height* by

$$H(P) = H_F(P)^{1/[E:F]}.$$

The *logarithmic height* (or simply *height*) is defined, as before,

$$h(P) = \log H(P)$$

where log is taken with a proper base. Note that $H(P) \geq 1$ since we can always choose one of the coordinates to be 1.

Let F/K be a finite extension and σ be an emmbeding of F over K, then we have

$$H_F(P) = H_{F^\sigma}(P^\sigma).$$

Therefore we have $H(P) = H(P^\sigma)$.

For $x \in K$, we define its height by the height of $(1, x) \in \mathbb{P}^1_K$, *i.e*,

$$H(x) = \prod_{v \in M_K} \sup(1, \|x\|_v).$$

If $0 \neq x \in K$, then by the product formula we have

$$H(x) = H(x^{-1}),$$

and for a positive integer n, we have

$$H(x^n) = H(x)^n.$$

Further since $\sup(1, \|xy\|_v) \leq \sup(1, \|x\|_v)\sup(1, \|y\|_v)$ we have

$$H(xy) \leq H(x)H(y).$$

2 . Number field Case

Let $K = \mathbb{Q}$, $\alpha \in \mathbb{Q}$, $\alpha = a/b$ where a, b are relatively prime. Then we have

$$H\left(\frac{a}{b}\right) = H(b, a) = \prod_p \sup(|a|_p, \ |b|_p) = \sup(|a|, \ |b|).$$

The last equality is true because for $p < \infty$, $|a|_p \leq 1$, $|b|_p \leq 1$ and one of them $= 1$.

More generally, if $P = (x_0, \ldots, x_n) \in \mathbb{P}^n_{\mathbb{Q}}$ where x_i are relatively prime, then

$$H_{\mathbb{Q}}(P) = \sup_i |x_i|.$$

Therefore if b is a positive number then $\left\{P \in \mathbb{P}^n_{\mathbb{Q}} |\ H(P) < b\right\}$ is a finite set. Now suppose K is a number field, $P = (x_0, \ldots, x_n) \in \mathbb{P}^n_K$. We may assume x_i are algebraic integers. As in the case for $\mathbb{Q}$, we have

$$H_K(x) = \prod_{v \in S_\infty} \sup_i \|x_i\|_v$$

where S_∞ is the set of infinite places.

Proposition 3. If $0 \neq \alpha \in K$ with $(\alpha) = \mathfrak{a}/\mathfrak{b}$ where $\mathfrak{a}$, $\mathfrak{b}$ are relatively prime ideals, then

$$H_K(\alpha) = N(\mathfrak{b}) \prod_{v \in S_\infty} \sup(1, \|\alpha\|_v).$$

More generally if $\mathfrak{a}$ is the fractional ideal generated by $x_0, \ldots, x_n$ in K, then the height $P = (x_0, \ldots, x_n) \in \mathbb{P}^n_K$ is given by

$$H_K(P) = N(\mathfrak{a})^{-1} \prod_{v \in S_\infty} \sup \|x_i\|_v.$$

Proof. It suffice to show $\prod_{p < \infty} \sup(1, \|\alpha\|_p) = N(\mathfrak{b})$. We have $\|\alpha\|_p > 1$ if and only if $p | \mathfrak{b}$. Write

$$(\alpha) = \mathfrak{a} \Big/ \prod p_i^{e_i} = \mathfrak{a} \Big/ \Big(\prod \pi_i^{e_i} \Big)$$

where π_i is a local paramater at p_i. Then

$$\left\| \frac{1}{\pi} \right\|_p = \left| \frac{1}{\pi} \right|_p^{N_p} = p^{f_p} = N(p). \qquad \blacksquare$$

Proposition 4. Let K be a number field and $x \in K$ be nonzero. Then $H(x) = 1$ if and only if x is a root of 1.

Proof. If x is a root of 1, then trivially we have $H(x) = 1$. Conversely suppose $H(x) = 1$. Then for a finite place v, we have $\|x\|_v \leq 1$; hence $x \in \mathcal{O}_K$. If v is an infinite place, we also have $\|x\|_v \leq 1$. Hence the coefficients of the irreducible polynomial and its degree is bounded. Therefore such x's are a finite subgroup of $K^\times$. Hence x is a root of unity. $\blacksquare$

Theorem 1. If $c, d > 0$ are constants, then

$$\left\{P = (x_0, \ldots, x_n) \in \mathbb{P}^n_{\overline{\mathbb{Q}}} \mid H(P) < c, [\mathbb{Q}(P) : \mathbb{Q}] < d \right\}$$

is a finite set.

Proof. We already know this for $\mathbb{Q}$–points. If $H(P) < c$ and $[\mathbb{Q}(P) : \mathbb{Q}] < d$, then $H(x_i) < c$ and $[\mathbb{Q}(x_i) : \mathbb{Q}] < d$. Hence it suffices to show that the set

$$\left\{ (1, x) \in \mathbb{P}^1_{\overline{\mathbb{Q}}} \mid H(x) < c,\ [\mathbb{Q}(x) : \mathbb{Q}] = d \right\}$$

is finite. Let $x_1, \ldots, x_d$ be the conjugates of x, and $1 = s_0, s_1, \ldots, s_d$ be the elementary symmetric polynomials of x_i. We have

$$f(t) = \sum (-1)^i s_i t^{d-i} = \prod (t - x_i)$$

is the irreducible polynomial of x over $\mathbb{Q}$. Since f is determined by $s_0, \ldots, s_d$ and $H(s_i)$ are bounded, there are only finitely many possible f's. Hence there are only finitely many x's with bounded height and bounded extension degree, as desired. ∎

3 . Geometry of heights

Let K be field, M_K a proper set of absolute values of K. Let V be a normal projective variety over K. Let λ, λ' be real valued functions on a set of points on V. We say that λ and λ' are (*multiplicatively*) *equivalent* if there are constants c_1 and c_2 such that

$$c_1 \lambda(P) \leq \lambda'(P) \leq c_2 \lambda(P),$$

for all points P of our consideration. Taking logarithm, we say that λ, λ' are (*additively*) *equivalent* if $\lambda - \lambda'$ is a bounded function. If this is the case,we will use notation

$$\lambda \sim \lambda'.$$

Let V be a variety defined over K, and let $\varphi: V \to \mathbb{P}^n$ be a morphism defined over K. Since the morphism φ is defined over K, the image of the set of all K–points V_K is in $\mathbb{P}^n_K$. For $P \in V_K$, we have

$$H_{K,\varphi}(P) = H_K(\varphi(P)) \qquad \text{and} \qquad H_\varphi(P) = H(\varphi(P)).$$

Their logarithmic heights will be denoted by $h_{K,\varphi}$ and h_φ, respectively. If $f{:}U \to V$, $g{:}V \to \mathbb{P}^n$ are morphisms, then trivially we have

$$H_{g\circ f} = H_g \circ f \qquad \text{and} \qquad h_{g\circ f} = h_g \circ f.$$

Let $V \subseteq \mathbb{P}^n$ be a variety over K and let $A = (a_{ij})(0 \le i \le m,\ 0 \le j \le n)$ with $a_{ij} \in K$. Corresponding to A we define a rational map

$$A{:}V \to \mathbb{P}^m$$

by sending $P = (x_0, \ldots, x_n)$ to AP given by matrix multiplication. We call this map a *linear projection* defined by A.

Proposition 5. Let V be a projective variety in $\mathbb{P}^n$ over K. If $\varphi{:}V \to \mathbb{P}^n$ is a linear projection, then there is a constant c (depending only on φ) such that

$$H_\varphi(P) \le cH(P)$$

for all $P \in V_{\overline{K}}$ on which φ is defined.

Proof. Let φ be defined by the matrix (a_{ij}). Let S_K be the set of all v such that $|a_{ij}|_v \ne 1$ for some a_{ij} or v is an infinite place. Let $P = (x_0, \ldots, x_n) \in \mathbb{P}^n_F$ where F is a finite extension of K, and let $y_i = \sum_{j=0}^{n} a_{ij}x_j$. For $w \in M_F$ over $v \in S_K$, we have

$$|y_i|_w \le \sum |a_{ij}|_w |x_j|_w \le \left[(n+1)\sup_{i,j}\left(|a_{ij}|_v, 1\right)\right] \sup_j |x_j|_w.$$

Letting $c_v = (n+1)\sup_{i,j}\left(|a_{ij}|_v, 1\right)$, we have

$$\sup |y_i|_w \le c_v \sup_j |x_j|_w.$$

For $v \notin S_K$, since $|a_{ij}|_v = 1$, we have

$$|y_i|_w \le \sum |x_j|_w \le \sup_j |x_j|_w$$

where $w \in M_F$ is over v. Hence

$$\sup_i |y_i|_w \le \sup_j |x_j|_w.$$

Therefore if we set $c = \Big[\prod_{v\in M_K}\prod_{w|v} c_v^{N_v}\Big]^{1/[K:F]}$, then we have

$$H_\varphi(P) \le cH(P).$$

■

Let $f{:}V \to \mathbb{P}^n$, $g{:}V \to \mathbb{P}^m$ be two morphisms. Let $f = (f_0, \dots, f_n)$, $g = (g_0, \dots, g_m)$. We define

$$f \otimes g{:}V \to \mathbb{P}^{(n+1)(m+1)-1} \quad \text{by} \quad (f \otimes g)_{ij} = f_i g_j.$$

Then we have

$$H_{f\otimes g} = H_f H_g \qquad \text{and} \qquad h_{f\otimes g} = h_f + h_g.$$

These follow from the equality,

$$\sup_{i,j} |x_i y_j|_v = \sup_i |x_i|_v \sup_j |y_j|_v.$$

In particular, if $\varphi{:}\mathbb{P}^n \to \mathbb{P}^N$ is given by $(M_0, \dots, M_N)$ be the monomials of degree d in $x_0, \dots, x_n$, then

$$H_\varphi = H^d \qquad \text{and} \qquad h_\varphi = dh.$$

Proposition 6. Let $f_0, \dots, f_n$ be homogeneous polynomials of degree d in $x_0, \dots, x_n$. Let $f = (f_0, \dots, f_n)$ be a rational map on $\mathbb{P}^n$ to $\mathbb{P}^m$. For $P \in \mathbb{P}^n_{\overline{K}}$ on which f is defined, we have

$$h_f(P) \le dh(P) + c_1$$

for some constant c_1 independent of x.

Proof. We will omit the routine of the dependence of the field. We estimate

$$H(f(P)) = \prod_v \sup_i |f_i(P)|_v \le \prod_v c \sup |x_i|_v^d = cH(P)$$

where c is a constant depending on the number of monomials of f's and their coefficients. ■

Proposition 7. Let $V \subseteq \mathbb{P}^n$ be locally closed with respect to Zariski topology. If $f{:}V \to \mathbb{P}^m$ is a morphism over K, then there are constants c_1, c_2 such that

$$h_f \leq c_1 h + c_2.$$

Proof. By compactness of V, it suffices to prove the statement locally. Near a point $P \in V$, f is represented in the form

$$f = (\varphi_0, \ldots, \varphi_m), \quad \varphi_0 = 1,$$

where $\varphi_i = f_i/f_0$ $(i = 0, \ldots, m)$ and f_i are homogeneous polynomials of the same degree in $x_0, \ldots, x_n$. Then we have

$$H_\varphi(P) = \prod_v \sup_i |\varphi_i(P)|_v = \prod_v \frac{\sup_i f_i(P)}{|f_0(x)|_v} \leq cH(P)^d.$$

Here in the second equality we used the product formula, $\prod_v |f_0(x)|_v = 1$. ∎

Theorem 2. Let $f{:}\mathbb{P}^n \to \mathbb{P}^N$ be a morphism of degree d, *i.e*, $f = (f_0, \ldots, f_N)$ where f_i are homogeneous of degree d. Then we have

$$h_f \sim dh.$$

Proof. One inequality was proved in Proposition 7. We need to show $H(P) \leq cH(f(P))$. Since f is a morphism, the set of common zeros of $f_1, \ldots, f_N$ is the origin. By Hilbert Nullstellensatz, there are $g_{ij} \in K[x_0, \ldots, x_n]$ such that

$$x_i^{m+d} = \sum g_{ij} f_j \quad \text{for some} \quad m > 0.$$

We may assume g_{ij} are also homogeneous of degree m since we can discard those monomials of degree$\neq m$. Further by multiplying some c which is integral in K, we may assume the coefficients of g_{ij} in $cx_i^{m+d} = \sum g_{ij} f_j$ are integral in K. Let $P = (x_0, \ldots, x_n) \in \mathbb{P}^n_K$ with x_i integral in K.

If $v \in M_K$ is non-archimedian, then

$$|c|_v \left|x_i^{m+d}\right|_v = \left|\sum g_{ij}(P) f_j(P)\right|_v \leq \max_j |g_{ij}(P)|_v \, |f_j(P)|_v .$$

Since g_{ij} are homogeneous polynomials of degree m with integral coefficients, we have

$$|g_{ij}(P)|_v \leq \max_i |x_i|_v^n.$$

Hence we get

$$\max_i |c|_v \left|x_i^{m+d}\right|_v \leq \max_{i,j} |x_i|_v^m |f_j(P)|_v.$$

Now let v be an archimedian place. We estimate,

$$\left|cx_i^{m+d}\right| \leq \sum_j |g_{ij}(P)|\,|f_j(P)| \leq C_1 |x_i|^m \max_j |f_j(P)|$$

where C_1 is a constant depending on the coefficients of g_{ij} and number of monomials in g_{ij}. Hence we get

$$|c|\max|x_i|^{m+d} \leq C_1 \max_i |x_i|^m \max_j |f_j(P)|.$$

Now take N_v–th power and then take the product over all v to get

$$H_K(P)^{m+d} \leq cH_K(P)^m H_K(f(P)),$$

as contented. ∎

3.1. Line Bundles and Divisors

Let V be a projective variety over a field K. To fix the idea we assume V is nonsingular. A *line bundle* L consists of the following datum ; there is an (affine) open covering $\{U_i\}$ of V and isomorphisms

$$f_i : L|_{U_i} \to \mathcal{O}_{U_i}.$$

Write $U_{ij} = U_i \bigcap U_j$ and $f_{ij} = (f_i|_{U_{ij}}) \circ (f_j|_{U_{ij}})^{-1}$. Then f_{ij} is an isomorphism

$$f_{ij} : \mathcal{O}_{U_{ij}} \to \mathcal{O}_{U_{ij}}.$$

Hence f_{ij} can be considered as a unit on U_{ij} ; $f_{ij} \in \mathcal{O}_{U_{ij}}^{\times}$. For these isomorphisms, we get the following cocycle condition,

$$f_{ii} = \mathrm{id}, \qquad f_{ij} f_{jk} = f_{ik}.$$

Hence $\{f_{ij}\}$ gives rise to an element of $H^1(V, \mathcal{O}_V^{\times})$. In fact, the map so described is isomorphism,

$$\left\{ \begin{array}{l} \text{Isomorphism class of} \\ \text{line bundles under } \mathcal{O} \end{array} \right\} \xrightarrow{\cong} H^1(V, \mathcal{O}^{\times}).$$

If $L_1 = \{f_{ij}\}$, $L_2 = \{g_{ij}\}$, then under the isomorphism above $L_1 \otimes L_2$ corresponds to the cocycle $\{f_{ij}g_{ij}\}$.

A *Cartier divisor* D consists of $\{(U_i, f_i)\}$ where $\{U_i\}$ is an open cover of V and $f_i \in k(U_i) = k(V)$, and such that $f_i/f_j \in \mathcal{O}_{U_{ij}}^{\times}$ *i.e*, a Cartier divisor is a global section of $\mathcal{K}^{\times}/\mathcal{O}_V^{\times}$ where $\mathcal{K}$ is the sheaf of total ring of quotients of V. We can view a Cartier divisor as an $\mathcal{O}_V$–subsheaf of $\mathcal{K}^{\times}$ locally generated by f_i. A Cartier divisor is said to *principal* if D is globally given by a rational function. If $D = \{(U_i, f_i)\}$ is a Cartier divisor, then we can associate a line bundle $L(D)$ which is given by

$$L(D)\Big|_{U_i} = f_i^{-1}\mathcal{O}_{U_i}.$$

In terms of cocycle, $L(D)$ is given by $\{f_{ij} = f_i/f_j\}$. For a nonsingular variety V, it is known [H] that the map so described is an isomorphism,

$$\left\{\begin{array}{c}\text{Cartier divisors on } V\\ \text{modulo principal divisors}\end{array}\right\} \xrightarrow{\cong} \left\{\begin{array}{c}\text{Isomorphism classes}\\ \text{of line bundle}\end{array}\right\}.$$

A *Weil divisor* is a formal sum $\sum n_i D_i$ where $n_i \in \mathbb{Z}$ and D_i is an irreducible divisor on V. A *principal Weil divisor* is, by definition, a divisor of a rational function. If $D = (U_i, f_i)$ is a Cartier divisor, we can associate a Weil divisor by

$$(U_i, f_i) \longmapsto \sum_Y v_Y(f_i)Y$$

where the sum is taken over the irreducible divisors Y and i can be chosen any index such that $U_i \bigcap Y \neq \emptyset$. Then one can check this is a well defined map. For a nonsingular V (more generally for locally factorial), this association is an isomorphism,

$$\{\text{ Cartier divisors }\} \xrightarrow{\cong} \{\text{ Weil divisors }\}.$$

Under this isomorphism, principal divisors correspond to principal divisors. Finally we have isomorphisms

$$\left\{\begin{array}{c}\text{Weil divisors}\\ \text{modulo principal}\\ \text{divisors}\end{array}\right\} \xleftarrow{\cong} \left\{\begin{array}{c}\text{Cartier divisors}\\ \text{modulo principal}\\ \text{divisors}\end{array}\right\} \xrightarrow{\cong} \left\{\begin{array}{c}\text{Isomorphism classes}\\ \text{of line bundle}\end{array}\right\}.$$

Example. Let $V = \mathbb{P}^n_K$, and let $U_i = \{P = (x_0, \ldots, x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$. The line bundle $\mathcal{O}_V(1)$ is defined by

$$\mathcal{O}_V(1)|_{U_i} = x_i \mathcal{O}_{U_i},$$

i.e, the section of $\mathcal{O}_V(1)$ on U_i is of the form

$$\frac{f(x_0, \ldots, x_n)}{x_i^{m-1}}$$

where f is a homogeneous polynomial of degree m. In terms of cocycle $\mathcal{O}_V(1)$ is given by $\{x_i/x_j\}$.

Consider the Cartier divisor $\left(U_i, \frac{x_0}{x_i}\right)$ $(i = 0, 1, \ldots, n)$. The corresponding Weil divisor is

$$\sum_Y v_Y\left(\frac{x_0}{x_i}\right) Y = Y_0$$

where Y_i $(i = 0, \ldots, n)$ is the hyperplane given by $x_i = 0$. Also note that the divisor $Y_i - Y_j$ is a principal divisor. The line bundle corresponding to the Cartier divisor is given by

$$\left\{ f_{ij} = \frac{x_0/x_i}{x_0/x_j} = \frac{x_j}{x_i} \right\}$$

which is $\mathcal{O}_V(1)$ describe as above. We define $\mathcal{O}_V(k)$ to be the k-fold tensor product of $\mathcal{O}_V(1)$. For example a Cartier divisor which coresponds to $\mathcal{O}_V(k)$ can be given by $\left(U_i, \frac{x_0^k}{x_i^k}\right)$ $(i = 0, \ldots, n)$.

A Weil divisor D is said to be *linearly equivalent* to 0 if D is the divisor of a rational function. Two divisors D_1 and D_2 are linearly equivalent (written $D_1 \sim D_2$) if $D_1 - D_2$ is linearly equivalent to 0. As we noted before two divisors D_1 and D_2 are linearly equivalent if and only if $L(D_1)$ and $L(D_2)$ are isomorphic. Intuitively, D_1 and D_2 are linearly equivalent if D_1 and D_2 can be parametrized by $\mathbb{P}^1$. In fact, these two notions are equivalent. See [F] for more details.

An effective (positive) Weil divisor D ($D = \sum n_i D_i$ with $n_i \geq 0$ and D_i are irreducible divisors) is said to be *algebraically equivalent* to 0 if there is a nonsingular variety T and a divisor D on $V \times T$ such that $D = D(t_0) - D(t_1)$ for some $t_0, t_1 \in T$. It is known that we may restrict T to be a nonsingular curve. Since we can choose T to be $\mathbb{P}^1$, we see that linear equivalence implies

algebraic equivalence. Arbitrary divisors D_1 and D_2 are said to be *algebraically equivalent* if there is a divisor E such that $D_1 + E$ and $D_2 + E$ are effective and they are algebraically equivalent. The equivalence relation on $\mathrm{Div}(V)$, the set of all divisors, generated by algebraic equivalence just described is denoted by $\equiv$. For more details see [F].

We have a chain of subgroups

$$\mathrm{Div}_\ell(V) \subseteq \mathrm{Div}_a(V) \subseteq \mathrm{Div}(V)$$

where $\mathrm{Div}_\ell(V)$ (respectively, $\mathrm{div}_a(V)$) is the group of divisors linearly (algebraically) equivalent to 0. The group $\mathrm{Div}(V)/\mathrm{Div}_a(V)$ is called the *Néron–Severi group* which is denoted by $NS(V)$. It is known that $NS(V)$ is a finitely generated abelian group. The group $\mathrm{Div}(V)/\mathrm{Div}_\ell(V)$, denoted by $\mathrm{Pic}^0(V)$, is called the *Picard variety* of V, which is an abelian variety over K. For more details we refer [F].

To get intuitive idea, let's consider the case $K = \mathbb{C}$. We have the exponential sequence,

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_V \xrightarrow{\exp} \mathcal{O}_V^\times \longrightarrow 0$$

which gives us an exact sequence

$$0 \longrightarrow \mathrm{H}^1(V, \mathbb{Z}) \longrightarrow \mathrm{H}^1(V, \mathcal{O}_V) \longrightarrow \mathrm{H}^1(V, \mathcal{O}_V^\times) \xrightarrow{c_1} \mathrm{H}^2(V, \mathbb{Z}).$$

We quote the facts [G-H] :

(1) Two divisors are algebraically equivalent if and only if they are homologous.

(2) (Lefeschetz (1,1) theorem) A cycle in $H^2(V, \mathbb{Z})$ comes from an algebraic cycle if and only if it belongs to $H^{1,1}(V)$.

Hence we have

$$\text{Image of } c_1 = H^{1,1}(V) \bigcap H^2(V, \mathbb{Z}).$$

In particular, we see that $NS(V)$ is finitely generated. We also have

$$\mathrm{Pic}^0(V) = H^1(V, \mathcal{O}_V)/H^1(V, \mathbb{Z}).$$

3.2. Line bundles and Morphism

Let L be a line bundle on V. We say that the global sections $\{s_0, \ldots, s_n\}$ *generate* L if $\{s_0(x), \ldots, s_n(x)\}$ generate L_x as $\mathcal{O}_{V,x}$-module for all $x \in V$. Since L is a line bundle, this is samething to say that the sections $s_0, \ldots, s_n$ have no common vanishing points. Let $\varphi_i : L|_{U_i} \to \mathcal{O}_{U_i}$ be an isomorphism giving the line bundle, and let $x \in U_i$. We define

$$U_i \longrightarrow \mathbb{P}^n \text{ by sending } x \text{ to } (\varphi_i(s_0(x)), \ldots, \varphi_i(s_n(x))).$$

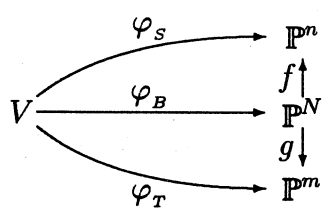
If $x \in U_i \bigcap U_j$, then since $\varphi_{ij}(x) \in \mathcal{O}_{V,x}^{\times}$, we see that $(\varphi_i(s_0(x)), \ldots, \varphi_i(s_n(x)))$ and $(\varphi_j(s_0(x)), \ldots, \varphi_j(s_n(x)))$ differ by a nonzero constant $\varphi_{ij}(x)$. Hence we get a map $V \to \mathbb{P}^n$. Conversely, if $\varphi : V \to \mathbb{P}^n$ is a morphism, then $\varphi^* \mathcal{O}_{\mathbb{P}^n}(1)$ is a line bundle with the set of sections $\varphi^*(x_0), \ldots, \varphi^*(x_n)$ which generates $\varphi^* \mathcal{O}_{\mathbb{P}^n}(1)$ and gives rise to the morphism φ. Hence we have shown,

Proposition 8. Giving a morphism $V \to \mathbb{P}^n$ is the samething as giving a line bundle L and a set of global sections $\{s_0, \ldots, s_n\}$ which generates L.

3.3. Ampleness

A line bundle L is said to be *very ample* if there is an embedding $\varphi : V \to \mathbb{P}^n$ such that $L \cong \varphi^* \mathcal{O}(1)$. In particular, if L is very ample, then L is generated by sections. A line bundle L is said to be *ample* if L^n (= n-fold tensor product) is a very ample line bundle. A divisor D is said to be *very ample* (respectively, *ample*) if the corresponding line bundles are very ample (respectively, ample).

Let L be a line bundle. Let $S = \{s_0, \ldots, s_n\}$ and $T = \{t_0, \ldots, t_m\}$ be any two sets generating L. If $B = \{b_1, \ldots, b_N\}$ is a base of the global sections $\Gamma(V, L)$, then $s_i = \sum \alpha_{ij} b_j$ and $t_i = \sum \beta_{ij} b_j$ where α_{ij}, β_{ij} are in K. We have a commutative diagram



where f and g are linear projections determined by (α_{ij}) and (β_{ij}). Hence by Proposition 5, we have

Proposition 9. If L is a line bundle and S and T are generating sections of L, then

$$h_{\varphi_S} \sim h_{\varphi_T}.$$

Hence we will simply write φ_L without specifying the generating set of sections. Let L, M be line bundles with the sets of generating sections S and T respectively, then $L \otimes M$ is a line bundle with a set of generating sections $\{s_i t_j\}$ (where the multiplication is done with proper identification with $\mathcal{O}_U$). By the remarks following Proposition 5, we have

$$h_{L\otimes M} \sim h_L + h_M.$$

Now we want to extend the definition of h_L to all line bundles. If L is a line bundle on V, then Serre's theorem [H] says that $L \otimes \mathcal{O}_V(n)$ is generated by sections. We define

$$h_L = h_{L\otimes\mathcal{O}_V(n)} - h_{\mathcal{O}_V(n)}.$$

up to a bounded function. Summing up we have shown,

Theorem 3. Let V be a nonsingular projective variety over a field K. Then there is a unique group homomorphism

$$\mathrm{Pic}(V) \longrightarrow \left\{ \begin{array}{c} \text{Real valued functions on } V(\overline{K}) \\ \text{modulo bounded functions} \end{array} \right\}$$

such that if L is very ample, it corresponds to h_L. Further, if $f{:}V \to W$ is a morphism of varieties defined over K, then

$$h_{f^*L} = h_L \circ f.$$

Two real valued functions λ_1, λ_2 are said to be (multiplicatively) *quasi–equivalent* if given $\varepsilon > 0$, there are constants c_1, c_2 depending on ε such that

$$c_1 \lambda_1^{1-\varepsilon} \leq \lambda_2 \leq c_2 \lambda_1^{1+\varepsilon}.$$

Additive quasi–equivalence is a logarithmic version of this ; for any $\varepsilon > 0$, there are c_1, c_2 such that

$$(1-\varepsilon)\lambda_1 - c_1 \leq \lambda_2 \leq (1+\varepsilon)\lambda_1 + c_2.$$

Theorem 4. Let V be a nonsingular variety over K. If X, Y are ample divisors which are algebraically equivalent, then h_X and h_Y are quasi–equivalent.

For a proof of this, we quote the following fact without proof. For a proof see [L].

Proposition 10. Let V be as in the theorem and X be an ample divisor on V. Then there is a positive integer e such that $eX + Z$ is very ample for all divisor Z which is algebraically equivalent to 0.

Proof of theorem 4. By the above proposition, there is $e > 0$ such that $Z_n = n(X - Y) + eX$ is very ample for all n. Hence

$$(n + e)h_X = nh_Y + h_{Z_n},$$

up to a bounded function. Dividing by n we have

$$\left(1 + \frac{e}{n}\right) h_X = h_Y + \frac{1}{n} h_{Z_n},$$

up to a bounded function. Since $h_{Z_n} \geq 0$, by choosing n so that $\frac{e}{n} < \varepsilon$ we can find c such that

$$c + (1 + \varepsilon)h_X \geq h_Y.$$

The other inequality is obtained by symmetry. ∎

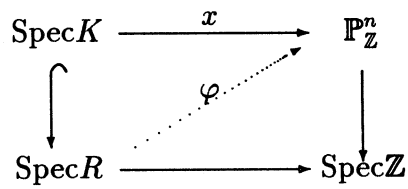
Corollary 1. Let X, Y be ample divisors which are algebraically equivalent. Then

$$\lim_{h_X(P) \to \infty} \frac{h_Y(P)}{h_X(P)} = 1.$$

Corollary 2. Let V be a nonsingular complete curve and X, Y be divisors of degree d, d' respectively. Then h_X and $(d/d')h_Y$ are quasi–equivalent.

3.4. Arakelov's View Point

Let K be a number field and R its ring of integers. For $x \in \mathbb{P}^n_K$, there is unique map φ:Spec$R \to \mathbb{P}^n_{\mathbb{Z}}$ extending the K–point x by properness of $\mathbb{P}^n_{\mathbb{Z}}$:



Example. Let $x = (2,3) \in \mathbb{P}^1_{\mathbb{Q}}$. $\mathbb{P}^1_{\mathbb{Z}}$ is covered by two standard open sets

$$U_1 = \text{Spec}\mathbb{Z}\left[\frac{x}{y}\right] \qquad \text{and} \qquad U_2 = \text{Spec}\mathbb{Z}\left[\frac{y}{x}\right],$$

with the identification on $U_1 \bigcap U_2$ given by

$$\mathbb{Z}\left[\frac{x}{y}\right] \xrightarrow{y/x} \mathbb{Z}\left[\frac{y}{x}\right].$$

Choose an open covering V_1, V_2 of Spec$\mathbb{Z}$;

$$V_1 = \text{Spec}\mathbb{Z}\left[\frac{1}{3}\right] \qquad \text{and} \qquad V_2 = \text{Spec}\mathbb{Z}\left[\frac{1}{2}\right].$$

Define φ_i:$V_i \to U_i$ by giving maps

$$\mathbb{Z}\left[\frac{x}{y}\right] \xrightarrow{\varphi_1} \mathbb{Z}\left[\frac{1}{3}\right] \qquad \text{and} \qquad \mathbb{Z}\left[\frac{y}{x}\right] \xrightarrow{\varphi_2} \mathbb{Z}\left[\frac{1}{2}\right]$$

where$\varphi_1\left(\frac{x}{y}\right) = \frac{2}{3}$, $\varphi_2\left(\frac{y}{x}\right) = \frac{3}{2}$. Then φ_1 and φ_2 coincide on $V_1 \bigcap V_2$, and they glue together to get φ. ∎

Let $\mathfrak{p}$ be a line bundle on R, *i.e*, $\mathfrak{p}$ is a projective module of rank 1. We say that $\mathfrak{p}$ is a *metrized line bundle* if for every $v \in S_\infty$, there is a hermitian metric $\|\cdot\|_v$ on $\mathfrak{p} \otimes_R \mathbb{C}$ (tensor product is taken with respect to the embedding v:$\mathbb{R} \to \mathbb{C}$) such that for complex conjugate embeddings the corresponding metrices are the same. The *degree* of a metrized line bundle $\mathfrak{p}$ is defined by

$$\deg(\mathfrak{p}) = \log\#\left(\mathfrak{p}/pR\right) - \sum_{v \in S_\infty} \varepsilon_v \log\|p\|_v$$

where $p \in \mathfrak{p}$ is a nonzero element, and $\varepsilon_v = 1$ or 2 depending on whether v is real or complex. One checks that this definition is independent of choice of $p \in \mathfrak{p}$ by using the product formula.

On the line bundle $\mathcal{O}(1)$ of $\mathbb{P}^n_{\mathbb{C}}$, we have a metric defined by

$$\|f(x)\|_v = \min_{\substack{0 \le i \le n \\ x_i \neq 0}} \left| \frac{f(x)}{x_i} \right|_v, \quad x = (x_0, \ldots, x_n)$$

where f is a section of $\mathcal{O}(1)$. Let $x \in \mathfrak{p}^n_K$ and φ:Spec$R \to \mathbb{P}^n_{\mathbb{Z}}$ be the corresponding map. Then $\varphi^*\mathcal{O}(1)$ is a metrized line bundle on Spec(R).

Proposition 11. $h(x) = \dfrac{1}{[K:\mathbb{Q}]} \deg \varphi^*(\mathcal{O}(1))$.

Proof. Let $(x_0, \ldots, x_n) \in \mathbb{P}^n_K$. We may assume $x_0 \neq 0$ so $\varphi^*(x_0)$ is a nonzero section of $\varphi^*\mathcal{O}(1)$. For $v \in M_K$, we have

$$\|\varphi^*(x_0)\|_v = \min_{\substack{0 \le i \le n \\ x_i \neq 0}} \left| \frac{x_0}{x_i} \right|_v .$$

On the other hand, since

$$\varphi^*\mathcal{O}(1) = \sum_{i=0}^{n} Rx_i \quad \text{and} \quad \varphi^*\mathcal{O}(1)/x_0R \cong \sum Rx_i/Rx_0 \cong \sum_{i=1}^{n} R\frac{x_i}{x_0}/R$$

we have

$$\#\left(\varphi^*\mathcal{O}(1)/x_0R\right) = N_{K/\mathbb{Q}}\Big(\sum R\frac{x_1}{x_0}\Big)^{-1} = \prod_{v<\infty} \max \left\| \frac{x_i}{x_0} \right\|_v .$$

Therefore,

$$\begin{aligned} \deg\varphi^*\mathcal{O}(1) &= \log\#\left(\varphi^*\mathcal{O}(1)/Rx_0\right) - \sum_{v \in M_\infty} \log \min_i \left\| \frac{x_0}{x_i} \right\|_v \\ &= \sum_{v \in M_K} \log \max_i \left\| \frac{x_i}{x_0} \right\|_v = [K:\mathbb{Q}]h\left(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \\ &= [K:\mathbb{Q}]h(x). \end{aligned}$$

■

4 . Heights on Abelian varieties

Let A be an abelian group. A map h on A to an abelian group where multiplication by 2 map is an isomorphism, is said to be *quadratic* (respectively, *quadratic form*) if

$$\Delta h(x,y) = h(x+y) - h(x) - h(y)$$

is bilinear (respectively, Δh is bilinear and h is even ; $h(-x) = h(x)$). If h is quadratic, then

$$h(x) - \frac{1}{2}\Delta h(x,x)$$

is linear. Hence any quadratic function is a sum of a quadratic form and a linear map. If h is even and $h(0) = 0$, then the linear part must be 0.
A map L on $A \times A$ is called *quasi–bilinear* if

$$\begin{aligned} \Delta_1 L(x,y,z) &= L(x+y,z) - L(x,z) - L(y,z) \qquad \text{and} \\ \Delta_2 L(x,y,z) &= L(x,y+z) - L(x,y) - L(x,z) \end{aligned}$$

are bounded.

Lemma 1. (i) If L is a quasi–bilinear, then there is a unique bilinear map L' such that $L - L'$ is bounded. In fact,

$$L'(x,y) = \lim_{n\to\infty} \frac{L(2^n x, 2^n y)}{4^n}.$$

(ii) If h is quasi–quadratic (*i.e*, Δh is quasi–bilinear), then there are uniquely determined quadratic form q and a linear function ℓ such that $h - q - \ell$ is a bounded function. Furthermore, if h is quasi–even, then $\ell = 0$.

Proof. (i) Let $L_n(x,y) = \frac{L(2^n, 2^n y)}{4^n}$. Then L_n is a Cauchy sequence. Hence converges to $L'(x,y)$. It is easy to check that this is bilinear. For uniqueness, if L'' is another one, then since both are bilinear, $L' - L''$ is unbounded which is a contradiction.
(ii) We can set $q(x) = \lim_{n\to\infty} \frac{h(2^n x)}{4^n}$. ∎

We recall some facts on abelian varieties. For the proofs see [M].

Theorem 5. [Theorem of Square] Let A be an abelian variety over a field K, and L a line bundle on A. For $a \in A(\overline{K})$ let $t_a{:}A \to A$ be the translation by a map. Then we have

$$\left(t_{a+b}^* L\right) \otimes L \simeq t_a^* L \otimes t_b^* L.$$

In terms of divisors, this means that $D_{a+b} + D$ and $D_a + D_b$ are linearly equivalent.

Theorem 6. [Theorem of Cube] Let

$$\pi_1, \pi_2, \pi_3, \pi_{12}, \pi_{13}, \pi_{23}, \pi_{123}{:}A \times A \times A \to A$$

be the maps projecting onto the indicated components and then adding. (e.g, $\pi_{23}(a, b, c) = b + c$ *etc.*) Then

$$\pi_{123}^* L \otimes \pi_{12}^* L^{-1} \otimes \pi_{13}^* L^{-1} \otimes \pi_{23} L^{-1} \otimes \pi_1^* L \otimes \pi_2^* L \otimes \pi_3^* L$$

is isomorphic to the trivial line bundle.

First, we draw consequences of these theorems. Let $c \in \mathrm{Pic}(A)$, $a \in A(\overline{K})$. First note that c_a is algebracally equivalent to c. Hence we have a map

$$\varphi_c{:}A(\overline{K}) \longrightarrow \mathrm{Pic}^0(A)$$

sending a to $c_a - c$. Now the theorem of square implies that φ_c is a group homomorphism.

We quote another fact whose proof we also refer [M].

Proposition 12. Let D be a divisor on an abelian variety A. Then D is algebraically equivalent to zero if and only if $D_a - D$ is linearly equivalent to zero for all $a \in A$.

Therefore we have an exact sequence

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \to \mathrm{Hom}(A, \mathrm{Pic}^0(A)).$$

($\mathrm{Pic}^0(A)$ is called the *dual abelian variety* of A.)

Proposition 13. Let $\alpha, \beta: A \to B$ be homomorphisms of abelian varieties and $c \in \mathrm{Pic}(B)$. Then the map

$$D_c: \mathrm{Hom}(A,B) \times \mathrm{Hom}(A,B) \to \mathrm{Pic}(A)$$

defined by $D_c(\alpha, \beta) = (\alpha+\beta)^*(c) - \alpha^*(c) - \beta^*(c)$ is bilinear.

Proof. We need to show

$$\begin{aligned}&(\alpha_1+\alpha_2+\alpha_3)^*(c) - (\alpha_1+\alpha_2)^*(c)\\ &\quad -(\alpha_2+\alpha_3)^*(c) - (\alpha_1+\alpha_3)^*(c) + \alpha_1^*(c) + \alpha_2^*(c) + \alpha_3^*(c)\end{aligned}$$

is the zero class in $\mathrm{Pic}(A)$. Let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ be a map from $A \times A \times A$ to $B \times B \times B$. Then the above class is the same as

$$\alpha^*(\pi_{123}^*(c) - \pi_{12}^*(c) - \pi_{13}^*(c) - \pi_{23}^*(c) + \pi_1^*(c) + \pi_2^*(c) + \pi_3^*(c)).$$

The theorem of cube implies the class inside the parenthesis is zero. As desired. ∎

Theorem 7. For any $c \in \mathrm{Pic}(A)$, the height h_c is quasi–quadratic. There are unique quadratic form q_c and a linear function ℓ_c such that $\hat{h}_c = q_c + \ell_c$ is equivalent to h_c. That is , there a unique homomorphism

$$\mathrm{Pic}(A) \longrightarrow \left\{ \begin{array}{c} \text{quadratic real valued} \\ \text{functions on } A(\bar{K}) \end{array} \right\}$$

which sends c to its canonical height $\hat{h}_c$. Further, if $\alpha: A \to B$ is a morphism of abelian varieties, then

$$\hat{h}_{\alpha^* c} = \hat{h}_c \circ \alpha.$$

Proof. Apply Proposition 13 with $\pi_{12}, \pi_1, \pi_2: A \times A \to A$, $\pi_{12} = \pi_1 + \pi_2$. We have

$$\begin{aligned}&h_c(P+Q) - h_c(P) - h_c(Q)\\ &\quad = h_{\pi_{12}^*(c)}(P) - h_{\pi_1^*(c)}(P,Q) - h_{\pi_2^*(c)}(P,Q)\\ &\quad = h_{\pi_{12}^*(c)-\pi_1^*(c)-\pi_2^*(c)}(P,Q).\end{aligned}$$

Now Proposition 13 implies that $\pi_{12}^*(c) - \pi_1^*(c) - \pi_2^*(c)$ is zero in $\mathrm{Pic}(A)$. To prove functoriality note that $\hat{h}_{\alpha^* c} = \hat{h}_c \circ \alpha + O(1)$, by Theorem 3. Hence $O(1)$ is a bounded quadratic function which must be zero. ∎

The sum $\hat{h}_c = q_c + \ell_c$ which is uniquely determined by c is called the *Néron–Tate height* or the *canonical height.* Now we derive some easy consequences.

Proposition 14. (i) If c is even (respectively, odd), then $\widehat{h}_c = q_c$ (respectively, $\widehat{h}_c = \ell_c$).
(ii) $\widehat{h}_{c_a}(x) = \widehat{h}_c(x-a) - \widehat{h}_c(-a)$ where $c_a = t^*_{-a}(c)$.

Proof. (i) follows from the properties of quadratic functions. For (ii), we compute

$$\begin{aligned}\widehat{h}_{c_a}(x) &= \widehat{h}_c(x-a) + O(1)\\ &= \widehat{h}_c(x) + \widehat{h}_c(-a) + \Delta\widehat{h}_c(x,-a) + O(1)\\ &= \widehat{h}_c(x) + \Delta\widehat{h}_c(x,-a) + O(1).\end{aligned}$$

As before the bounded function $O(1)$ is a sum of quadratic and linear functions. Hence it must be zero. ∎

Let A be an abelian variety, and $c \in \mathrm{Pic}(A)$. Then by Proposition 13, the map $\mathbb{Z} \to \mathrm{Pic}(A)$ sending n to n^*c is a quadratic function.

Proposition 15. If h is a quadratic function on $\mathbb{Z}$, then

$$h(n) = \frac{n(n+1)}{2}h(1) + \frac{n(n-1)}{2}h(-1).$$

In particular,

$$n^*c = \begin{cases} n^2c & \text{if } c \text{ is an even class in } \mathrm{Pic}(A)\\ nc & \text{if } c \text{ is an odd class.}\end{cases}$$

Proof. For this use the facts that if h is a quadratic form, then

$$h(x+y) + h(x-y) = 2h(x) + 2h(y),$$

and a quadratic function is a sum of quadratic form and a linear function. ∎

Proposition 16. Let A be an abelian variety, and $c \in \mathrm{Pic}(A)$ be an even ample class. Then h_c is a positive quadratic form.

Proof. By multiplying c by a large integer, we may assume c is very ample. Hence $h_c \geq 0 + O(1)$. If $h_c(P) \neq 0$, then

$$h_c(nP) = n^2 h_c(P) + O(1).$$

Therefore $h_c(P) \geq 0$. ∎

Before we proceed further, we digress to generalities on Picard varieties and Jacobians. Let X be a Riemmann surface (=nonsingular algebraic curve over $\mathbb{C}$). Then the Jacobian of X can be described as follows : Consider the exponential sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^{\times} \longrightarrow 0.$$

This induces cohomology exact sequence

$$\cdots \to \mathrm{H}^1(X,\mathbb{Z}) \to \mathrm{H}^1(X,\mathcal{O}) \to \mathrm{H}^2(X,\mathcal{O}^{\times}) \xrightarrow{c_1} \mathrm{H}^2(X,\mathbb{Z}) \to \cdots$$

By Serre duality $\mathrm{H}^1(X,\mathcal{O}) \cong \Gamma(\Omega)^*$ where $\Gamma(\Omega)$ is the global holomorphic 1−forms. We know that $\Gamma(\Omega)$ is a g dimensional complex vector space where g is the genus of X. For $\gamma \in \mathrm{H}^1(X,\mathbb{Z})$ we define $\phi_\gamma \in \Gamma(\Omega)^*$ by

$$\phi_\gamma(\omega) = \int_\gamma \omega.$$

Then $\Lambda = \{\phi_\gamma \mid \gamma \in \mathrm{H}^1(X,\mathbb{Z})\}$ is a lattice in the g−dimensional $\mathbb{C}$–vector space. The Jacobian of X is then

$$\Gamma(\Omega)^* \big/ \Lambda$$

which is isomorphic to $\mathrm{Pic}^0(X)$ (=kernel of c_1). Hence the set of line bundles of degree zero form an abelian variety of dimension g over $\mathbb{C}$.

Now let X be a complete nonsingular curve over a field K. Then the elements of $\mathrm{H}^1(X,\mathcal{O}^{\times})$ are represented by the line bundles over X. We have a bijection

$$\left\{ L \middle| \begin{array}{l}\text{line bundles on } X \\ \text{defined over } K\end{array} \right\} \longleftrightarrow \frac{\left\{ D \middle| \begin{array}{l}\text{divisors on } X \\ \text{defined over } K\end{array} \right\}}{\{\text{linear equivalence}\}}$$

The bijection is given by $D \mapsto L(D)$ and given a line bundle L we correspond a divisor of zeroes of a section. For $D = \sum n_i P_i$, $P_i \in X(\overline{K})$, we define the *degree* of D by

$$\deg(D) = \sum n_i [K(P_i) : K].$$

Example. Let $f \in K[t]$ be an irreducible polynomial of degree d. Consider $\mathrm{div}(f)$ on $\mathbb{P}^1_K$. Then f has zero on p_f the prime ideal (f) in $\mathrm{Spec}K[t]$. And f has pole at ∞ of order d. Hence

$$\mathrm{div}(f) = (p_f) - d(\infty)$$
$$\deg(\mathrm{div}(f)) = \left[K[t]/(f) : K\right] - d = 0.$$

Hence we see that a divisor of a rational function on a curve is of degree zero (by pulling back).

Now we define

$$\mathrm{Pic}^0(X) = \frac{\{\text{divisors of degree zero on } X \text{ defined over } K\}}{\{\text{linear equivalence}\}}.$$

Theorem 8. Let X be a nonsingular curve with a K–rational point P_0. Then there is an abelian variety J_X defined over K and of dimension g (g=genus of X) such that there is a functorial isomorphism

$$\mathrm{Pic}^0(X) \longrightarrow J_X.$$

In this case there is a natural embedding

$$\psi : X \longrightarrow J_X$$

sending P to $P - P_0$, which is defined over K.

Let A, $\hat{A}$ be abelian varieties over a field K and $\delta \in \mathrm{Div}(A \times \hat{A})$. We say that the pair $(\hat{A}, \delta)$ is a *Picard variety* or the *dual variety* of A if for any field extension F/K we have isomorphisms

$$\hat{A}_F \longrightarrow \mathrm{Pic}^0(A)_F$$

which sends y to $\delta/A \times \{y\}$.

Theorem 9. For any abelian variety A over K the Picard variety $(\hat{A}, \delta)$ of A exists and is uniquely determined up to a K–isomorphism. And δ is uniquely determined in $\mathrm{Pic}(A \times \hat{A})$. Furthermore, $\hat{\hat{A}} \cong A$.

For the proofs of these theorems see [M].

The divisor δ is called the *Poincaré divisor* and the corresponding line bundle is called the *Poincaré line bundle* which we denote by the same symbol δ. By the uniqueness of δ we see that

$$(-1)^*\delta = \delta.$$

That is δ is even. The Poincaré divisor δ satisfies the properties

(i) $\delta|_{\{0\}\times\widehat{A}}$ is trivial and $\delta|_{A\times\{a\}}$ lies in $\mathrm{Pic}^0(A_{k(a)})$.

(ii) For any variety X over K and a line bundle $A \times X$ such that $L|_{\{0\}\times X}$ is trivial and $L|_{A\times\{x\}}$ lies in $\mathrm{Pic}^0(A_{k(x)})$ then there is a unique morphism $f{:}X \to \widehat{A}$ such that $(1 \times f)^*\delta \cong L$.

If J_X is the Jacobian of a curve of genus ≥ 2, then we have a nice description of duality. Let Θ be the divisor (of J_X) $\Theta = X + \cdots + X$ where the sum is taken $(g-1)$ times in J_X. We will denote the class of Θ by θ.
Let $\delta = \pi_{12}^*\Theta - \pi_1^*\Theta - \pi_2^*\Theta$.

Theorem 10. The pair (J, δ) is dual for J. Hence the Jacobian of a curve is self dual. In particular the map $J_X \to \mathrm{Pic}^0(J)$ sending a to $[\Theta_a - \Theta]$ is an isomorphism.

For an embedding $\psi{:}X \to J$ and let $a \in J$, $X \cdot (\Theta_a - \Theta)$ is a divisor on X. Hence gives us a class in $\mathrm{Pic}^0(X)$ $(= J_X$, which we will denote by $S(X\cdot(\theta_a - \theta))$. Then we have

$$S(X \cdot (\theta_a - a)) = a.$$

Now we return to the analysis of height functions.

Proposition 17. Let A be an abelian variety and $(\widehat{A}, \delta)$ be the dual of A. Then

$$h_\delta(x, 0) = h_\delta(0, y) = 0.$$

The height $h_\delta(x, y)$ is bilinear.

Proof. For the first statement, we compute

$$h_\delta(x, 0) = h_\delta(\pi_1(x, y)) = h_{\delta|_{A\times\{0\}}}(x) = 0$$

since $\delta|_{A\times\{0\}} = 0$. Similarly for $h_\delta(0,y)$.

For the second statement, let $u,\ v \in A \times \widehat{A}$. Let

$$L_\delta(u,v) = h_\delta(u+v) - h_\delta(u) - h_\delta(v).$$

For $x \in A,\ y \in \widehat{A}$, let $L(x,y) = L_\delta((x,0),(0,y))$. Then

$$\begin{aligned} h_\delta(x,y) &= L_\delta((x,0),(0,y)) \\ &= L_\delta((x,0),(0,y)) + h_\delta(x,0) + h_\delta(0,y) \\ &= L_\delta((x,0),(0,y)) \end{aligned}$$

is bilinear. ∎

Proposition 18. Let δ be the Poincaré divisor class on the Jacobian of a curve X. Then $h_\delta(x,y)$ is symmetric bilinear. And if θ is the class of Θ, then

$$-h_\delta(x,x) = h_\theta(x) + h_\theta(-x).$$

Therefore the quadratic form $-h_\delta(x,x)$ is positive.

Proof. Symmetry of h_δ follows from the symmetry of δ and the functorial property of the height functions. For the second statement, we compute :
Let $d{:}J \to J \times J$ be the diagonal map. Then

$$\begin{aligned} -d^*(\delta) &= d^*(\pi_{12}^*\theta - \pi_1^*\theta - \pi_2^*\theta) = (\pi_{12}d)^*\theta - 2\theta \\ &= 2^*\theta - 2\theta = 3\theta + \theta^- - 2\theta \\ &= \theta + \theta^- \end{aligned}$$

by Proposition 15. Therefore

$$-h_\delta(x,x) = -h_\delta \circ d(x) = h_\theta(x) + h_\theta(-x).$$

Now the facts that $\theta + \theta^-$ is even and ample gives us the result. ∎

We will use the following fact without proof. For a proof see [L].

Proposition 19. Let $\delta_{X\times X}$ be the restriction of δ on $J \times J$ via an embedding $\psi{:}X \to J$ sending P to $[P] - c_0$ where c_0 is a divisor class of degree 1. Then

$$\delta_{X\times X} = [\Delta - \{c_0\} \times X - X \times \{c_0\}]$$

where Δ is the diagonal on $X \times X$.

The corresponding statement for height function is

Proposition 20. For $x, y \in X$, we have

$$-h_{\delta_{X\times X}}(x,y) + h_\Delta(x,y) = h_{c_0}(x) + h_{c_0}(y) + O(1).$$

If $x \neq y$, then

$$-h_\delta(x,y) \leq h_{c_0}(x) + h_{c_0}(y) + O(1).$$

Proof. Notice that

$$h_{c_0\times X}(x,y) = h_{\pi_1^* c_0}(x,y) = h_{c_0}(x) + O(1).$$

Similarly, $h_{X\times c_0}(x,y) = h_{c_0}(y) + O(1)$. Hence

$$h_{\delta_{X\times X}}(x,y) = h_\Delta(x,y) - h_{c_0}(x) - h_{c_0}(y) + O(1).$$

The last statement follows from the fact that the height function corresponding to a positive divisor is bounded below off the support of the divisor. (cf. Proposition 16) ∎

Let X be a curve and c_0 be a divisor class of degree 1. Let $\psi: X \to J$ be the embedding given by sending x to $[x] - c_0$. Let $S_\psi: \mathrm{Pic}(X) \to J$ be the map sending $\sum n_i x_i$ to $\sum n_i([x_i] - c_0)$. We will use the following fact.

Proposition 21. If Θ is the divisor introduced before, then

$$S_\psi\big((\Theta + \Theta^-)\cdot X\big) = \kappa + 2c_0$$

where κ is the canonical class and $\Theta^- = \Theta_{-\kappa}$.

We can choose c_0 so that Θ is even. In fact, we can choose c_0 so that $(2g-2)c_0 = \kappa$. If c_0 is chosen in this way, we will say that the corresponding emmbeding is *normalized.*

Proposition 22. If ψ is normalized, then $-h_{\delta_{X\times X}}(x,x) = 2g h_{c_0}(x) + O(1)$ where $x \in X$.

Proof. We compute

$$-h_\delta(x,x) = h_{\theta+\theta^-}(x) = h_{x+2c_0}(x) = 2gh_{c_0}(x) + O(1). \qquad \blacksquare$$

We have seen that $-h_\delta(x,y)$ is symmetric bilinear on $J \times J$. Now we define for $x, y \in J$,

$$<x,y>= -h_\delta(x,y) \qquad \text{and} \qquad |x| = \sqrt{<x,x>}.$$

Theorem 11. [Mumford] For x, y on a curve X we have

$$2g <x,y> +2gh_\Delta(x,y) =<x,x> + <y,y> +O(1).$$

If $x \neq y$, then

$$2g <x,y> \leq |x|^2 + |y|^2 + O(1).$$

Proof. Multiply $2g$ to both sides of the equality (Proposition 20)

$$-h_\delta(x,y) + h_\Delta(x,y) = h_{c_0}(x) + h_{c_0}(y) + O(1)$$

and use Proposition 22 to get the result. $\blacksquare$

Now we consider the abelian varieties over a number field. Let A be an abelian variety over a number field. For $c \in \mathrm{Pic}(A)$ we let $\widehat{h}_c = h_c$ be the canonical height. We define

$$\begin{aligned} <x,y>_c &= h_c(x+y) - h_c(x) - h_c(y) \\ |x|_c &= \sqrt{<x,x>_c} \ \text{(if defined).} \end{aligned}$$

Theorem 12. Let A be an abelian variety over a number field K. Let c be an ample even divisor class on A. Then $|x|_c = 0$ if and only if $x \in A(\overline{\mathbb{Q}})_{tor}$.

Proof. Since c is even we have $|x|_c = n|x|_c$. Let $x \in A$ be defined over a finite extension F of K. Then nx is also defined over F for each n. Now we notice the fact that A is projective and there are only finitely many points of bounded height in a finite extension of K (Theorem 1). Hence if $|x|_c = 0$ then $\{nx | n \in \mathbb{Z}\}$ must be a finite set. $\blacksquare$

Theorem 13. Let A be an abelian variety over a number field K. Let $(\hat{A}, \delta)$ be the dual of A. Then

(i) Each side of the kernel of

$$A \times \hat{A} \longrightarrow \mathbb{R}$$

sending (x, y) to $h_\delta(x, y)$ is A_{tor} and $\hat{A}_{tor}$, respectively.

(ii) The kernel of the map

$$\mathrm{Pic}(A) \longrightarrow \{\text{quadratic functions on } A(\overline{\mathbb{Q}})\}$$

is precisely $(\mathrm{Pic}(A))_{tor}$.

Proof. See [L]. ∎

5 . Mordell–Weil Theorem

In this section, we will prove Mordell–Weil Theorem.

Theorem 14. [Mordell–Weil Theorem] Let K be a number field and A an abelian variety defined over K. Then $A(K)$ is a finitely generated abelian group.

To prove this it will suffices to prove,

Theorem 15. [Weak Mordell–Weil Theorem] Let K be a number field and A an abelian variety over K. Then $A(K)/nA(K)$ is a finite group for an integer $n > 1$.

To show Theorem 15 implies Theorem 14, we need

Proposition 23. [Infinite descent] Let Γ be an abelian group such that

(1) $\Gamma/n\Gamma$ is finite for some $n > 1$.

(2) There is a symmetric bilinear pairing $\Gamma \times \Gamma \xrightarrow{<,>} \mathbb{R}$ such that

(i) $<a, a> \geq 0$ on Γ.

(ii) $\{a \in \Gamma |\ <a, a> < C\}$ is finite for all constant $C > 0$.

Then Γ is finitely generated.

Proof. Let $a_1, \ldots, a_s$ be the representatives of $\Gamma/n\Gamma$. First we claim that there is a constant C such that whenever $<a, a> \geq C$, then

$$<a - a_i, a - a_i> < 2<a, a> \qquad (i = 1, \ldots, s).$$

To see this note that the Schwartz inequality

$$<a, a_i> \leq \sqrt{<a, a>}\sqrt{<a_i, a_i>}$$

holds since $<a, a> \geq 0$. Since

$$<a - a_i, a - a_i> = <a, a> - 2<a, a_i> + <a_i, a_i>$$

we see that $<a - a_i, a - a_i>$ increase asymtotically as $<a, a>$ for $<a, a> \to \infty$. Hence the claim.

Now let $M = \{a_1, \ldots, a_s\} \cup \{a \in \Gamma | <a, a> < C\}$, where C is the constant chosen above. Let Γ_0 be the subgroup generated by M. We want to show $\Gamma_0 = \Gamma$. Assume the contrary. Choose $x \notin \Gamma_0$ and $<x, x>$ is minimal. (The set $\{a \in \Gamma | <a, a> \leq C + N\}$ will be finite for a positive integer N.) Obviously $<x, x> \geq C$. Let $x - a_i = nb$ for some $b \in \Gamma$ and $a_i \in M$. Then

$$<b, b> = \frac{1}{n^2} <x - a_i, x - a_i> < \frac{2}{n^2} <x, x><x, x> .$$

By minimality of $<x, x>$ we have $b \in \Gamma_0$. Hence $x = nb + a_i \in \Gamma_0$. A contradiction. ∎

Now we will explain why weak Mordell–Weil theorem implies the Mordell–Weil theorem. Choose an even (very) ample divisor class c on A. Hence h_c is a positive quadratic form (Proposition 16). Define

$$<x, y> = h_c(x + y) - h_c(x) - h_c(y).$$

Therefore $<x, x> = 2h_c(x)$. By theorem 1, there are only finitely many points of bounded height and of bounded degree. Hence the pairing meets all the conditions of Proposition 23. Hence $A(K)$ is finitely generated.

Now we will prove weak Mordell–Weil theorem in several steps. As before we let A be an abelian variety defined over a number field K. Let

$$A_n = \{x \in A(\overline{K}) | nx = 0\}$$

for any group variety A. If A is an abelian variety, then $A_n \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ where g is the dimension of A and $A_n = \mu_n$ if $A = K^*$. For the rest of this section we will assume $A_n \subset A(K)$. This can be achieved by a finite extension and obviously it suffices to prove the Mordell–Weil theorem for a finite extension of K.

For $x \in A$, let $K(n^{-1}x)$ be the field by adjoining all coordinates of $n^{-1}x$, the inverse image of x under the multiplication by n map. Then we first notice that $K(n^{-1}x)/K$ is an abelian extension of exponent n. In fact, if σ is a conjugate of $K(n^{-1}x)$ over K and if $ny = x$, then $n(\sigma(y)) = \sigma(ny) = x$. Hence the extension is normal. Write $a_\sigma = \sigma(y) - y \in A_n$ so that $\sigma(y) = y + a_\sigma$. If τ is another conjugate, then we have $\tau\sigma(y) = y + a_\sigma + a_\tau$. Hence $K(n^{-1}x)/K$ is abelian of exponent n.

Let B be subgroup of $A(K)$ containing $nA(K)$. Let

$$L_B = K\left(\{n^{-1}b | b \in B\}\right).$$

Then the above observation shows that L_B/K is abelian of exponent n. Let G_B be the Galois group of L_B/K. Define the bilinear pairing

$$G_B \times B \xrightarrow{<,>} A_n \quad \text{by} \quad <\sigma, b>= \sigma(n^{-1}b) - n^{-1}b.$$

One can check easily that the definition does not depend on the choice of $n^{-1}b$. If $<\sigma, b>= 0$ for all $b \in B$, then σ is an identity since L_B is generated by $n^{-1}b$, $b \in B$. On the other hand, if $<\sigma, b>= 0$ for all $\sigma \in G_B$, then $n^{-1}b \in A(K)$ *i.e*, $b \in nA(K)$. Hence we have a nondegenerate bilinear pairing

$$G_B \times B/nA(K) \longrightarrow A_n.$$

Therefore we have proved ;

Proposition 24. Let A be an abelian variety over a number field K. Assume $A_n \subseteq A(K)$ and let B be a subgroup of $A(K)$ containing $nA(K)$. Then $K(n^{-1}B)$ is an abelian extension of exponent n. Further $K(n^{-1}B)$ is a finite extension if and only if $B/nA(K)$ is a finite group.

If A is the multiplicative group $K^\times$, then we have more precise information.

Proposition 25. Let K be a number field containing the n–th roots of unity μ_n. Let F be a maximal abelian extension of K with Galois group H. Then we have a nondegenerate pairing

$$H \times K^{\times}/K^{\times n} \longrightarrow \mu_n \quad \text{defined by} \quad (\sigma, \overline{a}) \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Hence there is a bijection

$$\left\{E/K \middle| \begin{matrix}\text{abelian extension} \\ \text{of exponent } n\end{matrix}\right\} \longleftrightarrow \left\{B \subset K \middle| \text{ subgroups containing } K^{\times n}\right\}.$$

The bijection being given by

$$E \longmapsto G\left(F/E\right)^{\perp} \qquad \text{and} \qquad B \longmapsto K(n^{-1}B).$$

Furthermore, we have $[E_B : K] = [B : K^{\times n}]$ where E_B is the abelian extension corresponding to B.

Proof. See Lang's Algebra. ∎

According to Proposition 24, to prove Weak Mordell–Weil theorem we need to show $K(n^{-1}A(K))$ is a finite abelian extension of K. We need some Néron model theory. Let R be the ring of integers of a number field K, and A an abelian variety over K.

Theorem 16. There is an open set Y of Spec$R$ and a group scheme $\tilde{A}$ over Y such that

(i) $\tilde{A} \times_Y \text{Spec}K = A$.

(ii) For every $y \in Y$, the fiber $\tilde{A}_y$ is an abelian variety.

(iii) $\tilde{A}(Y) \simeq A(K)$ *i.e*, the group of Y-points of $\tilde{A}$ is isomorphic to the group of K-points of A.

Proof. See [N]. ∎

Let $x \in \tilde{A}(Y)$. Then $n^{-1}x$ is a finite (affine) scheme over Y. The natural projection $n^{-1}x \longrightarrow Y$ is étale over all $y \in Y$ whenever $\text{char}\, k(y) \nmid n$. Let

S be the set of primes dividing n and the primes excluded in Theorem 16. Then it follows that for $y \in n^{-1}x$, $K(y) \supset K$ is unramified outside S. Hence $K(n^{-1}x) \supset K$ is an abelian extension of exponent n unramified outside S. Accordingly so is $K(n^{-1}A(K))$ over K. Therefore to complete the proof of Mordel–Weil theorem, it suffices to show

Proposition 26. Let K be a number field containing μ_n. Let L be a maximal abelian extension of exponent n unramified outside the finite set of primes S. Then L/K is a finite extension.

To prove this we quote a fact whose proof we refer to [L].

Proposition 27. Let v be a discrete valuation on K and n a positive integer prime to the characteristic of the residue field of v. Then v is unramified in $K(\sqrt[n]{a})$ if and only if $n|\mathrm{ord}_v(a)$.

Hence if E_B is the Kummer extension belonging to $B \subseteq K^\times$, then E_B is unramified outside S if and only if for any $b \in B$, there is an S–ideal $\mathfrak{b}$ such that $(b) = n\mathfrak{b}$. Now if $B_u \subseteq K^\times$ belongs to a maximal abelian extension of K of exponent n unramified outside S, then

$$B_u = \left\{ b \in K^\times \mid \text{there is an } S\text{–ideal } \mathfrak{b} \text{ such that } (b) = n\mathfrak{b} \right\}.$$

If we write C_n for the n–torsions of S–ideal classes and U_S for the S–units, then we have an exact sequence

$$0 \longrightarrow U_S/U_S^n \longrightarrow B_u/K^{\times n} \longrightarrow C_n \longrightarrow 0.$$

From number theory we know that U_S is a finitely generated abelian group and hence U_S/U_S^n is finite. Also we know that the S–ideal class group is also finite. Therefore $B_u/K^{\times n}$ is finite. Now Proposition 25 finishes the proof of Proposition 26. Thereby finishing the proof of Mordell–Weil Theorem.

6 . Roth Theorem

Let α be a real number which is not rational. We want to approximate α by rational numbers p/q but p and q not too large. Classical Dirichlet theorem says

Theorem 17. [Dirichlet] Let $\alpha \in \mathbb{R} - \mathbb{Q}$. Then

$$\left\{\frac{p}{q} \middle| \left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^2}\right\}$$

is an infinite set.

Proof. See Silverman [S] ∎

But Liouville theorem says the approximation cannot be arbitrarily close.

Theorem 18. [Liouville] Let $\alpha \in \overline{\mathbb{Q}} - \mathbb{Q}$ be of degree d. Then there is a constant C such that for any $p/q \in \mathbb{Q}$, we have

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d}.$$

Proof. See Silverman [S]. ∎

Let $\tau(d)$ be a positive real valued function on rational numbers. We say that a number field K has an *approximation exponent* τ if for any $\alpha \in \overline{K}$ of degree d over K, for any $v \in M_K$ (extended to $K(\alpha)$ in some way) and for any constant C the set

$$\left\{x \in K \middle| \ |x - \alpha|_v < C H_K(x)^{-\tau(d)}\right\}$$

is finite. Note that $|x - \alpha|_v$ is something about topology of K and $H_K(x)$ has something to do with arithmetic of K. Liouville's theorem says that $\mathbb{Q}$ has an approximation exponent $\tau(d) = d + \varepsilon$, $\varepsilon > 0$. Here are some list of improvement.

Liouville	1851	$\tau(d) = d + \varepsilon$
Thue	1909	$\tau(d) = 2^{-1}d + 1 + \varepsilon$
Siegel	1921	$\tau(d) = 2\sqrt{d} + \varepsilon$
Gelfond, Dyson	1947	$\tau(d) = \sqrt{2d} + \varepsilon$
Roth	1955	$\tau(d) = 2 + \varepsilon$

In view of Dirichlet's theorem, Roth's theorem is the best possible.

Theorem 19. [Roth] Let K be a number field and S be a finite set of places. For each $v \in S$, let α_v be algebraic over K. Extend v to $\overline{K}$ in some way. Let $\kappa > 2$ be a real. Then the set

$$\left\{\beta \in K \Big| \prod_{v \in S} \inf(1, \|\alpha_v - \beta\|_v \leq \frac{1}{H(\beta)^\kappa}\right\}$$

is of bounded height.

For a proof of Roth's Theorem we refer [L]. However we will show how to reformulate Roth's Theorem in a geometric form which we will use to prove Siegel's theorem. Here is a preliminary version.

Proposition 28. Let $G(y) \in K[y]$ be a polynomial such that the multiplicity of roots of G is bounded by r. Let S be a finite set of places and $C > 0$, $\kappa > 2$ be constants. Then the set

$$\left\{\beta \in K \Big| \prod_{v \in S} \inf(1, \|G(\beta)\|_v) \leq \frac{C}{H(\beta)^{\kappa r}}\right\}$$

is of bounded height.

Proof. We may assume G has leading coefficient 1. Write $G(y) = \prod_{i=1}^{d} (y - \alpha_i)^{e_i}$. Extend v in S to $\overline{K}$ in some way then

$$\prod_{v \in S} \inf(1, \|G(\beta)\|_v) \geq \prod_{v \in S} \prod_{i=1}^{d} \inf(1, \|\beta - \alpha_i\|_v)^{e_i} \geq \prod_{v \in S} \prod_{i=1}^{d} \inf(1, \|\beta - \alpha_i\|_v)^{r}.$$

Roth's theorem implies that

$$\left\{\beta \Big| \prod_{v \in S} \prod_{i=1}^{d} \inf(1, \|\beta - \alpha_i\|_v)^{r} \leq \frac{1}{H(\beta)^{\kappa r}}\right\}$$

is of bounded height. Therefore the set of solutions to the original inequality is also of bounded height. ∎

Using this we will prove the first geometric formulation of the Roth's theorem.

Theorem 20. Let W be a complete nonsingular curve. Let z, y be nonconstant rational functions on W. Let r be the maximum of the order of zero of z and let y be defined on the set of zeroes and poles of z and y takes distinct values at zeroes of z. Let $\kappa > 2$, $C > 0$. Then the set

$$\left\{ Q \in W(K) \,\middle|\, \begin{array}{l} Q \text{ is not a zero or pole of } z \text{ and} \\ \prod\limits_{v \in S} \inf(1, \|z(Q)\|_v) \leq \frac{C}{H(y(Q))^{\kappa r}} \end{array} \right\}$$

is of bounded height (with respect to H_y).

Proof. We may assume $K(W) = K(z, y)$ for otherwise we may take the nonsingular model of $K(z, y)$. Next we may assume $\|y(Q)\|_v$ are bounded for all $v \in S$ for otherwise we can make a coordinate change

$$y' = \frac{ay + b}{cy + d} \quad (a, b, c, d \in K)$$

so that y' satisfies the same property as y and $\|y'(Q)\|_v$ are bounded.

Let Φ be the zero set of z. Since y has no poles on Φ, we see that y is integral over $K[z]_{(z)}$ which we denote by θ. Let $F(y)$ be the irreducible equation of y over $\mathcal{O}$ and let $G(y) \in K[y]$ be such that $G(y) \equiv F(y) (\mathrm{mod}\, z)$. Then by hypothesis y maps Φ into $\overline{K}$ injectively. Hence we conclude that the multiplicity of roots of $G(y)$ is bounded by r. Write

$$F(y) = G(y) + zA(z, y), \quad A(z, y) \in \mathcal{O}[y].$$

Since $A(0, y)$ is defined, $A(z(Q), y)$ is also defined for small $\|z(Q)\|_v$. Since we may assumed $\|y(Q)\|_v$ are bounded, the value $\|A(z(Q), y(Q))\|_v$ are bounded. Since $0 = F(y) = G(y) + zA(z, y)$ we have

$$\|G(y(Q))\|_v \leq c'' \|z(Q)\|_v \|A(z(Q), y(Q))\|_v \leq c' \|z(Q)\|_v \quad (v \in S)$$

for some constant c'. Take the product to get,

$$\prod_{v \in S} \inf(1, \|G(y(Q))\|_v) \leq c' \prod_{v \in S} \inf(1, \|z(Q)\|_v) \leq c / H(y(Q))^{\kappa r}.$$

Using Theorem 19, one can easily check that the points satisfying the inequality of the theorem is H_y–bounded. ∎

Theorem 21. Let W be a nonsingular curve over K. Let $\psi \in K(W)$ be a nonconstant function and r be the maximal order of pole of ψ. Let $\kappa>2, c>0$ and S be a finite set of places. Then the set

$$\left\{ Q \in W(K) \middle| \begin{array}{c} Q \text{ is not a pole of } \psi \text{ and} \\ \prod_{v \in S} \sup(1, \|\psi(Q)\|_v \geq cH(Q)^{\kappa r} \end{array} \right\}$$

is of bounded height.

Proof. Choose $z = 1/\psi$ in the previous theorem and take the reciprocals. ∎

We will prove the Siegel's theorem on finiteness of integral points on an affine curve. Even though Siegel's theorem is overwhelmed by Faltings' proof of Mordell conjecture we will follow the classical line of proofs.

Using weak Mordell–Weil theorem we can improve the Roth theorem as in

Theorem 22. Let K be a number field and $v \in M_K$. Let C be a projective nonsingular curve of genus≥ 1 which is defined over K. Let φ be a nonconstant rational function on C. Let ρ, $c > 0$ be constants. Then the set

$$\left\{ P \in C(K) \middle| \begin{array}{c} P \text{ is not a pole of } \varphi \text{ and} \\ |\varphi(P)|_v \geq cH(P)^{\rho} \end{array} \right\}$$

is of bounded height.

To prove this we need

Proposition 29. Let C be a nonsingular curve over a number field K and let J be its Jacobian. Let m be an integer with $J(K)/mJ(K)$ is finite. Then there is a nonsingular curve U over K and a map $\omega: U \to C$ which is unramified such that $H \circ \omega$ is quasi–equivalent to H^{m^2}.

Proof. Let $m: J \to J$ be the multiplication by m map. Then m is unramified. Let U be the pull back of C. Assume we have a projective embedding $J \subset \mathbb{P}^N$ and let X be a hyperplane section. Then since X is algebraically equivalent to an even class, we have that m^*X is algebraically equivalent to m^2X. By functoriality $H \circ \omega$ is equivalent to $H_{\omega^* X} = H_{m^* X}$. Hence $H \circ \omega$ is quasi–equivalent to H^{m^2}. ∎

Proof of Theorem 22. Let $\varepsilon > 0$. Choose m large enough so that

$$m^2\rho > \kappa r \qquad \text{and} \qquad m^2\rho(1-\varepsilon) > \kappa r.$$

Then there is a constant c_1 such that

$$H\circ\omega(P) \geq c_1 H(P)^{m^2(1-\varepsilon)}.$$

Rasing ρ–th power we have inequalities with some constant c_2,

$$|\psi(Q)|_v \geq c_2 H\circ\omega(P)^\rho \geq c_1c_2 H(P)^{m(1-\varepsilon)\rho} \geq c_1c_2 H(P)^{\kappa r}.$$

Hence we have

$$\{Q \in U|\ |\psi(Q)|_v \geq c_1 H(Q)^\rho\} \subseteq \{Q \in U|\ |\psi(Q)|_v \geq c_1c_2 H(P)^{\kappa r}\}.$$

and the latter is of bounded height. Therefore the former is also of bounded height. This complete the proof of theorem 22. ∎

Theorem 23. Let K, C, φ be as before. Let S be a finite set of places containing all infinite places. Let R be the S–integers. Then the set

$$\Re = \{P \in C(K)|\ P \text{ is not a pole of } \varphi \text{ and } \varphi(P) \in R\}$$

is of bounded height.

Proof. Assume the contrary. Let $\Re_1$ be a sequence of points of $\Re$ whose height tends to infinity. We have ($H = H_K$)

$$H(\varphi(P)) = \prod_{v\in S} \sup(1, |\varphi(P)|_v).$$

Let s be the number of places in S. Then for any $P \in \Re_1$, there is $v \in S$ such that

$$H(\varphi(P)) \leq |\varphi(P)|_v^s.$$

Since S is finite and $\Re_1$ is infinite, we can find an infinite subset $\Re_2$ of $\Re_1$ and $v \in S$ such that

$$H(\varphi(P)) \leq |\varphi(P)|_v^s$$

for all $P \in \Re_2$. View φ as a section of the line bundle corresponding to the divisor $(\varphi)_\infty$ and let $r = \deg(\varphi)_\infty$. Let r be the degree of C (in a projective

embedding). Then by Corollary 2 to Theorem 4, we have that $(H \circ \varphi)^d$ and H^r are quasi–equivalent. Hence for any $\varepsilon > 0$, there is c_1 such that

$$H(P)^{(r/d)-\varepsilon} \leq c_1 H(\varphi(P)).$$

Then for any $P \in \mathfrak{R}_2$, there is $\rho = \frac{1}{s}\left(\frac{r}{d} - \varepsilon\right) > 0$ such that

$$|\varphi(P)|_v \geq c_2 H(P)^\rho.$$

This contradicts to our previous theorem. ∎

Theorem 24. [Siegel] Let K be a number field, R be the ring of integers. Let C be an affine curve over R with genus≥ 1. Then the number of integral points of C is finite.

Proof. We have embeddings

$$C \subset A^n \subset \mathbb{P}^n.$$

Let $x_1, \ldots, x_n$ be the coordinates of A^n. Then

$$C(R) = \{P \in C(K) |\ x_i(P) \in R \text{ for all } i\}$$

is of bounded height. But the set of points of bounded height in $\mathbb{P}^n_K$ is finite by Theorem 1. ∎.

References

[F] W. Fulton, Intersection Theory, Springer–Verlag, 1984

[G-H] P. Griffith, J. Harris, Principles of Algebraic Geometry, Wiley–Interscience, 1978

[H] R. Hartshone, Algebraic Geometry, Springer–Verlag, 1977

[L] S. Lang, Fundamentals of Diophantine Geometry, Springer–Verlag 1983

[M] D. Mumford, Abelian Varieties, Oxford University Press, 1974

[N] A. Néron, Modèles mimaux des variétiés abéliennes sur les corps locaux et globaux, Pub. I.H.E.S 21, 1964

[S] J. Silverman, The Arithmatic of Elliptic Curves, Springer–Verlag, 1986

Cyclotomic Fields I

Jae Moon Kim

Department of Mathematics
In Ha University
Incheon 402 – 751, Korea

Contents

§ 1. Λ and finitely generated Λ–modules

Let $\mathbb{Z}_p$ be the ring of p-adic integers and let $\Lambda = \mathbb{Z}_p[[T]]$ be the ring of power series in T. Then Λ is a topological Noetherian local ring with the maximal ideal

$$\mathfrak{m} = \mathbb{Z}_p[[T]] - \mathbb{Z}_p[[T]]^\times = p\mathbb{Z}_p + T\mathbb{Z}_p[[T]] = (p, T).$$

The topology on Λ is the product topology $\prod_0^\infty \mathbb{Z}_p$, so $f_k(T) = \sum a_{n,k}T^n$ approaches to $f(T) = \sum a_n T^n$ if and only if $a_{n,k} \to a_n$ in $\mathbb{Z}_p$ for all n.

Definition 1.1 Let $f(T) \in \Lambda$. By $\mu(f)$, we mean the highest power of p dividing $f(T)$. Let $f(T) = a_0 + a_1T + a_2T^2 + \cdots$. Then $\lambda(f)$ is defined to be the first index i whose p-adic valuation is $\mu(f)$ *i.e.*, $p^{\mu(f)+1} | a_k$ for $k = 0, 1, \ldots, \lambda(f) - 1$, but $p^{\mu(f)+1} \nmid a_{\lambda(f)}$.

Theorem 1.1 (Euclidean Algorithm) Let $f(T) \in \Lambda$ with $\mu(f) = 0$, $\lambda(f) = n$. Then for any $g(T) \in \Lambda$, there are unique $q(T) \in \Lambda$ and $r(T) \in \mathbb{Z}_p[T]$ of degree $< n$ such that

$$g(T) = q(T)f(T) + r(T).$$

Proof. Refer to [9] Chapter 7, section 1. ∎

Some Consequences

(1) If $\mu(f) = 0$, then $\mathbb{Z}_p[[T]]/(f) \simeq \mathbb{Z}_p^\lambda$ as $\mathbb{Z}_p$–modules, where $\lambda = \lambda(f)$.

(2) (Weierstrass Preparation Theorem)
If $\mu(f) = 0$, then there are unique $U(T) \in \Lambda^\times$ and a distinguished polynomial $P(T)$ of degree $\lambda = \lambda(f)$ such that $f(T) = U(T)P(T)$.

> A polynomial $h(T) = a_0 + a_1T + \cdots + a_kT^k$ is distinguished if $p | a_i$ for $0 \le i \le k-1$ and $p \nmid a_k$.

More generally, for any $f(T) \in \Lambda$, $f(T) = p^\mu U(T)P(T)$, where $U(T) \in \Lambda^\times$, $P(T)$ is a distinguished polynomial of degree $\lambda(f)$ and $\mu = \mu(f)$.

Proof. It is enough to show the first half. Let $g(T) = T^\lambda$ and apply the division algorithm ;

$$\begin{aligned} T^\lambda &= q(T)f(T) + r(T), \quad \deg r < \lambda \\ T^\lambda &\equiv q(T)T^\lambda f_1(T) + r(T) \bmod p, \end{aligned}$$

where $f_1(T) = \dfrac{f-(a_0+a_1T+\cdots+a_{\lambda-1}T^{\lambda-1})}{T^\lambda}$, $f(T)=\sum a_iT^i$. Hence $r(T)\equiv 0 \bmod p$. Therefore, $P(T)=T^\lambda - r(T)$ is a distinguished polynomial. By reading the coefficients of $T^\lambda (\bmod p)$, we obtain $1\equiv q(0)f_1(0)$. Hence $q(0)\in \mathbb{Z}_p^\times$ and $q(T)\in \Lambda^\times$. Let $U(T)=1/q(T)$. Uniqueness follows from the uniqueness of q and r. ∎

(3) Suppose $\mu(f)=0$, so $f=UP$ as before. Then the natural injection

$$\mathbb{Z}_p[T]/(P) \longrightarrow \Lambda/(f)$$

is an isomorphism.

(4) Λ is a unique factorization domain having p and irreducible distinguished polynomials as prime elements.

Proof. Since $\Lambda/(p)\simeq \mathbb{F}_p[[T]]$ is an integral domain, (p) is a prime ideal, hence p is a prime element. If $P(T)$ is an irreducible distinguished polynomial, then

$$\Lambda/(P(T)) \simeq \mathbb{Z}_p[T]/(P(T))$$

is again an integral domain, so $P(T)$ is a prime element. Let $f(T)\in\Lambda$. Then $f(T)=p^\mu P(T)U(T)$ for some distinguished polynomial $P(T)$ and unit $U(T)$. Since $\mathbb{Z}_p[T]$ is a U.F.D, we can factorize $P(T)$ as $P(T)=P_1(T)^{e_1}\cdots P_r(T)^{e_r}$ in $\mathbb{Z}_p[T]$, where $P_i(T)$'s are irreducible polynomials in $\mathbb{Z}_p[T]$. By reading this mod p, we have $T^\lambda \equiv \overline{P}_1^{e_1}\cdots\overline{P}_r^{e_r} \bmod p$, thus $\overline{P}_i \equiv T^{\lambda_i} \bmod p$ for some λ_i. Hence P_i is distinguished and irreducible in Λ. ∎

(5) Suppose $f(T)$ and $g(T)$ are relatively prime in $\mathbb{Z}_p[[T]]$. Then $\Lambda/(f,g)$ is a finite set.

Proof. One of f or g is not divisible by p, say $p\nmid f$. Write $f(T)=P(T)U(T)$, and $g(T)=p^aQ(T)V(T)$, where $P(T)$, $Q(T)$ are distinguished polynomials and $U(T),V(T)\in\Lambda^\times$. Then $(f,g)=(P(T),p^aQ(T))$. Since f and g are relatively prime in Λ, so are $P(T)$ and $Q(T)$ in $\mathbb{Z}_p[T]$. Since $\mathbb{Q}_p[T]$ is a principal ideal domain, there exist $R(T),S(T)\in\mathbb{Q}_p[T]$ such that $RP+SQ=1$. By clearing the denominators, we get $p^c=R_1P+S_1Q$ for some integer $c\geq 0$. Hence

$$p^{a+c}=R_2P(T)+S_1p^aQ(T)\in(P(T),p^aQ(T))=(f,g).$$

Hence $(p^{a+c},f)\subset(f,g)$. Since $\Lambda/(p^{a+c},f)$ is finite, so is $\Lambda/(f,g)$. ∎

Now we study finitely generated λ-modules.

Lemma 1.1 Suppose that X is a finitely generated Λ–module such that $fX = gX = 0$ for some relatively prime elements $f, g \in \Lambda$. Then X is finite.

Proof. Let $g_1, g_2, \ldots, g_r$ be a set of generators of X. Then we have a surjection $\Lambda^r \to X$ defined by $(f_1, \ldots, f_r) \mapsto f_1 g_1 + \cdots + f_r g_r$. This map factors through $(\Lambda/(f,g))^r \to X$. Since $\Lambda/(f,g)$ is finite, so is X. ∎

Definition 1.2 A Λ–module homomorphism $\varphi: X \to Y$ is called a pseudo–isomorphism if $\ker\varphi$ and $\operatorname{coker}\varphi$ are finite. When there exists such a φ, we say that X and Y are pseudo-isomorphic and write $X \sim Y$.

Remark. (i) $X \sim X$,

(ii) $X \sim Y$ and $Y \sim Z$ implies $X \sim Z$,

(iii) $X \sim Y$ does not imply $Y \sim X$. For example, $\mathfrak{m} = (p, T) \hookrightarrow \Lambda$ is a pseudo–isomorphism but there is no pseudo–isomorphism $\Lambda \to \mathfrak{m}$. The proof is left as an exercise.

Proposition 1.1 Suppose that X, Y are finitely generated torsion Λ–modules. Then $X \sim Y$ implies $Y \sim X$.

To prove this proposition, we need two lemmas.

Lemma 1.2 Suppose that X is a finitely generated torsion Λ–module, say $fX = 0$. Let $g \in \Lambda$ be relatively prime to f. Then $X \xrightarrow{g} X$ is a pseudo–isomorphism.

Proof. Since $f(\ker g) = g(\ker g) = 0$, $\ker g$ is finite. And since $f(X/g(X)) = g(X/g(X)) = 0$, $X/g(X)$ is finite. ∎

Lemma 1.3 Suppose that B is a finite Λ–module. Then for any element $g(T)$ in $\mathfrak{m} = (p, T)$, we have $g^n B = \{0\}$ for all $n \gg 0$.

Proof. Take $b \in B$. Since Λb is a finite set, $g^n b = g^m b$ for some $n < m$. Thus $g^n(1 - g^{m-n})b = 0$. Since $1 - g^{m-n} \in \Lambda^\times$, we have $g^n b = 0$. Since B is finite, we have $g^s B = 0$ for $s \gg 0$ ∎

Proof of Proposition 1.1. Let $X \xrightarrow{\varphi} Y$ be a pseudo–isomorphism. Let $A = \ker\varphi$, $Z = \mathrm{Im}\varphi$. Suppose that $f_1 X = f_2 Y = 0$ for some $f_1, f_2 \in \Lambda$. Choose $g \in \mathfrak{m}$ relatively prime to both f_1 and f_2. Then the composition of following maps gives a desired pseudo–isomorphism :

$$Y \xrightarrow[n\gg 0]{g^n} Z \rightarrowtail X/A \xrightarrow[m\gg 0]{g^m} X. \qquad \blacksquare$$

Theorem 1.2 (Iwasawa) Let X be a finitely generated Λ–module. Then

$$X \sim \Lambda^r \oplus \bigoplus_{i=1}^{n} \Lambda/(f_i)^{e_i}$$

for some prime elements $f_1, \ldots, f_n \in \Lambda$, $r \geq 0$. And $r, f_1^{e_1}, \ldots, f_n^{e_n}$ are unique up to ordering.

Proof. X can be shown to be isomorphic to a direct sum of free part Λ^r and torsion part $t(X)$. And the rank of the free part is invariant. Furthermore, the torsion part is pseudo–isomorphic to a Λ–module which has no finite submodule *i.e.*,

$$t(X) \sim t(X)/A,$$

where A is the maximal finite submodule *i.e.*, the sum of all finite submodules. Therefore, we may assume that X is a torsion Λ–module without finite submodules.

Step 1. Since X is a finitely generated torsion Λ–module, there is a polynomial $f \in \mathbb{Z}_p[T]$ such that $fX = 0$. Write $f = q_1^{e_1} \cdots q_r^{e_r}$ where q_i is either p or an irreducible distinguished polynomial. Let

$$X(q_i) = \{\, x \in X : q_i^m x = 0 \text{ for some } m \in \mathbb{N} \,\}.$$

Then $X \sim \oplus X(q_i)$.

Proof. Suppose that $\sum x_{q_i} = 0$ with $x_{q_i} \in X(q_i)$. Let $q_i^* = \frac{f}{q_i^{e_i}}$. Then for an $n \gg 0$ $q_i^{*n}(\sum x_{q_i}) = q_i^{*n} x_{q_i} = 0$ and $q_i^m x_{q_i} = 0$. Thus Λx_{q_i} is finite, hence is 0 and $x_{q_i} = 0$. This means that the map $\oplus X(q_i) \xrightarrow{\varphi} X$ defined by

$(\cdots, x_{q_i}, \cdots) \mapsto \sum x_{q_i}$ is injective . Since $q_i^{e_i}(q_i^* X) = 0$, $q_i^* X \subset X(q_i) \subset \mathrm{Im}\varphi$. Let $\mathfrak{a}$ be the ideal of Λ generated by $q_1^*, \ldots, q_r^*$. Then $\mathfrak{a}X \subset \mathrm{Im}\varphi$ and $X/\mathrm{Im}\varphi$ is finite by the following lemma.

Lemma 1.4 Let $\mathfrak{a}$ be an ideal of Λ whose greatest common divisor is 1, that is, $\mathfrak{a}$ is not contained in a proper principal ideal. Then $\Lambda/\mathfrak{a}\Lambda$ is finite.

Proof. Let $f \in \mathfrak{a}$ be a polynomial of the smallest degree in $\mathfrak{a}$. Write $f = p^a Q$, where Q is distinguished. Let g be any element in $\mathfrak{a}$. By Euclidean algorithm, $g = qQ + r$, $\deg r < \deg Q$ or $r = 0$. But since the degree of $p^a r \in \mathfrak{a}$ is smaller than $\deg Q$, r must be zero. Hence $g = qQ$. Since the greast common divisor of $\mathfrak{a}$ is 1, $Q = 1$. Hence $f = p^a$. Take $h \in \mathfrak{a}$ which is not divisible by p. Then $(p^a, h) \subset \mathfrak{a} \subset \Lambda$ and $\Lambda/(p^a, h)$ is finite. ∎

Step 2. Let q be one of q_i in Step 1. There are $x_1, \ldots, x_s \in X(q)$ such that $X(q) \sim \bigoplus \Lambda x_i$.
Proof. Localize Λ and $Y = X(q)$ at the prime ideal (q). We get a $\Lambda_{(q)}$–module $Y_{(q)}$. Since $\Lambda_{(q)}$ is a principal ideal domain,

$$Y_{(q)} \simeq \Lambda_{(q)} x_1 \oplus \cdots \oplus \Lambda_{(q)} x_s$$

for some $x_1, \ldots, x_s \in Y$. The map

$$\begin{aligned} \bigoplus \Lambda x_i &\xrightarrow{\varphi} Y \\ (\ldots, f_i x_i, \ldots) &\mapsto \sum f_i x_i \end{aligned}$$

is an injection, since $\bigoplus \Lambda x_i \subseteq \bigoplus \Lambda_{(q)} x_i \simeq Y_{(q)}$. Let $\overline{z_1}, \ldots, \overline{z_n}$ be generators of $Y/\mathrm{Im}\varphi$ for some $z_1, \ldots, z_n \in Y$. Note that for each $z \in Y \subset Y_{(q)}$, z can be written as $z = \sum \frac{f_i}{g_i} x_i$ with $q \nmid g_i$. Let $g = \prod g_i$, $g^* = \frac{g}{g_i}$. Then $gz = \sum g_i^* f_i x_i \in \mathrm{Im}\varphi$. Hence $g\overline{z} = q^m \overline{z} = 0$. Thus $\Lambda\overline{z}$ is finite. Apply this argument to each generator of $Y/\mathrm{Im}\varphi$ to conclude $Y/\mathrm{Im}\varphi$ is finite. ∎

Step 3. So far we have proved

$$X \sim \bigoplus_{q|f} X(q) \sim \bigoplus_{q|f} \bigoplus \Lambda x_{q_i}.$$

Hence it remains to show that for each $x \in X(q)$, $\Lambda x \simeq \Lambda/(q^e)$ some $e \geq 0$.
Proof. The map $\Lambda \longrightarrow \Lambda x$ defined by $h \mapsto hx$ is a surjection. Let $\mathfrak{a}$ be the kernel of this map and q^e be the smallest power of q such that $q^e x = 0$. Then $(q^e) \subseteq \mathfrak{a}$. It is easy to show that $(q^e) = \mathfrak{a}$. ∎

§ 2. Iwasawa Invariants μ, λ and ν

Let k be a number field (*i.e.*, $[k:\mathbb{Q}]$ is finite) and p be a prime number. A $\mathbb{Z}_p$–extension of k is a tower

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_n \subseteq \cdots$$

such that k_n/k is Galois and cyclic of order p^n. Let $k_\infty = K = \bigcup_{n\geq 0} k_n$. Then $\mathrm{Gal}(K/k) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$. We also say that K/k is a $\mathbb{Z}_p$–extension. One often denotes the Galois group $\mathrm{Gal}(K/k)$ by Γ and we will use this notation.

Facts from Local Class Field Theory

Let F be the completion of a number field at some finite prime. Let E be a finite abelian extension of F. Then there is a surjection

$$\begin{array}{ccc} F^\times & \to & \mathrm{Gal}(E/F) \\ a & \mapsto & (a, E/F) \end{array}$$

with the following properties :

(1) Suppose that $F \subset E \subset D$ for some abelian extension D of F. Then

$$(a, D/F)\big|_E = (a, E/F).$$

(2) The kernel is $N_{E/F}(E^\times)$, so $F^\times/N_{E/F}(E^\times) \simeq \mathrm{Gal}(E/F)$.

(3) Let $U_F = \mathcal{O}_F^\times$ be the group of units in the ring of integers of F. Then

$$(U_F, E/F) = T_{E/F} = \text{ inertia group.}$$

(4) If E is an unramified extension of F, then $(U_F, E/F) = \{1\}$ and thus U_F is in the norm group $N_{E/F}(E^\times)$. So $F^\times \to \mathrm{Gal}(E/F)$ induces $\mathbb{Z} \to \mathrm{Gal}(E/F)$ since $F^\times \simeq U_F \times \mathbb{Z}$.

(5) There is a one-to-one correspondence between

$$\left\{ \begin{array}{c} \text{finite abelian} \\ \text{extension } E \text{ of } F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{open subgroup } H \subseteq F^\times \\ \text{of finite index} \end{array} \right\}$$

$$E \longrightarrow N_{E/F}(E^\times)$$

We now return to $\mathbb{Z}_p$-extensions. Let k be a number field and K be a $\mathbb{Z}_p$-extension of k.

Proposition 2.1 Let v be a prime (may be infinite) of k such that $v \nmid p$. Then v is unramified in K.

Proof. Let w be a place of K extending v. Then

$$T(w|v) \subseteq Z(w|v) \subseteq \Gamma = \mathrm{Gal}(K/k),$$

where $Z(w|v)$ is the decomposition group. And $Z(w|v) \simeq \mathrm{Gal}(K_w/k_v)$. By the class field theory, $U_{k_v} \to T(w|v)$ is surjective. Note that

$$U_{k_v} \simeq \text{ finite} \times \mathbb{Z}_l^{[k_v:\mathbb{Q}_l]}, \quad \text{where } l \text{ is the prime such that } v|l.$$

Since U_{k_v} has no factor group isomorphic to $\mathbb{Z}_p$, $T(w|v) = \{1\}$. If $v|\infty$, then

$$Z(w|v) \simeq \mathrm{Gal}(K_w/k_v) = \text{ order 1 or 2 } \subseteq \Gamma.$$

Therefore, $Z(w|v) = T(w|v) = \{1\}$, and v splits completely in K/k. ∎

Since the Hilbert class field of k is finite over k, we have :

Corollary. Some prime above p must ramify.

Let $\Gamma_n = \mathrm{Gal}(K/k_n)$, thus $\mathrm{Gal}(k_n/k_0) \simeq \Gamma/\Gamma_n$. We consider the group ring $\mathbb{Z}_p[\Gamma/\Gamma_n]$ and its projective limit $\varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$ under the natural surjection (restriction) $\Gamma/\Gamma_m \to \Gamma/\Gamma_n$ for $m > n$. Let γ be a topological generator of Γ. Then the following map can be easily shown to be an isomorphism.

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma/\Gamma_n] & \xrightarrow{\sim} & \mathbb{Z}_p[T]/\big(w_n(T)\big) \\ \gamma \bmod \Gamma_n & \mapsto & 1+T \bmod (w_n(T)), \end{array}$$

where $w_n(T) = (1+T)^{p^n} - 1$ which is a distinguished polynomial. Moreover, the following diagram commutes : for $m > n$

$$\begin{array}{ccccc} \mathbb{Z}_p[\Gamma/\Gamma_m] & \xrightarrow{\sim} & \mathbb{Z}_p[T]/(w_m) & f \bmod w_m \\ \downarrow & & \downarrow & \downarrow \\ \mathbb{Z}_p[\Gamma/\Gamma_n] & \xrightarrow{\sim} & \mathbb{Z}_p[T]/(w_n) & f \bmod w_n \end{array}$$

Hence

$$\varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n] \simeq \varprojlim \mathbb{Z}_p[T]/(w_n) \simeq \varprojlim \mathbb{Z}_p[[T]]/(w_n).$$

Proposition 2.2 (Serre) $\varprojlim \mathbb{Z}_p[[T]]/(w_n) \simeq \mathbb{Z}_p[[T]]$.

Proof. We have a natural map

$$\begin{array}{ccc} \mathbb{Z}_p[[T]] & \longrightarrow & \varprojlim \mathbb{Z}_p[[T]]/(w_n) \\ f & \longmapsto & (\cdots, f \bmod w_n, \cdots) \end{array}$$

Check $w_n \in \mathfrak{m}^{n+1}$ by induction. Hence if $f \longmapsto 0$, then $f \in \bigcap \mathfrak{m}^{n+1} = (0)$. Let $(\cdots, f_n, \cdots) \in \varprojlim \mathbb{Z}_p[[T]]/(w_n)$. Then $f_{n+1} \equiv f_n \bmod w_n$, hence $\bmod \mathfrak{m}^{n+1}$. This implies that coefficients of $\{f_n\}$ of given degree are Cauchy and thus $\lim f_n = f$ exists and $f \longmapsto (\cdots, f_n, \cdots)$. ∎

Now we describe an important Λ-module. For each number field F, let H_F be the Hilbert class field of F, that is, the maximal abelian extension of F, unramified at all places. Then $\mathrm{Gal}(H_F/F) \simeq \mathrm{Cl}(F) =$ ideal class group of F. Let E be an extension of F. Then the following diagram is commutative :

$$\begin{array}{ccc} \mathrm{Gal}(H_E/E) & \xrightarrow{res} & \mathrm{Gal}(H_F/F) \\ \wr\updownarrow & & \wr\updownarrow \\ \mathrm{Cl}(E) & \xrightarrow[N]{norm} & \mathrm{Cl}(F) \end{array}$$

So N:$\mathrm{Cl}(E) \to \mathrm{Cl}(F)$ is surjective if and only if restriction map is surjective if and only if $E \bigcap H_F = F$. Thus, especially, N:$\mathrm{Cl}(E) \to \mathrm{Cl}(F)$ is surjective if E/F is totally ramified at some prime. We apply this to the $\mathbb{Z}_p$-extension K/k. By Corollary 2, K/k_{n_0} is totally ramified at some prime for some n_0. Hence N:$\mathrm{Cl}(k_m) \to \mathrm{Cl}(k_n)$ is surjective for all $m > n \geq n_0$. Let A_m be the Sylow p-subgroup of $\mathrm{Cl}(k_m)$. Then N:$A_m \to A_n$ is surjective for all $m > n \geq n_0$. Let H_n be the subfield of H_{k_n} such that $\mathrm{Gal}(H_n/k_n) \simeq A_n$. Let

$$X = \varprojlim A_n \simeq \varprojlim \mathrm{Gal}(H_n/k_n) = \varprojlim \mathrm{Gal}(KH_n/K) = \mathrm{Gal}(L/K),$$

where $L = \bigcup_{n \geq 0} KH_n$. $\mathrm{Gal}(k_n/k) = \Gamma/\Gamma_n$ acts on $\mathrm{Cl}(k_n)$, hence on A_n. Γ/Γ_n also acts on $\mathrm{Gal}(H_n/k_n)$ by inner automorphisms. And these two actions are compatible in the sense that

$$\left(\mathfrak{a},\, H_n/k_n\right)^{\sigma} = \left(\mathfrak{a}^{\sigma},\, H_n/k_n\right), \text{ for all } \sigma \in \Gamma/\Gamma_n,\ \ \mathfrak{a} \lhd k_n.$$

Hence A_n is isomorphic to the Sylow p-subgroup of $\mathrm{Gal}(H_n/k_n)$ as $\mathbb{Z}_p[\Gamma/\Gamma_n]$-modules. Therefore

$$\begin{array}{ccccc} \varprojlim A_n & \simeq & \varprojlim \mathrm{Gal}(H_n/k_n) & \text{as} & \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]\text{-modules.} \\ \| & & \| & & \| \\ X & & \mathrm{Gal}(L/K) & & \Lambda \end{array}$$

Exercise. Check actions are compatible with the maps involved in $\varprojlim$.

Theorem 2.1 X is a finitely generated torsion Λ-module.

Proof. For a while, we assume that primes of k that ramify in K are totally ramified. (One can ensure this by replacing k by k_{n_0} for some n_0). Let γ_0 be a topological generator of Γ, so γ_0 corresponds to $1+T$ under the map $\mathbb{Z}_p[[\Gamma]] \xrightarrow{\sim} \Lambda = \mathbb{Z}_p[[T]]$. Let $G = \mathrm{Gal}(L/k)$ and let L_0 the maximal abelian extension of k in L. Then $\mathrm{Gal}(L/L_0) = \overline{G'}$ is the closure of the commutator subgroup of G. Take a lift of γ_0 in G, call it γ_0 again. Let $\Gamma_0 = \overline{<\gamma_0>}$ be the subgroup of G generated by γ_0 in G. Since Γ_0 is an inertia subgroup of some prime, we have

$$\Gamma_0 \bigcap X = \{1\}, \qquad X\Gamma_0 = \Gamma_0 X = G,$$

since we are assuming that K is totally ramified over k.

Let $g,\ h \in G$, write $g = x\gamma_0^s,\ h = y\gamma_0^t$ with $x,\ y \in X$. Then

$$\begin{aligned} ghg^{-1}h^{-1} &= x\gamma_0^s y\gamma_0^t\gamma_0^{-s}x^{-1}\gamma_0^{-t}y^{-1} \\ &= x(\gamma_0^s y\gamma_0^{-s})(\gamma_0^t x^{-1}\gamma_0^{-t})y^{-1} \\ &= xy^{\gamma_0^s}(x^{-1})^{\gamma_0^t}y^{-1} \\ &= y^{\gamma_0^s-1}(x^{-1})^{\gamma_0^t-1}. \end{aligned}$$

So G' is generated by $\{y^{\gamma_0^s-1}\} \subset X$. Since $y^{\gamma_0^s-1} = ((1+T)^s-1)y \in TX$, $G' = TX$ and thus $\overline{G'} = G' = TX$. Therefore $\mathrm{Gal}(L/L_0) = TX$. Let $v_1, \ldots, v_s$ be the primes of k that ramify in K, hence in L_0 and L. Let T_i be the inertia group of v_i in L_0/k. Since the fixed field of $< T_1, \ldots, T_s >$ is the maximal unramified extension over k, $T_1 \cdots T_s = \mathrm{Gal}(L_0/H_0)$ is a finitely generated $\mathbb{Z}_p$-module. Since $\mathrm{Gal}(H_0/k)$ is finite, $\mathrm{Gal}(L_0/k)$ is a finitely generated $\mathbb{Z}_p$-module and so is its submodule $\mathrm{Gal}(L_0/K)$. Therefore $X/TX = \mathrm{Gal}(L_0/K)$

is a finitely generated $\mathbb{Z}_p$-module, hence a finitely generated Λ-module. Let $x_1 \bmod TX, \ldots, x_n \bmod TX$ be generators of X/TX as Λ-module. Then

$$\begin{aligned} X &= \Lambda x_1 + \cdots + \Lambda x_n + TX \\ &= \Lambda x_1 + \cdots + \Lambda x_n + T(\Lambda x_1 + \cdots + \Lambda x_n + TX) \\ &= \Lambda x_1 + \cdots + \Lambda x_n + T^2 X \\ &\quad \vdots \\ &= \Lambda x_1 + \cdots + \Lambda x_n + T^n X \end{aligned}$$

But for any neighborhood V of 0 in X, $T^n X \subset V$ for $n \gg 0$. Hence $\Lambda x_1 + \cdots + \Lambda x_n$ is dense in X. So $\Lambda x_1 + \cdots + \Lambda x_n = X$ is a finitely generated Λ-module.

Now we have to prove that X is a torsion Λ-module. Note that a finitely generated Λ-module Y is torsion if and only if Y/hY is finite for some $h \in \mathfrak{m}$. Let $Y_n = \mathrm{Gal}(L/KH_n)$, so that $A_n \simeq X/Y_n$. Let $T_i^{(n)} = T_i^{p^n}$ be the inertia group of v_i in L/k_n. Then

$$\mathrm{Gal}\,(L/H_n) = X^{\gamma_n - 1} T_1^{(n)} \cdots T_s^{(n)}, \quad \gamma_n = \gamma_0^{p^n}$$

and

$$Y_n = X \bigcap X^{\gamma_n - 1} T_1^{(n)} \cdots T_s^{(n)}.$$

Since $T_i \subset G = XT_1$, for each generator σ_i of T_i, $\sigma_i = x_i \gamma_0$ for some $x_i \in X$. Here γ_0 is taken to be a topological generator of T_1. So topological generator of $T_i^{(n)}$ is

$$\sigma_i^{p^n} = (x_i \gamma_0)^{p^n} = x_i^{1+\gamma_0+\cdots+\gamma_0^{p^n}} \gamma_0^{p^n}.$$

Hence

$$T_i^{(n)} = \overline{< \sigma_i^{p^n} >} = \overline{< x_i^{\delta_n} \gamma_0^{p^n} >} = \overline{< x_i^{\delta_n} \gamma_n >},$$

where $\delta_n = 1 + \gamma_0 + \cdots + \gamma_0^{p^n - 1}$. So

$$\begin{aligned} \mathrm{Gal}(L/H_n) &= X^{\gamma_n - 1} \overline{< \gamma_n, x_2^{\delta_n} \gamma_n, \ldots, x_s^{\delta_n} \gamma_n >} \\ &= X^{\gamma_n - 1} \overline{< \gamma_n, x_2^{\delta_n}, \ldots, x_s^{\delta_n} >} \\ &= X^{\gamma_n - 1} \overline{< x_2^{\delta_n} > \cdots < x_s^{\delta_n} >< \gamma_n >}. \end{aligned}$$

And

$$Y_n = X \bigcap \mathrm{Gal}(L/H_n) = X^{\gamma_n - 1} \overline{< x_2^{\delta_n} >} \cdots \overline{< x_s^{\delta_n} >}$$

$$= \overline{< w_n X, \frac{w_n}{w_0} x_2, \ldots, \frac{w_n}{w_0} x_s >}$$
$$= \frac{w_n}{w_0} \overline{< w_0 X, x_2, \ldots, x_s >}$$
$$= \frac{w_n}{w_0} Y_0.$$

Therefore

$$A_n = \mathrm{Gal}\,(KH_n/K) \simeq X/Y_n \simeq X/\frac{w_n}{w_0} Y_0.$$

Note that if there is only one prime in k that ramifies in K, then $Y_n = w_n X$ and $A_n = X/w_n X$. Since $\dfrac{w_n}{w_0} \in \mathfrak{m}$ and since

$$X/\frac{w_n}{w_0} Y_0 = A_n$$

is finite, X is a torsion module because $\dfrac{w_n}{w_0} Y_0 \subseteq \dfrac{w_n}{w_0} X$. Even if we do not assume that all $v_1, \ldots, v_s$ ramify totally, there is n_0 such that K/k_{n_0} is totally ramified. Hence

$$A_{n+n_0} \simeq X/Y_{n_0+n}, \qquad Y_{n_0+n} \simeq \frac{w_{n_0+n}}{w_{n_0}} Y_{n_0}. \qquad \blacksquare$$

Theorem 2.2 Let $\#A_n = p^{e_n}$. Then there are integers μ, λ, and ν ($\mu, \lambda \geq 0$) such that $e_n = \mu p^n + \lambda n + \nu$ for $n \gg 0$.

Proof. Let $\xi_n = \dfrac{w_n}{w_{n-1}} = \dfrac{(1+T)^{p^n} - 1}{(1+T)^{p^{n-1}} - 1}$ be the distinguished irreducible polynomial of $\zeta_{p^n} - 1$ over $\mathbb{Z}_p$.

Lemma 2.1 Let $Z \sim \oplus \Lambda/q_i^{e_i}$ where q_i are primes in Λ. Let $f = \prod q_i^{e_i}$. Suppose the maximal finite submodule Z^0 of Z is 0. Then for all $n \gg 0$,

$$\#\,(Z/\xi_n Z) = \prod_{\zeta} f(\zeta - 1) \cdot (\text{unit in } \mathbb{Z}_p)$$

where ζ runs over all prmitive p^n-th roots of 1.

Proof of Lemma. Apply Snake Lemma to :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Z & \longrightarrow & \oplus\Lambda/q_i^{e_i} & \longrightarrow & B \longrightarrow 0 \\ & & \downarrow \xi_n & & \downarrow \xi_n & & \downarrow \xi_n \\ 0 & \longrightarrow & Z & \longrightarrow & \oplus\Lambda/q_i^{e_i} & \longrightarrow & B \longrightarrow 0 \end{array}$$

By taking $n \gg 0$ so that ξ_n and f are relatively prime, we have

$$0 \to \ker(B \to B) \to Z/\xi_n Z \to \oplus\Lambda/(q_i^{e_i}, \xi_n) \to \mathrm{Coker}(B \to B) \to 0.$$

Since B is finite, $\#\ker(B \to B) = \#\mathrm{Coker}(B \to B)$. Thus

$$\#Z/\xi_n Z = \# \oplus \Lambda/(q_i^{e_i}, \xi_n).$$

Note $\Lambda/(\xi_n) \simeq \mathbb{Z}_p[T]/\xi_n(T)$ and $\mathbb{Z}_p[T]/\xi_n(T) \simeq \mathbb{Z}_p[\zeta_{p^n}]$ under the map sending T to $\zeta_{p^n} - 1$. Under this isomorphism, we obtain

$$\mathbb{Z}_p[T]/(q_i^{e_i}, \xi_n) \simeq \mathbb{Z}_p[\zeta_n]/(q_i^{e_i}(\zeta_{p^n} - 1)).$$

Hence $\#(\Lambda/(\xi_n, q_i^{e_i})) = N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}(q_i^{e_i}(\zeta_{p^n} - 1)) \times$ unit in $\mathbb{Z}_p$. Therefore

$$\begin{aligned} \#(Z/\xi_n Z) &= N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p} f(\zeta_{p^n} - 1) \times (\text{unit in } \mathbb{Z}_p) \\ &= \prod f(\zeta - 1) \times (\text{unit in } \mathbb{Z}_p). \end{aligned}$$ ∎

Lemma 2.2 Let Z and f be as before. Write $f = p^\mu(a_0 + a_1 T + a_2 T^2 + \cdots a_\lambda T^\lambda + \cdots)$ with $\mu = \mu(f)$, $\lambda = \lambda(f)$. Then

$$\#(Z/\xi_n Z) = p^{\mu(p^n - p^{n-1}) + \lambda} \qquad \text{for } n \gg 0.$$

Proof. For $n \gg 0$, $|f(\zeta_{p^n} - 1)|_p = \left|p^\mu(\zeta_{p^n} - 1)^\lambda\right|_p$. Hence

$$N(f(\zeta - 1)) = p^{\mu(p^n - p^{n-1}) + \lambda} \times \text{unit in } \mathbb{Z}_p.$$ ∎

Apply the above lemma to $X \simeq \mathrm{Gal}(L/K)$.

Lemma 2.3 $Y_m^0 = \{0\}$ for $m \gg 0$.

Proof. First take n large enough so that $\dfrac{w_t}{w_n}$ is relatively prime to f for all $t > n$. For such an n, consider Y_n^0. For each $z \in Y_n^0$, there exists an integer $m = m(z)$ such that $\dfrac{w_m}{w_n} z = 0$. The existence of such an $m(z)$ is left

as an exercise. Let $m = \max_z\{m(z) \mid z \in Y_n^0\}$. Then $\frac{w_m}{w_n}Y_n^0 = 0$. With this choice, we claim that $Y_m^0 = 0$. Take $y \in Y_m^0$. Since $Y_m = \frac{w_m}{w_n}Y_n = 0$, we can write $y = \frac{w_m}{w_n}y'$ for some $y' \in Y_n$. Then it suffices to show that $y' \in Y_n^0$. Since $fX \subset X^0$, $f^N X = 0$ for $N \gg 0$. Hence $f^N y' = 0$. Since Y_m^0 is finite, there exists h in $\mathfrak{m}$ which is relatively prime to f such that $hY_m^0 = 0$. Hence $h\frac{w_m}{w_n}y' = 0$. Therefore both f^N and $h\frac{w_m}{w_n}$ annihilates $\Lambda y'$. Since $h\frac{w_m}{w_n}$ were chosen to be relatively prime to f, $\Lambda y'$ is a finite set. This proves the claim. ∎

Proof of Theorem. Take $n \gg 0$ so that $Y_n^0 = 0$. Since $Y_n \sim X \sim \oplus\Lambda/(q_i^{e_i})$, We can apply Lemma 2.2 to obtain

$$[A_n : A_{n-1}] = \#(Y_{n-1}/Y_n) = \#(Y_{n-1}/\xi_n Y_{n-1}) = p^{\mu(p^n - p^{n-1})+\lambda}$$

since $Y_n = \frac{w_n}{w_{n_0}}Y_{n_0}$. Hence

$$e_n - e_{n-1} = \mu(p^n - p^{n-1}) + \lambda = (\mu p^n + \lambda n) - (\mu p^{n-1} + \lambda(n-1)).$$

Therefore $e_n = \mu p^n + \lambda n + \nu$ for some integer ν. ∎

Now we give a criterion of vanishing of the invariants μ and λ.

Corollary. (i) $\mu = 0$ if and only if $rank_{\mathbb{F}_p} A_n/pA_n$ is bounded as $n \to \infty$.

(ii) $\lambda = 0$ if and only if exponent of A_n is bounded as $n \to \infty$.

Proof. (i) Note that $\mu = 0$ if and only if $p \nmid f$ and $rank A_n/pA_n$ is bounded if and only if $rank Y_n/pY_n$ is bounded, where $Y_n = Y_{n_0}/\delta_n Y_{n_0}$, $\delta_n = \frac{w_n}{w_{n_0}}$. Suppose that $\mu = 0$. So $p \nmid f$ and thus X/pX is finite. Therefore Y_{n_0}/pY_{n_0} is also finite. Hence $rank Y_n/pY_n = rank Y_{n_0}/(p, \delta_n)Y_{n_0}$ is bounded by the rank Y_{n_0}/pY_{n_0}. Conversely, suppose $rank Y_{n_0}/pY_{n_0}$ is bounded. Then $rank \overline{Y}/\delta_n\overline{Y}$ is bounded, where $\overline{Y} = Y_{n_0}/pY_{n_0}$. Hence $\delta\overline{Y} = \delta_{n+1}\overline{Y}$ for some n. Thus we have $\delta_n\left(1 - \frac{\delta_{n+1}}{\delta_n}\right)\overline{Y} = 0$. But $1 - \frac{\delta_{n+1}}{\delta_n} = 1 - \frac{w_{n+1}}{w_n} \in \Lambda^\times$. Therefore $\delta_n\overline{Y} = 0$, and $\overline{Y} = Y_{n_0}/pY_{n_0}$ is a finite set. Thus X/pX is also finite and$p \nmid f$.
(ii) If $\lambda = 0$, then $X \sim \oplus\Lambda/(p^{a_i})$. Thus there exists an M such that $p^M X = 0$, hence that $p^M A_n = 0$. Conversely, if $p^M A_n = 0$ for some M, then $p^M(X/\delta Y_{n_0}) =$

0. Thus $p^M X \subset \delta Y_{n_0}$ for all $n \geq n_0$, hence $p^M X \subset \bigcap \delta_n Y_{n_0} = \{0\}$. Therefore $\lambda = 0$. ∎

Remark. (i) As was mentioned earlier, if only one prime ramifies and totally ramifies in K/k, then $A_n \simeq X/w_n X$. So $A_0 = \{0\}$ if and only if $X = TX$ if and only if $X = 0$ if and only if $A_n = \{0\}$. Therefore $p|h_0$ if and only if $p|h_n$, where h means the class number of appropriate level. Examples of such extensions are

(a) $k = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$ where p is an odd prime.

(b) $k = \mathbb{Q}$, $K = \mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$ where $\mathbb{Q}_n$ is the subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ such that $[\mathbb{Q}_n : \mathbb{Q}] = p^n$.

(c) $k = \mathbb{Q}(\zeta_4)$, $K = \mathbb{Q}(\zeta_{2^n}) = \bigcup_{n\geq 2} \mathbb{Q}(\zeta_{2^n})$.

(ii) Let $i_{n,m}: A_n \to A_m$ be the natural map induced by the map sending the ideal $\mathfrak{a}_n$ of K_n to $\mathfrak{a}_n \mathcal{O}_{K_m}$ for $n < m$, where $\mathcal{O}_{K_m}$ is the ring of integers of K_m. We leave the commutativity of the following diagram as an exercise ;

$$\begin{array}{ccc} A_n & \xrightarrow{i_{n,m}} & A_m \\ \downarrow\wr & & \downarrow\wr \\ X/\delta_n Y_{n_0} & \xrightarrow[w_n]{w_m} & X/\delta_m Y_{n_0} \end{array}$$

So we have the following exact sequence with commuting diagrams :

$$\begin{array}{ccccccccc} 0 & \to & \delta_n Y_{n_0} & \longrightarrow & X & \longrightarrow & A_n & \to & 0 \\ & & \downarrow{\scriptstyle w_m/w_n} & & \downarrow{\scriptstyle w_m/w_n} & & \downarrow{\scriptstyle i_{n,m}} & & \\ 0 & \to & \delta_m Y_{n_0} & \longrightarrow & X & \longrightarrow & A_m & \to & 0 \end{array}$$

Choose $m \gg n \gg 0$ so that $(\delta_n Y_{n_0})^0 = 0$ and $\ker(X \xrightarrow{w_m/w_n} X) = X^0$. Then by appling the Snake lemma, we have

$$X^0 \simeq \ker(A_n \xrightarrow{i_{n,m}} A_m) \quad \text{for} \quad m \gg n \gg 0.$$

(iii) Suppose k is a C.M. field *i.e.*, totally complex quadratic extension of a totally real field k^+. Then its $\mathbb{Z}_p$-extension is also a C.M. field over K^+ and K^+/k^+ is a $\mathbb{Z}_p$-extension. Suppose p is an odd prime. Let $A_n^+ = \{c \in A_n \mid jc = c\}$ and $A_n^- = \{c \in A_n \mid jc = -c\}$, where j is the complex conjugation. Then $A_n = A_n^+ \oplus A_n^-$ since $c = \frac{1+j}{2}c + \frac{1-j}{2}c$. Hence $X = \varprojlim A_n =$

$\varprojlim A_n^+ \oplus \varprojlim A_n^- = X^+ \oplus X^-$, where $X^\pm = \varprojlim A_n^\pm$. So we can define $\mu^\pm$, $\lambda^\pm$ and $\nu^\pm$ so that $\mu = \mu^+ + \mu^-$, $\lambda = \lambda^+ + \lambda^-$ and $\nu = \nu^+ + \nu^-$.

Definition 2.1 A $\mathbb{Z}_p$-extension K/k is called a basic (or cyclotomic) $\mathbb{Z}_p$-extension if $K = k\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty/\mathbb{Q}$ is the $\mathbb{Z}_p$-extension explained in the above remark.

Theorem 2.3 Suppose p is an odd prime and K/k is a cyclotomic $\mathbb{Z}_p$-extension over a C.M. field k. Then $i_{n,m}: A_n^- \to A_m^-$ is injective. Hence $(X^-)^0 = (X^0)^- = \{0\}$.

Proof. It is enough to show that $i_{n,n+1}: A_n^- \to A_{n+1}^-$ is injective. Suppose $i(a) = 0$ for some $a \in A_n^-$. Write $a = 2b$ for some $b \in A_n^-$, so $a = (1-j)b$ and $i(b) = 0$. Take an ideal $\mathfrak{b}$ such that $[\mathfrak{b}] = b$. since $i(b) = 0$, $\mathfrak{b} = (\beta)$ for some $\beta \in k_{n+1}$. Let $\mathfrak{a} = \mathfrak{b}^{1-j}$ and $\alpha = \beta^{1-j}$. Then $[\mathfrak{a}] = a$. Let σ be a generator of $\mathrm{Gal}(k_{n+1}/k_n)$. Since $\mathfrak{a}^\sigma = \mathfrak{a}$, $(\alpha^\sigma) = (\alpha)$. Hence $\alpha^{\sigma-1} = \eta$ is a unit in k_{n+1}. By taking the norm of η from k_{n+1} to k_{n+1}^+, we have $N(\eta) = N(\alpha^{\sigma-1}) = N((\beta^{\sigma-1})^{1-j}) = 1$. Since k is a C.M. field, this implies that $|\eta|_v = 1$ for any archimedian place v. Therefore η is a root of 1 and its norm to k_n is $N(\eta) = N(\alpha^{\sigma-1}) = 1$. Since $H^1(<\sigma>, \{\text{root of 1 in } k_{n+1}\}) = 0$, $\eta = \xi^{\sigma-1}$ for some ξ, a root of 1. Hence $\alpha^{\sigma-1} = \xi^{\sigma-1}$, so $\alpha = \xi\alpha_0$ for some $\alpha_0 \in k_n$. Therefore $\mathfrak{a} = (\alpha) = (\alpha_0)$. ∎

Corollary. Let K/k as in the theorem. If $X^- \neq 0$, then either $\lambda^- \text{ or } \mu^- > 0$. Hence, in particular, if $A_n^- \neq 0$ for some n, then $\lambda^- \text{ or } \mu^- > 0$.

Remark. (i) Let $k = \mathbb{Q}(\zeta_p)$. Since $p|h^+$ implies $p|h^-$, if p is irregular, then $\lambda^- > 0$.
(ii) The structure of X^+ is not well understood even when $k = \mathbb{Q}(\zeta_p)$. We introduce two conjectures.
(a) Greenberg's conjecture: $\lambda^+ = 0$ for every C.M. field K/k.
(b) Vandiver's conjecture: $p \nmid h_0^+$ when $k = \mathbb{Q}(\zeta_p)$.

§ 3. Stickelberger Theorem

Let m be a positive integer not congruent to 2 mod 4. Let $k = \mathbb{Q}(\zeta_m)$ and $G = \mathrm{Gal}(k/\mathbb{Q})$. In this section, we will find elements of $\mathbb{Z}[G]$ which annihilate

the ideal class group $\mathrm{Cl}(k)$ of k under the obvious action of G on $\mathrm{Cl}(k)$.

We need some properties of power residue symbol and its Gauss sum. Let q be a prime congruent to 1 mod m so that q splits completely in k. Let $\mathfrak{q}$ be one of the prime ideals of k above q. Since q splits in k, $\mathcal{O}/\mathfrak{q} \simeq \mathbb{Z}/q$, where $\mathcal{O}$ is the ring of integers of k. Then $(\mathcal{O}/\mathfrak{q})^\times \simeq (\mathbb{Z}/q)^\times$ is a cyclic group of order $q-1$. Since $m|q-1$, $(\mathcal{O}/\mathfrak{q})^\times$ has a unique subgroup of order m. We can take $\mu_m = \{\zeta_m^i \,|\, 0 \le i < m\}$ as a set of representatives in $\mathcal{O}$ for this unique subgroup of $(\mathcal{O}/\mathfrak{q})^\times$ of order m, since $\zeta_m^i \not\equiv \zeta_m^j \bmod \mathfrak{q}$ if $i \neq j$. For any $x \in \mathcal{O} - \mathfrak{q}$, $(x^{\frac{q-1}{m}})^m \equiv 1 \bmod \mathfrak{q}$. Hence $x^{\frac{q-1}{m}} \equiv \zeta \bmod \mathfrak{q}$ for some $\zeta \in \mu_m$.

Definition 3.1 The m th power residue symbol $\left(\frac{\cdot}{\mathfrak{q}}\right)_m$ is a map

$$\left(\frac{\cdot}{\mathfrak{q}}\right)_m : \mathcal{O} - \mathfrak{q} \to \mu_m \text{ satisfying } \left(\frac{x}{\mathfrak{q}}\right)_m \equiv x^{\frac{q-1}{m}} \bmod \mathfrak{q}.$$

Definition 3.2 For any integer a, the Gauss sum $g_a(\mathfrak{q})$ attached to $\left(\frac{\cdot}{\mathfrak{q}}\right)_m$ is defined by

$$g_a(\mathfrak{q}) = -\sum_{x=1}^{q-1} \left(\frac{x}{\mathfrak{q}}\right)_m^a \zeta_q^x.$$

Note that $g_a(\mathfrak{q})$ is an algebraic integer in $\mathbb{Q}(\zeta_{qm})$. And if $m = 2$, $\left(\frac{\cdot}{\mathfrak{q}}\right)_m$ is just the Legedere symbol, and $g_1(\mathfrak{q})$ is the usual Gauss sum. Thus it is not suprising to expect that $g_a(\mathfrak{q})$ enjoy those properties satisfied by the Gauss sums coming from Legedere symbol or other characters. In the following propositions, we state some properties of $\left(\frac{\cdot}{\mathfrak{q}}\right)_m$ and $g_a(\mathfrak{q})$ without proofs.

Proposition 3.1 (i) $\left(\frac{xy}{\mathfrak{q}}\right)_m = \left(\frac{x}{\mathfrak{q}}\right)_m \left(\frac{y}{\mathfrak{q}}\right)_m$.

(ii) For $\sigma \in G = \mathrm{Gal}(k/\mathbb{Q})$, $\left(\frac{x}{\mathfrak{q}}\right)^\sigma = \left(\frac{x}{\mathfrak{q}^\sigma}\right)_m$ if $x \in \mathbb{Z}$.

Proposition 3.2 (i) If $m|a$, then $g_a(\mathfrak{q}) = 1$.

(ii) If $m \nmid a$, then $g_a(\mathfrak{q})\overline{g_a(\mathfrak{q})} = q$.

(iii) $\sigma_t g_a(\mathfrak{q}) = \begin{cases} g_{at}(\mathfrak{q}) & \text{if } t \equiv 1 \bmod q \\ \left(\frac{t}{\mathfrak{q}}\right)_m^{-a} g_a(\mathfrak{q}) & \text{if } t \equiv 1 \bmod m. \end{cases}$

Now assume that $m \nmid a$. Since $g_a(\mathfrak{q})$ depends on $a \bmod m$, we may also assume that $1 \leq a < m$. From Proposition 3.2 (ii), the prime ideals of $\mathbb{Q}(\zeta_{qm})$ that can divide the principal ideal $(g_a(\mathfrak{q}))$ are those above q. We will find the explicit factorization of $(g_a(\mathfrak{q}))$ in $\mathbb{Q}(\zeta_{qm})$. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Q}(\zeta_{qm})$ above $\mathfrak{q}$ and i be the power of $\mathfrak{P}$ in the factorization of $(g_a(\mathfrak{q}))$, *i.e.*, $(g_a(\mathfrak{q})) = \mathfrak{P}^i\mathfrak{b}$ for some ideal $\mathfrak{b}$ prime to $\mathfrak{P}$. Note that $\mathfrak{P}$ is totally ramified over $\mathfrak{q}$ and so $\mathbb{Q}(\zeta_m)$ is the inertia field of $\mathbb{Q}(\zeta_{qm})$ for $\mathfrak{P}$ over $\mathfrak{q}$. Thus for any algebraic integer α in $\mathbb{Q}(\zeta_{qm})$ and for any $\sigma_t$with $t \equiv 1 \bmod m$, we have $\alpha^{\sigma_t} \equiv \alpha \bmod \mathfrak{P}$. This congruence is also valid when we take α from the ring of integers $\mathcal{O}_{\mathfrak{P}}$ of $K_{\mathfrak{P}}$, the completion of $K = \mathbb{Q}(\zeta_{qm})$ at $\mathfrak{P}$, *i.e.*, $\alpha^{\sigma_t} \equiv \alpha \bmod \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$ for every $\alpha \in \mathcal{O}_{\mathfrak{P}}$. We take $\alpha = \dfrac{g_a(\mathfrak{q})}{(1-\zeta_q)^i}$. Then $\alpha \in \mathbb{Q}(\zeta_{qm})$. If we view α as an element of $K_{\mathfrak{P}}$, α is a unit in $\mathcal{O}_{\mathfrak{P}}$. Thus $\alpha^{\sigma_t} \equiv \alpha \bmod \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. Since α is a unit, we can write this congruence as $\dfrac{\alpha^{\sigma_t}}{\alpha} \equiv 1 \bmod \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. By Proposition 3.2 (iii), $\alpha^{\sigma_t} = \left(\dfrac{t}{\mathfrak{q}}\right)^{-a} \dfrac{g_a(\mathfrak{q})}{(1-\zeta_q^t)^i}$. Hence $\dfrac{\alpha^{\sigma_t}}{\alpha} = \left(\dfrac{t}{\mathfrak{q}}\right)^{-a}\left(\dfrac{1-\zeta_q}{1-\zeta_q^t}\right)^i \equiv 1 \bmod \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. Since $\dfrac{1-\zeta_q}{1-\zeta_q^t}$ is a unit in $\mathcal{O}_{\mathfrak{P}}$, we have

$$\left(\frac{t}{\mathfrak{q}}\right)^{-a} \equiv \left(\frac{1-\zeta_q^t}{1-\zeta_q}\right)^i \equiv t^i \bmod \mathfrak{P}\mathcal{O}_{\mathfrak{P}}.$$

Since $\left(\dfrac{t}{\mathfrak{q}}\right) \in \mathbb{Q}(\zeta_m)$, $\left(\dfrac{t}{\mathfrak{q}}\right)^{-a} \equiv t^i \bmod \mathfrak{q}$. Therefore $t^{\frac{q-1}{m}(-a)} \equiv t^i \bmod \mathfrak{q}$, hence mod q. If we take a generator of $(\mathbb{Z}/q\mathbb{Z})^\times$ for t, we obtain $\dfrac{q-1}{m}(-a) \equiv i \bmod q-1$. By Proposition 3.2 (ii), i is less than $q-1$. Hence $i = (q-1)\left\langle -\dfrac{a}{m} \right\rangle$ where $< x >$ denotes the real number such that $0 \leq < x > < 1$ and $x - < x >$ is an integer. Thus we have found that $i = (q-1)\left\langle -\dfrac{a}{m} \right\rangle$ is the power of $\mathfrak{P}$ in the factorization of $(g_a(\mathfrak{q}))$. We use this for the complete factorization of $(g_a(\mathfrak{q}))$

in the following proposition .

Proposition 3.3 $(g_a(\mathfrak{q})) = \mathfrak{P}^{(q-1)\sum_{\sigma_t \in G} \langle \frac{-at}{m} \rangle \sigma_t^{-1}}$.

Proof. As was mentioned, the only prime ideals of $\mathbb{Q}(\zeta_{qm})$ that can divide $(g_a(\mathfrak{q}))$ are those above q. Let $\mathfrak{P}'$ be one of those. Then $\mathfrak{P}' = \mathfrak{P}^{\sigma_t^{-1}}$ for some σ_t, $t \equiv 1 \bmod q$. If j is the power of $\mathfrak{P}'$ in $(g_a(\mathfrak{q}))$, then j is the power of $\sigma_t(\mathfrak{P}') = \mathfrak{P}$ in $\sigma_t(g_a(\mathfrak{q})) = g_{at}(\mathfrak{q})$. Hence $j = (q-1)\left\langle -\frac{at}{m} \right\rangle$. Therefore

$$(g_a(\mathfrak{q})) = \prod_t \mathfrak{P}^{\sigma_t^{-1} j} = \prod_t \mathfrak{P}^{\sigma_t^{-1}(q-1)\langle -\frac{at}{m} \rangle} = \mathfrak{P}^{(q-1)\sum_{\sigma_t} \langle -\frac{at}{m} \rangle \sigma_t^{-1}}. \quad \blacksquare$$

Now we are ready to find annihilators of $\mathrm{Cl}(k)$. For any integer a, define a Stickelberger element $\theta(a)$ by

$$\theta(a) = \sum_{\sigma_t \in G} \left\langle -\frac{at}{m} \right\rangle \sigma_t^{-1}.$$

Then $\theta(a)$ is an element in the group ring $\mathbb{Q}[G]$. Let S' be the $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G]$ generated by $\theta(a), a \in \mathbb{Z}$, and let $S = S' \bigcap \mathbb{Z}[G]$. Then S is an ideal in $\mathbb{Z}[G]$ which is called the Stickelberger ideal of k. In Theorem 1, we will show that elements in S annihilate $\mathrm{Cl}(k)$. First we describe elements of S more explicitly.

Lemma 3.1 S is the abelian group generated by $\{\theta(a) - a\theta(1)\}, a \in \mathbb{Z}$.

Proof. Since $\left\langle -\frac{at}{m} \right\rangle - a\left\langle -\frac{t}{m} \right\rangle \in \mathbb{Z}$, $\theta(a) - a\theta(1) \in S$. For the converse, note that $\sigma_c\theta(a) = \theta(ca)$ for any $\sigma_c \in G$. Hence any element in S is of the form $\sum_a x_a\theta(a)$ for some integer x_a. Since $\sum x_a\theta(a) = \sum x_a(\theta(a) - a\theta(1)) + (\sum a x_a)\theta(1)$, and since $\theta(a) - a\theta(1) \in S$, $\sum x_a\theta(a) \in S$ if and only of $\sum a x_a$ is divisible by m. But $-m\theta(a) = \theta(m+1) - (m+1)\theta(1)$. Therefore if $\sum x_a\theta(a)$ is in S, then it is of the form $\sum y_a(\theta(a) - a\theta(1))$. This proves the Lemma. $\blacksquare$

Theorem 3.1 (Stickelberger Theorem) S annihilates $\mathrm{Cl}(k)$.

Proof. By Lemma 3.1, it is enough to show that $\theta(a) - a\theta(1)$ annihilates $\mathrm{Cl}(k)$ for any integer a such that $m \nmid a$. Let C be any ideal class in $\mathrm{Cl}(k)$. One can choose, for a representative of C, a prime ideal $\mathfrak{q}$ such that the residue class degree $f(\mathfrak{q}) = 1$ by the Tchebotarev density theorem. Let q be the prime in $\mathbb{Z}$ below $\mathfrak{q}$, so $q \equiv 1 \bmod m$. We have to show that $\mathfrak{q}^{\theta(a)-a\theta(1)}$ is principal. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Q}(\zeta_{qm})$ above $\mathfrak{q}$. Then by Proposition 3.3, $(g_a(\mathfrak{q})) = \mathfrak{P}^{(q-1)\theta(a)}$. Hence

$$\left(\frac{g_a(\mathfrak{q})}{g_1(\mathfrak{q})^a}\right) = \frac{\mathfrak{P}^{(q-1)\theta(a)}}{\mathfrak{P}^{(q-1)\theta(1)a}} = \mathfrak{P}^{(q-1)(\theta(a)-a\theta(1))} = \mathfrak{q}^{\theta(a)-a\theta(1)}.$$

Therefore our theorem follows once we check that $\dfrac{g_a(\mathfrak{q})}{g_1(\mathfrak{q})^a}$ is in k. For this, let $t \equiv 1 \bmod m$. Then

$$\sigma_t\left(\frac{g_a(\mathfrak{q})}{g_1(\mathfrak{q})^a}\right) = \frac{\left(\frac{t}{\mathfrak{q}}\right)^{-a} g_a(\mathfrak{q})}{\left(\left(\frac{t}{\mathfrak{q}}\right)^{-1} g_1(\mathfrak{q})\right)^a} = \frac{g_a(\mathfrak{q})}{g_1(\mathfrak{q})^a}.$$

This finishes the proof. ∎

Remark. (i) K. Iwasawa proved that when m is a prime power, $[\mathbb{Z}[G]^- : S^-] = h^-$, where the superscript $-$ has the same meaning as in §2 and $h^- = \dfrac{h}{h^+}$ is the relative class number. W. Sinnott generalized this to arbitrary m. Namely, $[\mathbb{Z}[G]^- : S^-] = 2^a h^-$, where a is an integer depending on the number of prime divisors of m. These formulas are algebraic interpretation of the so called analytic class number formula. There is a similar algebraic interpretation for h^+ by using cyclotomic units. For detail, we refer [3], [8].
(ii) One can generalize Stickelberger theorem to the case when k is any abelian field. More generally, even when K is an abelian extension of a totally real field F, one can define some kind of Stickelberger ideal $S_n(K/F)$ coming from Hurwitz zeta function so that $S_n(K/F)$ annihilates K-groups. For more discussions, refer [1], [6].

As an application of Stickelberger theorem, we introduce Herbrand theorem. Let G be a finite abelian group and $\widehat{G}$ be its character group. For each $\chi \in \widehat{G}$, define ε_χ by

$$\varepsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}.$$

Then ε_χ is an element of $\overline{\mathbb{Q}}[G]$, or an element of any group ring $R[G]$ if R contains all the values $\chi(\sigma)$ and if $|G|$ is invertible in R. The followings are easy to check.

Proposition 3.4 (i) $\varepsilon_\chi^2 = \varepsilon_\chi$.

(ii) $\varepsilon_\chi \varepsilon_\psi = 0$ if $\chi \neq \psi$.

(iii) $\sum_\chi \varepsilon_\chi = 1$.

(iv) $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$.

Because of the properties (i) and (ii) ε_χ's are called orthogonal idempotents of $\overline{\mathbb{Q}}[G]$ or of $R[G]$ for suitable R. Let M be a $\overline{\mathbb{Q}}[G]$-module or an $R[G]$-module for suitable R. Then $\varepsilon_\chi M = M_\chi$ is a submodule of M. In fact, by the property (iv), it is the eigenspace with the eigenvalue $\chi(\sigma)$ of the automorphism $\sigma: M \to M$. By (iii), M is the sum of these eigenspaces. Since ε_χ's are orthogonal idempotents, $M = \bigoplus_\chi \varepsilon_\chi M$.

We apply this discussion to the following situation. Let $k = \mathbb{Q}(\zeta_p)$ for an odd prime p. Let A be the Sylow p-subgroup of the ideal class group of k. Then A is a $\mathbb{Z}_p[G]$-module, where $G = \mathrm{Gal}(k/\mathbb{Q})$. Let $\omega: G \to \mathbb{Z}_p$ be the Teichmüller character so that $\omega(\sigma_a) = \omega(a) \equiv a \bmod p$. Then $\widehat{G} = \{\omega^i \mid 0 \leq i \leq p-2\}$. We abbreviate ε_{ω^i} by ε_i for $0 \leq i \leq p-2$. The above discussion shows that $A \simeq \oplus A_i$, where $A_i = \varepsilon_i A$. We will analyze each A_i. Let $\theta = \theta(1) = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1}$. Then

$$\varepsilon_i \theta = \left(\frac{1}{p}\sum a\omega^{-i}(a)\right)\varepsilon_i = B_{1,\omega^{-i}}\varepsilon_i$$

and so

$$\varepsilon_i(c - \sigma_c)\theta = (c - \omega^{-i}(c))B_{1,\omega^{-i}}\varepsilon_i,$$

where $B_{1,\omega^{-i}}$ is the first Bernoulli number associated to the character ω^{-i}. Since $(c - \sigma_c)\theta$ annihilates A by the Stickelberger theorem, $(c - \omega^{-i}(c))B_{1,\omega^{-i}}$ annihilates A_i for all integers c. We examine this for various i's case by case. If i is nonzero and even, then $B_{1,\omega^{-i}} = 0$. Thus we get no information. If $i = 0$, then $B_{1,\omega^{-i}} = \frac{1}{2}$. Thus $\frac{c-1}{2}$ annihilates A_0. But we can certainly choose c so that $\frac{c-1}{2}$ is prime to p. Therefore $A_0 = 0$. This is

also clear since $\varepsilon_0 = \frac{1}{p-1}\text{Norm}$. Suppose $i = 1$. We take $c = 1 + p$. Then $(c - \omega(c))B_{1,\omega^{-1}} \equiv pB_{1,\omega^{-1}} \equiv \sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv p - 1 \bmod p$. Hence $A_1 = 0$. Finally, suppose i is odd, not equal to 1. We take c so that $c - \omega^{-i}(c) \not\equiv 0 \bmod p$. Then $B_{1,\omega^{-i}}$ annihilates A_i. So if $A_i \neq 0$, then $B_{1,\omega^{-i}} \equiv 0 \bmod p$. Since $B_{1,\omega^{-i}} \equiv \dfrac{B_{p-i}}{p-i} \bmod p$, we have the following theorem.

Theorem 3.2 (Herbrand theorem) Let i be odd with $3 \leq i \leq p-2$. If $A_i \neq 0$, then $p | B_{p-i}$.

Remark. (i) The converse of Herbrand theorem is also true. This much deeper theorem was proved by Ribet: if $p | B_{p-i}$ for some odd i, $3 \leq i \leq p-2$, then $A_i \neq 0$.
(ii) The number of such i's is called the index of irregularity, *i.e.*,

$$i(p) = \text{ index of irregularity } = \#\{i \mid i = \text{odd},\ 3 \leq i \leq p-2,\ p | B_i\}.$$

Clearly, $\dim_{\mathbb{F}_p} A^-/pA^- \geq i(p)$ since $\sum_{i=odd} \varepsilon_i = \dfrac{1-\sigma_{-1}}{2}$, $A^- = \bigoplus_{i=odd} A_i$. It is an open question whether or not $\dim_{\mathbb{F}_p} A^-/pA^- = i(p)$. Vandiver's conjecture ($p \nmid h^+$) is known to give an affirmative answer to this question.

References

[1] J. Coates, p-adic L-functions and Iwasawa's theory, Algebraic Number Fields (Durham Symposium, 1975; ed. by A. Fröhlich), 269–353. Academic Press: London, 1977

[2] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., 65 (1959), 183–226

[3] K. Iwasawa, On the theory of cyclotomic fields, Ann. of Math. (2), 70 (1959), 530–561

[4] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. (2), 98 (1973), 246–326. MR 50: 2120

[5] S. Lang, Algebraic Number Theory, Addison-Wesley.

[6] S. Lang, Cyclotomic Fields, GTM. Springer-Verlag: New York, 1978

[7] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. Math., 34 (1976), 151–162.

[8] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math., (2), 108 (1978), 107–134.

[9] L. Washington, Introduction of Cyclotomic Fields, GTM 83, Springer-Verlag: New York, 1980

Classical Theory of Modular Forms - An Introduction

Myung-Hwan Kim

Department of Mathematics
Seoul National University
Seoul 151–742, Korea

Contents

1. Prologue

1.1 Golay Code

Definition 1. *A binary code of length n is a subset C of $\mathbb{F}_2^n$. For $x, y \in C$, let $d(x,y)$ be the distance of x, y in C defined to be the number of coordinates in which x and y differ.*

Definition 2. *The distance $d(C)$ of a code C is defined by*

$$d(C) = min\{d(x,y) : \ x, y \in C, \ x \neq y\}.$$

We introduce Golay code $G \subseteq \mathbb{F}_2^{24}$. G is a 12-dimensional subspace of $\mathbb{F}_2^{24}$ spanned by the rows of the matrix

$$\begin{pmatrix} {}^t\underline{1} & I_{11} & {}^t\underline{0} & H \\ 0 & \underline{0} & 1 & \underline{1} \end{pmatrix} \in M_{12\times 24}(\mathbb{F}_2)$$

where $\underline{1} = (1, 1, \cdots, 1)$, $\underline{0} = (0, 0, \cdots, 0) \in \mathbb{F}_2^{11}$ and $H \in M_{11}(\mathbb{F}_2)$ is defined as follows :
Let $Q = (q_{ij})$, $q_{ij} = \left(\frac{i-j}{11}\right)$, $1 \leq i, j \leq 11$, where $(-)$ is the extended Legendre symbol. H is the matrix obtained from $Q - I_{11}$ by replacying 1 by 0 and -1 by 1. It is not hard to show $d(G) = 8$. So G give us a very good error correcting code which can correct up to 3 errors ; for $e \in \mathbb{F}_2^{24}$, there exists a unique $c \in G$ such that $d(e,c) \leq 3$ if exists.

1.2 Sphere Packing

Definition 3. *A lattice L of rank n is a discrete subgroup of $\mathbb{R}^n$ such that $\mathbb{R}^n/L$ is of finite volumn.*

Let $l_1, l_2, \cdots, l_n$ be a $\mathbb{Z}$-basis of L. We set $A_L = (a_{ij})$, $a_{ij} = < l_i, l_j >$, where $<,>$ is the Euclidean inner product. Then A is symmetric, positive definite $n \times n$ matrix. Observe that

$$\text{vol}(\mathbb{R}^n/L) = \sqrt{\det A_L}.$$

Also note that L can be regarded as a positive definite quadratic module.

Definition 4. *A sphere packing S on L is a packing of $(n-1)$-spheres of the same diameter centered at lattice points of L without overlapping. The density $\delta_L(S)$ of a sphere packing S on L is defined by*

$$\delta_L(S) = vol((n-1)\text{-}sphere)/\sqrt{detA_L}.$$

Definition 5. *The dense sphere packing on L is the sphere packing on L with the maximal density.*

Let δ_L be the density of the dense sphere packing on L. Then

$$\delta_L = \text{vol}((n-1)\text{-sphere of diameter } \lambda)/\sqrt{\det A_L},$$

where $\lambda = \min\{<l,l> : \ l \in L - \{0\}\}$.
So if $rank(L)$ and $\det A_L$ are given, then density gets larger as the minimal vector gets longer.

Question. For a given rank n, find a lattice on which the densest sphere packing is possible after normalizing L to have $\det A_L = 1$.

Remark 1. *Among 24 dimensional even unimodular lattices, the so called Leech lattice gives the densest sphere packing.*

1.3 Leech Lattice

Definition 6. *Let L be a lattice on $\mathbb{R}^n$. L is unimodular if $A_L \in GL_n(\mathbb{Z})$. L is even if $<l,l> \in 2\mathbb{Z}$ for any $l \in L$.*

Fact 1. *(1) Let L be an even unimodular lattice on $\mathbb{R}^n$. Then 8 divide n.*

(2) The Leech lattice is even unimodular on $\mathbb{R}^{24}$ and it contains no vector of length 2. In fact, this is the only such lattice on $\mathbb{R}^{24}$ (up to equivalence).

Remark 2. *There are 23 other classes of even unimodular lattices on $\mathbb{R}^{24}$ (Niemeier). They all have vectors of length 2. We give the definition of Leech lattice Λ. Λ is the set of the points*

$$\frac{1}{2\sqrt{2}}(\underline{0} + 2c + 4x), \quad \frac{1}{2\sqrt{2}}(\underline{1} + 2c + 4y)$$

where $\underline{0} = (0,\cdots,0)$, $\underline{1} = (1,\cdots,1)$, $x = (x_1,\cdots,x_{24})$ and $y = (y_1,\cdots,y_{24}) \in \mathbb{R}^{24}$ such that $\sum x_i \equiv 0\,(mod\,2)$, $\sum y_i \equiv 1\,(mod\,2)$, and $c \in G$, Golay code.

1.4 Theta Functions

Let L be an even unimodular lattice on $\mathbb{R}^n$. We set

$$r_L(m) = |\{l \in L : < l, l >= 2m\}|$$

and define

$$\vartheta_L^*(q) = \sum_{m \geq 0} r_L(m) q^m. \tag{1.1}$$

It is not hard to check that $\vartheta_L^*(q)$ is holomorphic on the open unit disc $\{q \in \mathbb{C} : |q| < 1\}$. We substitute $q = e^{2\pi i z}$ and get

$$\vartheta_L(z) = \vartheta_L^*(q) = \sum_{m \geq 0} r_L(m) e^{2\pi i m z}. \tag{1.2}$$

Then $\vartheta_L(z)$ is holomorphic on the open upper half plane

$$\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im} z > 0\}.$$

And $\vartheta_L(z)$ is also holomorphic at ∞. We call $\vartheta_L(z)$ the theta function associated to L. Observe that

$$\vartheta_L(Z) = \sum_{x \in L} e^{\pi i < x, x > z}, \quad z \in \mathfrak{H}. \tag{1.3}$$

We also have :

$$\vartheta_L(z+1) = \vartheta_L(z) \quad \text{and} \quad \vartheta_L(-\frac{1}{z}) = (-iz)^{n/2} \vartheta_L(z), \tag{1.4}$$

These two conditions characterize ϑ_L as a modular form of weight $\frac{n}{2}$, with respect to $\mathrm{SL}_2(\mathbb{Z})$. The first equality is obvious. The second equality can be proved by using Poisson summation formula. For a rapidly decreasing smooth function $f(x)$ on $\mathbb{R}^n$, Poisson summation formula gives

$$\sum_{x \in L} f(x) = \frac{1}{v} \sum_{y \in L^*} \hat{f}(y), \tag{1.5}$$

where L is a lattice on $\mathbb{R}^n$, L^* is the dual of L, $v = \mathrm{vol}(\mathbb{R}^n / L)$ and

$$\hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i < x, y >} f(x) dx$$

is the Fourier transform of $f(x)$. Since L is unimodular, we have $v = 1$ and $L = L^*$. It suffices to prove the equality for $z = it$, $t > 0$. We now let $f(x) = e^{-\pi<x,x>}$. Then

$$\widehat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i<x,y>} e^{-\pi<x,x>} dx = e^{-\pi<y,y>}$$

because the Fourier transformation of $e^{-\pi x^2}$ is $e^{-\pi y^2}$. Combining all these, we have

$$\vartheta_L(it) = \sum_{x\in L} e^{-\pi<x,x>t} = \sum_{x\in\sqrt{t}L} e^{-\pi<x,x>}.$$

Clearly

$$\mathrm{vol}(\mathbb{R}^n/\sqrt{t}L) = t^{n/2} \text{ and } (\sqrt{t}L)^* = \frac{1}{\sqrt{t}}L.$$

Therefore, by the Poisson summation formula,

$$\vartheta_L(it) = t^{-n/2} \sum_{y\in\frac{1}{\sqrt{t}}L} e^{-\pi<y,y>} = t^{-n/2} \sum_{y\in L} e^{-\pi<y,y>/t} = t^{-n/2}\vartheta_L(-\frac{1}{it}),$$

and hence $\vartheta_L(-\frac{1}{z}) = (-iz)^{n/2}\vartheta_L(z)$ by replacing $z = it$, as desired.

Remark 3. *On $\mathbb{R}^{24}$, we know there are 24 even unimodular lattices L. To each of them, one can correspond $\vartheta_L(z)$. One notable fact is that this correspondence is not one to one. There are only 19 distinct theta functions that can be corresponded.*

2. Modular Forms

2.1 The Modular Group

Let $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}z > 0\}$. For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathfrak{H}$, we set

$$Mz = \frac{az+b}{cz+d}. \tag{2.1}$$

Since $\mathrm{Im}Mz = \frac{\mathrm{Im}z}{|cz+d|^2} > 0$, we have $Mz \in \mathfrak{H}$. So $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{H}$. We set

$$J(M,z) = \frac{dMz}{dz} = \frac{1}{(cz+d)^2}. \tag{2.2}$$

Since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$ acts trivially on $\mathfrak{H}$, $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\pm I_2$ acts faithfully on $\mathfrak{H}$. $\mathrm{PSL}_2(\mathbb{R})$ is actually the set of all the holomorphic automorphisms on $\mathfrak{H}$. Let $G = \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\pm I_2$. G is called the modular group. Let $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in G$. Then

$$T(z) = z + 1 \text{ and } S(z) = -\frac{1}{z}. \tag{2.3}$$

It is well known that T, S generate G ; $G = <T, S : (ST)^3 = S^2 = I_2>$.

Definition 7. *Let A be a group acting on a topological space X. A fundamental domain of this action is a closed subset D of X satisfying*

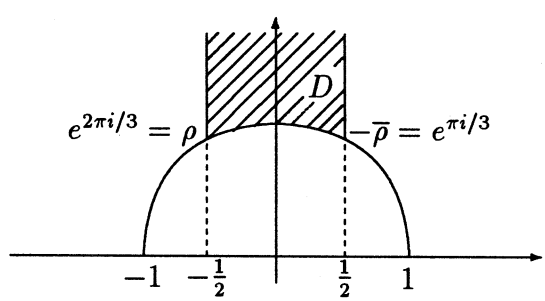
(i) $AD = X$

(ii) For $d_1, d_2 \in D$ and $a \in A$, if $ad_1 = d_2$, then either $a = 1$ or $d_1, d_2 \in \partial D$.

One can easily check that

$$D = \{z \in \mathfrak{H} : |z| \geq 1 \ , \ -\frac{1}{2} \leq \mathrm{Re}z \leq \frac{1}{2}\}$$

is a fundamental domain of the action (2.1).



(2.4)

We now give the stabilizer $G_z = \{M \in G : Mz = z\}$ for each $z \in \mathfrak{H}$. From direct computations, we obtain

$$G_i = \{I_2, S\}, \ G_\rho = \{I_2, ST, (ST)^2\}, \ G_{-\overline{\rho}} = \{I_2, TS, (TS)^2\} \tag{2.5}$$

and $G_z = \{I_2\}$, for any $z \neq i, \rho, -\overline{\rho}$, where $\rho = e^{2\pi i/3}$.

2.2 Modular Forms

Let k be an integer and let Γ be a subgroup of G.

Definition 8. *A weakly modular function of weight k for Γ is a meromorphic function f on $\mathfrak{H}$ satisfying*

$$f(Mz) = (cz+d)^k f(z), \ {}^\forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

If $-I_2 \in \Gamma$ and k is odd, then $f = 0$ trivially. Note that if f is a weakly modular function of weight k, k even, for Γ, then $f(z)(dz)^{k/2}$ is Γ-invariant, *i.e.*,

$$f(Mz)(dMz)^{k/2} = f(z)(dz)^{k/2}$$

for any $M \in \Gamma$. This is because

$$f(Mz) = ((cz+d)^2)^{k/2} f(z) = \left(\frac{dz}{dMz}\right)^{k/2} f(z).$$

We fix k and $\Gamma = G$ for the moment. For a meromophic function f on $\mathfrak{H}$, f is a weakly modular function of weight k for G if and only if

$$f(z+1) = f(z) \text{ and } f(-\frac{1}{z}) = (-z)^k f(z).$$

When a meromorphic function f on $\mathfrak{H}$ satisfies $f(z+1) = f(z)$, then f can be written as a function of $q = e^{2\pi i z}$, which will be denoted by f^*. f^* is meromorphic on $\{q \in \mathbb{C} : |q| < 1\} - \{0\}$.

Definition 9. *If f^* extends to a meromorphic function at the origin, then we say f is meromorphic at infinity. A weakly modular function f is called a modular function if f is meromorphic at infinity.*

For a modular function f, f^* has a Laurent series expansion

$$f^*(q) = \sum_{m \geq N}^{\infty} a_m q^m.$$

Definition 10. *A modular function f is called a modular form if f is holomorphic on $\mathfrak{H}_\infty = \mathfrak{H} \cup \{\infty\}$. In this case, we have $f^*(q) = \sum_{m=0}^{\infty} a_m q^m$. We set $f(\infty) = f^*(0) = a_0$. A modular form f is called a cusp form if $f(\infty) = 0$.*

For a modular form f, we have

$$f(z) = \sum_{m \geq 0} a_m e^{2\pi i m z}, \quad z \in \mathfrak{H}_\infty,$$

which is called a Fourier series expansion of f.

Example. For an even unimodular lattice L of rank n,

$$\vartheta_L(z) = \sum_{m \geq 0} r_L(m) e^{2\pi i m z}$$

satisfies $\vartheta_L(z+1) = \vartheta(z)$ and $\vartheta_L(-\frac{1}{z}) = (-iz)^{n/2}\vartheta_L(z)$. See (1.2) and (1.4). Since $8|n$, the second equality is nothing but $\vartheta_L(-\frac{1}{z}) = (-z)^{n/2}\vartheta_L(z)$. Therefore $\vartheta_L(z)$ is a modular form of weight $k = \frac{n}{2}$ for G. But this is not a cusp form since $r_L(0) = 1$.

2.3 Construction of Modular Forms

Let $f : \mathfrak{H} \to \mathbb{C}$ and let k be an even integer. Consider

$$f(z) = J(M,z)^{-k/2} f(Mz), \quad {}^\forall z \in \mathfrak{H}, \quad \text{for} \quad M \in G. \tag{2.6}$$

The condition (2.6) is called the automorphic condition of weight k for $M \in G$. It is easy to see that $J(M_1 M_2, z) = J(M_1, M_2 z) J(M_2, z)$ for any $M_1, M_2 \in G$ and $z \in \mathfrak{H}$. Let $\phi : \mathfrak{H} \to \mathbb{C}$ be a function. Then

$$f(z) = \sum_{M \in G} J(M,z)^{k/2} \phi(Mz) \tag{2.7}$$

satisfies (2.6) for any $K \in G$ if it converges. Indeed, for any $K \in G$,

$$\begin{aligned} f(Kz) &= \sum_{M \in G} J(M, Kz)^{k/2} \phi(MKz) \\ &= \sum_{M \in G} J(MK, z)^{k/2} J(K,z)^{-k/2} \phi(MKz) \\ &= J(K,z)^{-k/2} \sum_{M \in G} J(MK,z)^{k/2} \phi(MKz) \\ &= J(K,z)^{-k/2} f(z). \end{aligned}$$

Let P be a subgroup of G and let $\phi : \mathfrak{H} \to \mathbb{C}$ satisfy (2.6) for any $A \in P$. Then

$$f(z) = \sum_{M \in P \backslash G} J(M,z)^{k/2} \phi(Mz) \tag{2.8}$$

satisfies (2.6) for any $K \in G$ if it converges. This follows immediately from the above. We now apply this for $P =< T >= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : \ b \in \mathbb{Z} \right\}$ and $\phi \equiv 1$. It is easy to see that $\phi(Tz) = J(T,z)^{-k/2}\phi(z)$ and there is a one-to-one correspondence between $P\backslash G$ and $\{(c,d) \in \mathbb{Z}^2 : \gcd(c,d) = 1\}/\pm 1$. We set

$$E_k(z) = \frac{1}{2} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ gcd(c,d)=1}} (cz+d)^{-k} \quad , \quad z \in \mathfrak{H} \tag{2.9}$$

Then $E_k(z)$ satisfies (2.6). $E_k(z)$ is called an Eisenstein series of weight k. Let

$$\begin{aligned} G_k(z) &= \sum_{(c,d) \in \mathbb{Z}^2}{}' (cz+d)^{-k} = \sum_{m \geq 1} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ gcd(c,d)=m}} (cz+d)^{-k} \\ &= \sum_{m \geq 1} m^{-k} \sum_{\substack{(c',d') \in \mathbb{Z}^2 \\ gcd(c',d')=1}} (c'z+d')^{-k} = 2\zeta(k) E_k(z). \end{aligned}$$

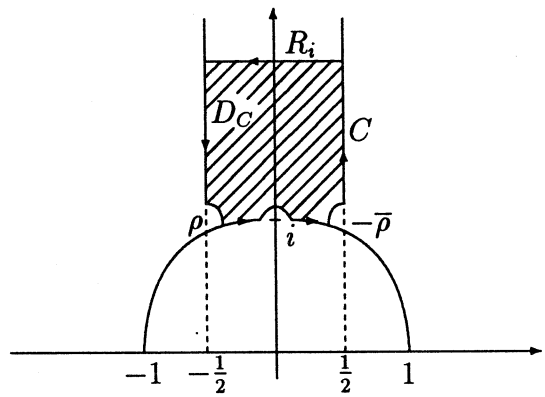
It is well-known that $G_k(z)$ is holomorphic on $\mathfrak{H}_\infty$ and $G_k(\infty) = 2\zeta(k)$ if $k > 2$. (Recall our assumption that k is even. In fact, if k is odd, then $G_k(z) \equiv 0$.) Therefore we have $E_k(z)$ holomorphic on $\mathfrak{H}_\infty$ with $E_k(\infty) = 1$ for $k = 4, 6, 8, \cdots$. In particular, they are modular forms of weight k for G.

2.4 Space of Modular Forms

Let M_k be the vector space over $\mathbb{C}$ of modular forms of weight k for G. Let M_k^0 be the subspace of M_k consisting of cusp forms. From the map $M_k \to \mathbb{C}$ defined by $f \mapsto f(\infty)$, one obtains $\dim_{\mathbb{C}}(M_k/M_k^0) = 0$ or 1. Recall that $M_k = 0$ if k is odd. So we extend our assumption that k is even. Let $f(z) \not\equiv 0$ be a meromorphic function and let $v_\tau(f)$ be the order of f at $\tau \in \mathfrak{H}_\infty$. From the residue theorem, we have

$$\frac{1}{2\pi i} \oint_C \frac{df}{f} = \sum_{\tau \in G \backslash \mathfrak{H}}{}^* v_\tau(f), \tag{2.10}$$

where $\sum^*$ means a summation over the orbits of $\tau \in \mathfrak{H}$ distinct from the orbits of i and ρ.



(2.11)

Note that $v_\tau(f) = v_{M\tau}(f)$, $^\forall M \in G$. Since poles and zeros are isolated, there exist $R > 0$ such that there are no poles and zeros in

$$\{z \in \mathfrak{H} : \mathrm{Im}z > R, \quad -\frac{1}{2} < \mathrm{Re}z < \frac{1}{2}\}$$

and there are only finitely many zeros and poles in D_C so that the righthand side of (2.10) make sense. Integrating the lefthand side of (2.10), we get

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\tau \in G\backslash\mathfrak{H}}^* v_\tau(f) = \frac{k}{12}. \tag{2.12}$$

We set $\Delta = E_4^3 - E_6^2$. Δ is a modular form of weight 12 for G. Moreover, Δ is a cusp form since $\Delta(\infty) = E_4(\infty)^3 - E_6(\infty)^2 = 0$. It is easy to see that Δ has no zeros in $\mathfrak{H}$ and a simple zero at ∞. We now investigate the $\dim_{\mathbb{C}} M_k$ for k even. For $f \in M_k$, $v_\tau(f) \geq 0$ for any $\tau \in \mathfrak{H}_\infty$and hence k can not be negative and hence we have :

Theorem 1. *$dim_{\mathbb{C}} M_k = 0$ for k negative or odd.*

For $k = 0, 2, 4, 6, 8, 10$, from (2.12) it follows immediately that :

Theorem 2. *$dim_{\mathbb{C}} M_0 = 1$, $dim_{\mathbb{C}} M_2 = 0$, and $dim_{\mathbb{C}} M_k = 1$ for $k = 4, 6, 8, 10$. More precisely, $M_0 = \mathbb{C}$, $M_2 = 0$, and $M_k = \mathbb{C}E_k$ for $k = 4, 6, 8, 10$.*

Consider the map $M_k \to M_{k+12}^0$ defined by $f \mapsto f\Delta$. This map is an isomorphism since Δ has no zeros on $\mathfrak{H}$ and has a simple zero at ∞. Actually,

this is true for any positive integer k. Since $E_k \in M_k - M_k^0$ for $k \geq 4$, we have $\dim_{\mathbb{C}}(M_k/M_k^0) = 1$. In other words, $\dim_{\mathbb{C}} M_k = \dim_{\mathbb{C}} M_k^0 + 1$ for $k \geq 4$. From the above, $\dim_{\mathbb{C}} M_k^0 = \dim_{\mathbb{C}} M_{k-12}$ so that $\dim_{\mathbb{C}} M_k = \dim_{\mathbb{C}} M_{k-12} + 1$ for $k \geq 12$. This gives us :

Theorem 3. *$dim_{\mathbb{C}} M_k = \begin{cases} \left[\frac{k}{12}\right] & \text{if } k \equiv 2 \ (mod 12) \\ \left[\frac{k}{12}\right] + 1 & \text{if } k \not\equiv 2 \ (mod 12) \end{cases}$* (2.13)

where k is nonnegative even.

We close this section with the following :

$$\mathbb{C}[x, y] \simeq \bigoplus_{\substack{k \geq 0 \\ k \text{ even}}} M_k, \tag{2.14}$$

via a map defined by $x \mapsto E^4$, $y \mapsto E^6$. In particular, M_k has a basis consisting of monomials of the form $E_4^{\alpha} E_6^{\beta}$ with $4\alpha + 6\beta = k$, α, β nonnegative integers.

3. Fourier Coefficients

3.1 Fourier Coefficients of E_k

Definition 11. *Let $\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_{2k} \frac{x^{2k}}{(2k)!}$. We call B_k the k-th Bernoulli number for $k = 1, 2, \cdots$.*

$$B_2 = \frac{1}{6},\ B_4 = \frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = \frac{1}{30},\ B_{10} = \frac{5}{66},\ B_{12} = \frac{691}{2730},$$
$$B_{14} = \frac{7}{6},\ B_{16} = \frac{3617}{510},\ B_{18} = \frac{43867}{798},\ \cdots;\ B_1 = -\frac{1}{2},\ B_{odd \neq 1} = 0.$$

Remark 4. *Let k be a positive integer. Then*

(1) $B_k \in \mathbb{Q}$.

(2) $2\zeta(2k) = \frac{(2\pi)^{2k}}{(2k)!} B_{2k}$.

(3) $\zeta(2k+1) = ?$

We prove (2) in the following :

From
$$\frac{2iz}{e^{2iz}-1} = 1 - iz - \sum_{k=1}^{\infty} B_{2k}\frac{(2z)^{2k}}{(2k)!}$$

follows
$$z\cot z = \frac{2iz}{e^{2iz}-1} + iz = 1 - \sum_{k=1}^{\infty} B_{2k}\frac{(2z)^{2k}}{(2k)!}.$$

On the other hand, from the Weierstrass factorization theorem follows
$$z\cot z = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\left(\frac{z^2}{n^2\pi^2}\right)^k.$$

Comparing the two expressions of $z\cot z$, we get (2).

Theorem 4. *Let k be a positive even integer ≥ 4. Then*
$$G_k(z) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sigma_{k-1}(m)q^m \tag{3.1}$$

where $q = e^{2\pi iz}$, $z \in \mathfrak{H}$, and $\sigma_{k-1}(m) = \sum_{d|m} d^{k-1}$. In particular,
$$E_k(z) = \frac{G_k(z)}{2\zeta(k)} = 1 + \frac{(-1)^{k/2}2k}{B_k}\sum_{m=1}^{\infty}\sigma_{k-1}(m)q^m \tag{3.2}$$

(Proof)
$$\begin{aligned}\pi\cot\pi z &= \frac{1}{z} + \sum_{m=1}^{\infty}\frac{2z}{z^2-m^2}\\ &= \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right)\\ \pi\cot\pi z &= \pi\frac{\cos\pi z}{\sin\pi z} = \pi i\frac{q+1}{q-1} = -\pi i - 2\pi i\sum_{n=1}^{\infty}q^n.\end{aligned}$$

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

Differentiating $(k-1)$-times, we obtain
$$\sum_{m\in\mathbb{Z}}\frac{(k-1)!(-1)^{k-1}}{(z+m)^k} = -(2\pi i)^k\sum_{n=1}^{\infty}n^{k-1}q^n.$$

Hence,

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

$$\begin{aligned} G_k(z) &= \sum_{(c,d)\in\mathbb{Z}^2}{}' \frac{1}{(cz+d)^k} = 2\zeta(k) + 2\sum_{c\geq 1}\sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^k} \\ &= 2\zeta(k) + 2\sum_{c\geq 1} \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^{cn} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sigma_{k-1}(m) q^m. \end{aligned}$$

This proves (3.1). (3.2) follows immediately. ∎

Remark 5. *(1)* $B_k E_k(z) \in \mathbb{Z}[[q]]$, $k = 4, 6, 8, \cdots$,

(2)
$$E_4(z) = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m, \tag{3.3}$$

$$E_6(z) = 1 - 504 \sum_{m=1}^{\infty} \sigma_5(m) q^m, \tag{3.4}$$

$$E_{10}(z) = 1 - 264 \sum_{m=1}^{\infty} \sigma_9(m) q^m, \tag{3.5}$$

(3) $E_{10} = E_4 \cdot E_6$ *implies*

$$264\sigma_9(m) = 504\sigma_5(m) - 240\sigma_3(m) + 120960 \sum_{k=1}^{m-1} \sigma_3(k)\sigma_5(m-k).$$

3.2 Ramanujan τ-Function

Recall that $\Delta = E_4^3 - E_6^2$ is a cusp form of weight 12. We now normalize it for convenience : we reset

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = \sum_{m=1}^{\infty} \tau(m) q^m. \tag{3.6}$$

It is easy to see that $\tau(1) = 1$. The map defined by $m \mapsto \tau(m)$ is called the Ramanujan τ-function. $(m = 1, 2, 3, \cdots)$

Theorem 5. $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$.

(Proof) The righthand side is a cusp form of weight 12. Since M_{12}^0 is of dimension one, it should be a multiple of Δ. Comparing the first nonzero coefficients, one gets the equality. ∎

Observe that $\tau(m) \in \mathbb{Z}$, $^\forall m = 1, 2, 3, \cdots$.

Conjecture. (Lehmer) $\tau(m) \neq 0$, $^\forall m = 1, 2, \cdots$.

Consider

$$E_{12}(z) = 1 + \frac{65520}{691}\sum_{m=1}^{\infty}\sigma_{11}(m)q^m. \tag{3.7}$$

$\{\Delta,\ E_{12}\}$ is good for a basis of M_{12}. We go back to an even unimodular lattice L on $\mathbb{R}^{24}$. Since $\vartheta_L \in M_{12}$, we have

$$\vartheta_L = \alpha_L E_{12} + \beta_L \Delta \tag{3.8}$$

for some $\alpha_L,\ \beta_L \in \mathbb{C}$. Recall that $\vartheta_L(z) = \sum_{m=0}^{\infty} r_L(m)q^m$ and $r_L(0) = 1$. Therefore $\alpha_L = 1$ for any such L, and hence $\beta_L = r_L(1) - \dfrac{65520}{691}$. If $L = \Lambda$, the Leech lattice, then $\beta_\Lambda = -\dfrac{65520}{691}$ because $r_\Lambda(1) = 0$. So we have

$$r_\Lambda(m) = \frac{65520}{691}(\sigma_{11}(m) - \tau(m)),\ ^\forall\ m = 1, 2, \cdots. \tag{3.9}$$

In particular, $\tau(m) \equiv \sigma_{11}(m) (\mathrm{mod}\, 691)$.

It turns out that there are exactly five pairs $\{L,\ L'\}$ with $r_L(1) = r_{L'}(1)$, among 24 even unimodular lattices on $\mathbb{R}^{24}$. So we get only 19 distinct thetasreies because

$$r_L(1) = r_{L'}(1) \Rightarrow \beta_L = \beta_{L'} \Rightarrow \vartheta_L = \vartheta_{L'}.$$

Anyway one can find the explicit formula for $r_L(m)$ for $m = 1, 2, \cdots$ as in (3.9). Also note $r_L(1) \neq 0$ if $L \not\cong \Lambda$.

3.3 Estimation of Fourier Coefficients

Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ be a modular form of weight k, k even ≥ 4. If $f = G_k$, then there exist $A, B > 0$ such that

$$An^{k-1} \leq |a_n| \leq Bn^{k-1}. \tag{3.10}$$

For, $a_n = (-1)^{k/2} A\sigma_{k-1}(n)$ for $A = \dfrac{2(2\pi)^k}{(k-1)!} > 0$, and hence

$$|a_n| = A\sigma_{k-1}(n) \geq An^{k-1}.$$

On the other hand,

$$\frac{|a_n|}{n^{k-1}} = A\sum_{d|n} \frac{1}{d^{k-1}} \leq A\sum_{d=1}^{\infty} \frac{1}{d^{k-1}} = A\cdot\zeta(k-1).$$

Taking $B = A \cdot \zeta(k-1) > 0$, we get $|a_n| \leq B \cdot n^{k-1}$ as desired. Therefore the order of magnitude of a_n is n^{k-1}. The following theorem due to Hecke estimates the growth of a_n when f is a cusp form.

Theorem 6. *Let f be a cusp form of weight k. Then $a_n = O(n^{k/2})$.*

(Proof) $f(z) = \sum_{n=1}^{\infty} a_n q^n = q(\sum_{n=1}^{\infty} a_n q^{n-1})$. So we have

$$|f(z)| = O(e^{-2\pi y}),\ y = \operatorname{Im} z \ \text{ as } \ z \to i\infty\ (y \to \infty).$$

Let $\phi(z) = |f(z)|y^{k/2}$. Then one can easily show that $\phi(z)$ is invariant under G, *i.e.*,

$$\phi(Mz) = \phi(z) \ \text{ for all } M \in G.$$

Moreover, $\phi(z)$ is bounded on D, the fundamental domain described in (2.4). So $\phi(z)$ is bounded on $\mathfrak{H}$, *i.e*, there exists a constant $M > 0$ such that $|f(z)| \leq My^{-k/2}$, $^\forall z \in \mathfrak{H}$. By Cauchy Theorem,

$$a_n = \frac{1}{2\pi i}\oint_C \frac{f(z)}{q^{n+1}}dq = \frac{1}{2\pi i}\oint_C \frac{f(z)}{q^n}\frac{dq}{q}$$

where C is a circle about the origin in the unit disc. Now, since $dq = 2\pi i q dz$ and a line segment $l:\ 0 \leq x \leq 1$ with a fixed $y > 0$ gives a circle about the origin in a unit disc via the substitution $q = e^{2\pi i z}$, we get

$$a_n = \int_{x=0}^{x=1} \frac{f(z)}{q^n}dz = \int_0^1 \frac{f(z)}{q^n}dx, \qquad (dz = dx + idy = dx).$$

So

$$|a_n| \leq \int_0^1 \frac{|f(z)|}{e^{-2\pi yn}} dx \leq M \cdot y^{-k/2} \cdot e^{2\pi yn}.$$

By setting $y = \frac{1}{n}$, we obtain $|a_n| \leq M \cdot n^{k/2} \cdot e^{2\pi} = M' n^{k/2}$ as desired. ∎

Remark 6. *(1) Let f be a modular form of weight k. Then $f = \alpha G_k + h$ for some $\alpha \in \mathbb{C}$, h a cusp form. From above, we may conclude that the order of magnitude of a_n is n^{k-1} .*

(2) $\tau(n) = O(n^6)$. *So* $r_{\Lambda}(m) = \dfrac{65520}{691}\sigma_{11}(m) + O(m^6)$.

(3) Theorem 6 can be improved. Indeed, Deligne proved $a_n = O(n^{\frac{k-1}{2}}\sigma_0(n))$ by proving the famous "Weil conjecture". This implies :

$$a_n = O(n^{\frac{k-1}{2}+\epsilon}), \quad \text{for } {}^{\forall}\epsilon > 0. \tag{3.11}$$

(4) Ramanujan conjectured $|\tau(p)| \leq 2p^{11/2}$, and this also was first proved by Deligne. (See (3) above.)

3.4 *L*-Functions

Let $f(z) = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k, k even ≥ 4. We set

$$D(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad s \in \mathbb{C} \tag{3.12}$$

and call it the Dirichlet series associated to f.

Theorem 7. *$D(f,s)$ converges uniformly and absolutely on compact subset if $Re(s) > 1 + \frac{k}{2}$.*

(Proof) $|D(f,s)| \leq \sum_{n=1}^{\infty} |a_n| n^{-s} \leq \sum_{n=1}^{\infty} M \cdot n^{k/2} n^{-s}$ for some $n > 0$. So the theorem follows if $\mathrm{Re}(s) - \frac{k}{2} > 1$. ∎

Definition 12. *We define the L-function associated to f by*

$$L(f,s) = (2\pi)^{-s}\Gamma(s)D(f,s),\ s \in \mathbb{C} \tag{3.13}$$

where $\Gamma(s) = \dfrac{e^{-\gamma s}}{s}\prod_{n=1}^{\infty}(1+\frac{s}{n})^{-1}e^{s/n}$ *is a* Γ*-function that is known to be a meromorphic function with simple poles at* $s = 0, -1, -2, \cdots$. *Here* $\gamma = \lim_{n\to\infty}((1+\frac{1}{2}+\cdots+\frac{1}{n}) - \log n)$ *is the Euler constant.*

Note that $\Gamma(1) = 1$ since $e^{\gamma} = \prod_{n=1}^{\infty}(1+\frac{1}{n})^{-1}e^{1/n}$ and that $\Gamma(n+1) = n!$ for nonnegative integers n. We may define $s! = \Gamma(s+1)$ for $s \neq -1, -2, \cdots$.
The following facts are consequences of direct computations :

Fact 2. *(1) D and L extend to entire functions and satisfy*

$$L(f, k-s) = i^k L(f,s). \tag{3.14}$$

(2) Hecke also proved the converse : For a Dirichlet series $D(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ converging uniformly and absolutely on compact subsets in some right half plane, if $L(s) = (2\pi)^{-s}\Gamma(s)D(s)$ extends to an entire function satisfying (3.14) for even positive integer k, then $f(z) = \sum_{n=1}^{\infty} a_n q^n$ is a cusp form of weight k.

Remark 7. *We know $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1-p^{-s})^{-1}$. The right hand side is called the Euler product of $\zeta(s)$. Similar question can be made : Does $D(f,s)$ have Euler product ? Sometimes the answer is yes ! We will see it later in Chapter 4.*

4. Hecke Operators

4.1 Modular Forms of Higher Levels

Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index and $k \in \mathbb{Z}$. For $f: \mathfrak{H} \to \mathbb{C}$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, we set

$$(f|_k g)(z) = (\det g)^{k/2}(cz+d)^{-k} f(gz). \tag{4.1}$$

Note that

$$f|_k g_1|_k g_2 = f|_k g_1 g_2, \quad \text{for } {}^\forall g_1, g_2 \in \mathrm{GL}_2^+(\mathbb{R}) \tag{4.2}$$

Definition 13. *A meromorphic function $f : \mathfrak{H} \to \mathbb{C}$ is called a modular function of weight k for Γ if*

(1) $f|_k\gamma = f$, ${}^\forall\gamma \in \Gamma$.

(2) f is meromorphic at each cusp.

Here cusps are the points in $\mathbb{Q} \cup \{\infty\}$.

Let s be a cusp. Then it is easy to show that there exists $\rho \in \mathrm{SL}_2(\mathbb{Z})$ such that $\rho s = \infty$. We set $\Gamma_s = \{\gamma \in \Gamma : \gamma s = s\}$. Then

$$\rho\Gamma_s\rho^{-1}(\pm I_2) = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\}$$

for some positive integer h. Clearly $\rho\Gamma_s\rho^{-1}$ fixes ∞. We call h the width of the cusp s. To explain the meaning of the second condition in the above definition, known as the cuspidal condition, we set $f_s = f|_k\rho^{-1}$. Firstly, assume k even.

$$\begin{aligned} f_s(z+h) &= f_s\left(\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} z\right) = f_s|_k \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \\ &= f|_k\rho^{-1}|_k \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} = f|_k\rho^{-1} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \\ &= f|_k\gamma\rho^{-1} = f|_k\gamma|_k\rho^{-1} = f|_k\rho^{-1} = f_s(z), \quad \gamma \in \Gamma_s. \end{aligned}$$

So $f_s(z) = f_s(e^{2\pi iz/h}) = f_s^*(q^{1/h})$. So (2) means that $f_s^*(q^{1/h})$ is meromorphic at $q = 0$. Secondly, let k be odd. If $-I_2 \in \Gamma$, then $f \equiv 0$. So assume $-I_2 \notin \Gamma$. Then $\rho\Gamma_s\rho^{-1}$ is generated by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix}$. If $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ generates $\rho\Gamma_s\rho^{-1}$, then since we again have $f_s(z+h) = f_s(z)$, (2) means $f_s^*(q^{1/h})$ is meromorphic at $q = 0$. If $\begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix}$ generates $\rho\Gamma_s\rho^{-1}$, we use $\begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2h \\ 0 & 1 \end{pmatrix}$. Since we have $f_s(z+2h) = f_s(z)$, (2) means $f_s^*(q^{1/2h})$ is meromorphic at $q = 0$. Note that the above argument is independent of the choice of ρ and it depends only on Γ_s.

A modular function is a modular form if f is holomorphic on $\mathfrak{H}$ and at cusps. Modular forms of weight k for Γ form a finite dimensional vector space over $\mathbb{C}$. We denote the space by $M_k(\Gamma)$.

4.2 Hecke Operators

Definition 14. *Let A be a group and B be its subgroup. We set*

$$Comm_A(B) = \left\{ a \in A : \begin{array}{c} aBa^{-1} \cap B \text{ is of finite} \\ \text{index in both } aBa^{-1} \text{ and } B \end{array} \right\}$$

We call this the commensurator of B in A.

It is easy to see that $\mathrm{Comm}_A(B)$ is a subgroup of A containing B. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let $A = \mathrm{GL}_2^+(\mathbb{R})$. Then it is known that

$$\mathrm{Comm}_A(\Gamma) = \mathbb{R} \cdot \mathrm{GL}_2^+(\mathbb{Q}).$$

Theorem 8. *Let Γ and A be as above.*

(1) If $g \in Comm_A(\Gamma)$, then $\Gamma g \Gamma = \dot{\bigcup}_i \Gamma g_i$, $g_i \in Comm_A(\Gamma)$, where the union is finite. Here $\dot{\bigcup}$ means a disjoint union.

(2) If $f \in M_k(\Gamma)$, then $\sum_i f|_k g_i \in M_k(\Gamma)$.

(See Definition 15 below : $f \in M_k(\Gamma) \Rightarrow f|_k T_g \in M_k(\Gamma)$, $^\forall g \in \mathrm{Comm}_A(\Gamma)$).

(Proof) (1) Let $\Gamma = \dot{\bigcup}_{i=1}^{\mu} (g^{-1}\Gamma g \cap \Gamma)\delta_i$ for $\delta_i \in \Gamma$. Then we have

$$\Gamma g \Gamma = \dot{\bigcup}_{i=1}^{\mu} \Gamma g \delta_i = \dot{\bigcup}_{i=1}^{\mu} \Gamma g_i,$$

where $g_i = g\delta_i \in \mathrm{Comm}_A(\Gamma)$, $i = 1, \ldots, \mu$.
(2) $\sum_i f|_k g_i|_k \gamma = \sum_i f|_k g_i \gamma = \sum_i f|_k \gamma_i g_i = \sum_i f|_k \gamma_i|_k g_i = \sum_i f|_k g_i$, for $\gamma, \gamma_i \in \Gamma$.
The cuspidal condition is easy to check. ∎

Definition 15. *Let $T_g = \Gamma g \Gamma = \dot{\bigcup}_i \Gamma g_i$, $g, g_i \in Comm_A(\Gamma)$. We set $f|_k T_g = \sum_i f|_k g_i$ for any f and g as above. T_g is a linear operator on the space of modular forms of weight k for Γ, which is called a Hecke operator.*

Remark 8. *Consider the vector space over $\mathbb{C}$ spanned by T_g, $g \in Comm_A(\Gamma)$. Elements can be written in the form $\dot{\bigcup}_i a_i \Gamma g_i$. In fact, it is a ring with the*

multiplication defined by $(\bigcup_i a_i\Gamma g_i)(\bigcup_i b_j\Gamma h_i) = \bigcup_{i,j} a_ib_j\Gamma g_ih_j$. *The addition is of course* $\bigcup$ *This ring is called the Hecke ring. We are not going into this ring. We will study Hecke operators in a classical way.*

Definition 16. *Let* N *be a positive integer. We set*

$$\begin{aligned}
\Gamma(N) &= \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \gamma \equiv I(mod\ N)\right\},\\
\Gamma_1(N) &= \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1(mod\ N), c \equiv 0(mod\ N)\right\},\\
\Gamma_0(N) &= \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0(mod\ N)\right\}.
\end{aligned}$$

$\Gamma(N)$ *is called the principle congruence subgroup of* $SL_2(\mathbb{Z})$ *of level* N. *A subgroup of* Γ *of* $SL_2(\mathbb{Z})$ *containing* $\Gamma(N)$ *is called a congruence subgroup of level* N.

Note that $M_k \subset M_k(\Gamma_0(N)) \subset M_k(\Gamma_1(N))$, $^\forall N \geq 1$. If $N = 1$, then they are the same space.

$\Gamma_i(N)$ are congruence subgroups of level q for $i = 0, 1$. Let

$$M_1^n(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = n, a \equiv 1, c \equiv 0(\text{mod } N)\right\}. \quad (4.3)$$

Then it is not hard to see that

$$M_1^n(N) = \bigcup_{\substack{ad=n,\ a,d>0 \\ (a,N)=1 \\ 0\leq b\leq d-1}} \Gamma_1(N)\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad (4.4)$$

where $\sigma_a \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \bmod N$.
Let $\Gamma = \Gamma_1(N)$ and $f \in M_k(\Gamma)$ from here on. We set

$$f|_kT(n) = n^{(k/2)-1} \sum_{a,b,d} f|_k\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad (4.5)$$

where the summation is over a, b, d as described in (4.4). From (4.4), one can easily recognize that $T(n) = M_1^n(N) = \Gamma M_1^n(N)\Gamma = \bigcup_{finite} \Gamma g\Gamma = \bigcup_{finite} T_g$, for

some g's in $M_1^n(N)$, up to a constant multiple of $n^{(k/2)-1}$.

Γ is a normal subgroup of $\Gamma_0(N)$ such that $\Gamma_0(N)/\Gamma \simeq (\mathbb{Z}/N\mathbb{Z})^*$. For any $d \in (\mathbb{Z}/N\mathbb{Z})^*$, we set

$$f|_k[d] = f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{4.6}$$

In fact, $[d] = T_\gamma = \Gamma\gamma\Gamma$ where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. One can easily check the well-definedness of (4.6).

We let $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character. f is said to be of type ε if $f|_k[d] = \varepsilon(d)f$. We denote the subspace of $M_k(\Gamma)$ consisting of the forms of type ε by $M_k(\Gamma, \varepsilon)$. Then it is well-known that

$$M_k(\Gamma) = \bigoplus_\varepsilon M_k(\Gamma, \varepsilon). \tag{4.7}$$

Note that $M_k(\Gamma, 1) = M_k(\Gamma_0(N))$.

We introduce one more Hecke operator : For $f \in M_k(\Gamma, \varepsilon)$ and $(n, N) = 1$, we set $f|_k T(n,n) = \varepsilon(n)n^{k-2}f$. For $f \in M_k(\Gamma)$, write $f = \sum_\varepsilon f_\varepsilon$, $f_\varepsilon \in M_k(\Gamma, \varepsilon)$. We define $T(n,n)$ by

$$f|_k T(n,n) = \sum_\varepsilon f_\varepsilon|_k T(n,n) = \sum_\varepsilon \varepsilon(n)n^{k-2}f_\varepsilon. \tag{4.8}$$

The algebra over $\mathbb{C}$ generated by $T(n), [d], T(n,n)$ is called the Hecke algebra of Hecke operators acting on $M_k(\Gamma)$. This algebra is, in fact, a commutative algebra.

4.3 Action on Fourier Coefficients

Definition 17. *Let d be a positive integer. For $\sum a_m q^m \in \mathbb{C}((q))$, we define*

$$V_d\Big(\sum a_m q^m\Big) = \sum a_m q^{dm} \quad \text{and} \quad U_d\Big(\sum a_m q^m\Big) = \sum_{d|m} a_m q^{m/d}.$$

Let $f(z) = \sum a_n q^n$, $q = e^{2\pi iz}$. Then obviously,

$$V_d(f(z)) = f(dz) \quad \text{and} \quad U_d(f(z)) = \frac{1}{d}\sum_{b=0}^{d-1} f\left(\frac{z+b}{d}\right).$$

The second equation follows from

$$\sum_{b=0}^{d-1} f\left(\frac{z+b}{d}\right) = \sum_m a_m q^{\frac{m}{d}} \left(\sum_{b=0}^{d-1} e^{2\pi ibm/d}\right) = d\sum_{d|m} a_m q^{m/d}.$$

Let $f \in M_k(\Gamma, \varepsilon)$ where $\Gamma = \Gamma_1(N)$. We make a convention : $\varepsilon(a) = 0$ if $(a, N) \neq 1$. Then

$$\begin{aligned} f(z)|_k T(n) &= n^{(k/2)-1} \sum_{a,b,d} f|_k \sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = n^{(k/2)-1} \sum_{a,b,d} \varepsilon(a) f|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \\ &= n^{(k/2)-1} \sum_{a,b,d} \varepsilon(a)(ad)^{k/2} d^{-k} f\left(\frac{az+b}{d}\right) \\ &= n^{k-1} \sum_{\substack{ad=n \\ a,d>0 \\ (a,N)=1}} \varepsilon(a) d^{-k} \left(\sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right)\right). \end{aligned}$$

where a, b, d run over those described as in (4.4). On the other hand,

$$\begin{aligned} \sum_{a|n} \varepsilon(a) a^{k-1} (U_{n/a} \circ V_a)(f(z)) &= \sum_{a|n} \varepsilon(a) a^{k-1} U_d(f(az)) \qquad (d = \frac{n}{a}) \\ &= \sum_{a|n} \varepsilon(a) a^{k-1} d^{-1} \sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right) \\ &= n^{k-1} \sum_{\substack{ad=n \\ a,d>0 \\ (a,N)=1}} \varepsilon(a) d^{-k} \left(\sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right)\right). \end{aligned}$$

So we may conclude that for any $f(z) \in M_k(\Gamma, \varepsilon)$,

$$f(z)|_k T(n) = \sum_{a|n} \varepsilon(a) a^{k-1} (U_d \circ V_a)(f(z)), \tag{4.9}$$

where $d = \dfrac{n}{a}$.

Theorem 9. *Let* $f(z) = \sum_{m=0}^{\infty} a_m q^m \in M_k(\Gamma, \varepsilon)$ *and let* $f(z)|_k T(n) = \sum_{l=0}^{\infty} b_l q^l$. *Then* $b_l = \sum_{c|(l,n)} \varepsilon(c) c^{k-1} a_{ln/c^2}$.

(Proof) We use the above formulas.

$$f(z)|_k T(n) = \sum_{c|n} \varepsilon(c) c^{k-1} \sum_{\frac{n}{c}|m} a_m q^{cm/(n/c)}.$$

$$(U_d \circ V_c)(f(z)) = \sum_{b=0}^{d-1} f\left(\frac{cz+b}{d}\right) = \sum_{b=0}^{d-1} \left(\sum a_m e^{2\pi i m(cz+b)/d}\right) = \sum_{d|m} a_m q^{cm/d}$$

where $d = \frac{n}{c}$. $\frac{cm}{n/c} = l \Rightarrow m = \frac{ln}{c^2}$ and $\frac{m}{n/c} = \frac{l}{c} \in \mathbb{Z} \Rightarrow c|l$. We set $l = \frac{c^2 m}{n}$. Then

$$f(z)|_k T(n) = \sum_{c|n} \varepsilon(c) c^{k-1} \sum_{c|l} a_{ln/c^2} q^l = \sum_{c|(n,l)} \varepsilon(c) c^{k-1} a_{ln/c^2} q^l. \quad \blacksquare$$

Corollary. *In Theorem 9, if* $n = p$ *a prime, then* $b_l = a_{lp}$ *if* $p \nmid l$ *and* $b_l = a_{lp} + \varepsilon(p) p^{k-1} a_{l/p}$ *if* $p|l$.

Theorem 10. *Let* $f(z) = \sum_{m=0}^{\infty} a_m q^m \in M_k(\Gamma, \varepsilon)$ $(\Gamma = \Gamma_1(N))$ *such that* $f(z) \not\equiv 0$ *and* $f(z)|_k T(n) = \lambda(n) f(z)$ *for all positive integers* n. *Then*

(1) $a_n = \lambda_n a_1 \ \forall n \geq 1$.

(2) $a_1 = 0 \Rightarrow k = 0$.

(3) $a_0 \neq 0, k > 0 \Rightarrow \lambda_n = \sum_{d|n} \varepsilon(d) d^{k-1}$.

(Proof). (2) is clear from (1). From

$$f|_k T(n) = \lambda_n \sum_{m=0}^{\infty} a_m q^m = \sum_{l=0}^{\infty} b_l q^l, \ b_l = \sum_{d|(l,n)} \varepsilon(d) d^{k-1} a_{ln/d^2} = \lambda_n a_l$$

follow $b_1 = a_n = \lambda_n a_1$ (putting $l = 1$) and $b_0 = \lambda_n a_0 = \sum_{d|n} \varepsilon(d) d^{k-1} a_0$ (putting $l = 0$). This proves (1) and (3). $\blacksquare$

Remark 9. *In the above theorem, normalize $f(z)$ so that $a_1 = 1$ if $a_1 \neq 0$. Then a_n are eigenvalues of $f(z)$ with respect to $T(n)$ for all $n \geq 1$. Moreover, if $a_0 \neq 0$, then*

$$f(z) = a_0 + \sum_{n=1}^{\infty} \left(\sum_{d|n} \varepsilon(d) d^{k-1} \right) q^n.$$

Note that if $\varepsilon = 1$, then

$$f(z) = a_0 + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

Hence if $a_0 = (-1)^{k/2} \dfrac{B_k}{2k}$, then $f(z)$ is nothing but a normalized $E_k(z)$, k even ≥ 4.

Remark 10. *Let $N = 1$. Then $M_k = M_k(\Gamma_0(1)) = M_k(\Gamma_1(1))$ and $\varepsilon = 1$.*

(1) $f|_k T(n) \in M_k$ if $f \in M_k$. So from Theorem 9 follows :

$$f|_k T(n) \in M_k^0 \quad \text{if} \quad f \in M_k^0, \quad \text{since} \quad b_0 = \sum_{c|n} c^{k-1} a_0 = 0. \tag{4.10}$$

(2) Δ is an eigenfunction of $T(n)$ with the eigenvalue $\tau(n)$, $^\forall n \geq 1$. $\Delta(z)|_k T(n) \in M_{12}^0$ and $dim M_{12}^0 = 1$. So $\Delta(z)|_k T(n) = \lambda(n)\Delta(z)$, $^\forall n \geq 1$. Since $\tau(1) = 1$, we may conclude that $\tau(n) = \lambda(n)$ $^\forall n \geq 1$.

(3) E_k is an eigenform of $T(n)$ with the eigenvalue $\sigma_{k-1}(n)$, $^\forall n \geq 1$.

4.4 Action on Lattices

Definition 18. *Let* $\mathfrak{R}_1(N) = \left\{ (t, L) : \begin{array}{c} L \text{ is a lattice on } \mathbb{C} \text{ and} \\ t \in \mathbb{C}/L \text{ is an } N\text{-division point} \end{array} \right\}$, *where N is a positive integer. $t \in \mathbb{C}/L$ is called an N-division point if $Nt = 0$ in $\mathbb{C}/L$ and N is the smallest among such positive integers. $\mathbb{C}^\times$ acts on $\mathfrak{R}_1(N)$: $(t, N) \mapsto (\lambda t, \lambda L)$, $\lambda \in \mathbb{C}^\times$. Consider*

$$\Phi_N : \mathfrak{H} \to \mathfrak{R}_1(N), \qquad z \mapsto \left(\frac{1}{N}, \{z, 1\}\right) \tag{4.11}$$

where $\{z, 1\}$ denotes the lattice $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot z$. Then we have

$$\mathfrak{H}/\Gamma_1(N) \simeq \mathfrak{R}_1(N)/\mathbb{C}^\times.$$

where the latter is called the moduli space of elliptic curves with N division points.

To see this, let $\gamma z = \dfrac{az+b}{cz+d}$ with $z \in \mathfrak{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. Then

$$\begin{aligned}\left(\frac{1}{N}, \left\{\frac{az+b}{cz+d}, 1\right\}\right) &= (cz+d)^{-1}\left(\frac{cz+d}{N}, \{az+b, cz+d\}\right) \\ &= (cz+d)^{-1}\left(\frac{cz+d}{N}, \{z, 1\}\right)\end{aligned}$$

since $d(az+b) - b(cz+d) = z$ and $-c(az+b) + a(cz+d) = 1$.
Since $\dfrac{cz+d}{N} - \dfrac{1}{N} = \dfrac{cz+d-1}{N} \in \{z, 1\}$,

$$\Phi_N(\gamma z) = \left(\frac{1}{N}, \left\{\frac{az+b}{cz+d}, 1\right\}\right) = (cz+d)^{-1}\left(\frac{1}{N}, \{z, 1\}\right) = (cz+d)^{-1}\Phi_N(z).$$

One can show the converse so that $^{\forall}(t, L) \in \mathfrak{R}_1(N)$, $\exists z \in \mathfrak{H}$ such that $\Phi_N(\gamma z) = \lambda(t, L)$ for some $\lambda \in \mathbb{C}^*$ and $\gamma \in \Gamma_1(N)$. ∎

Let V be a vector space over $\mathbb{C}$ with basis $\mathfrak{R}_1(N)$.
We define $T(n), [d], T(n,n) : V \to V$ by

$$\begin{cases} T(n) & : (t, L) \mapsto n^{-1} \sum\limits_{[L':L]=n} (t, L'). \\ [d] & : (t, L) \mapsto (dt, L),\ d \in (\mathbb{Z}/N\mathbb{Z})^*. \\ T(n,n) & : (t, L) \mapsto n^{-2}(t, n^{-1}L), \qquad (n, N) = 1. \end{cases} \tag{4.12}$$

Theorem 11. *(1)* $[d], T(n,n)$ *commute with all the above.*

(2) $T(n_1 n_2) = T(n_1)T(n_2)$ *if* $(n_1, n_2) = 1$.

(3) $T(p^n) = (T(p))^n$ *if* $p|N$ *where* p *is a prime.*

(4) $T(p^{n-1})T(p) = T(p^n) + p \cdot T(p^{n-2})T(p,p)$ *if* $p \nmid N$.

(Proof) We prove (2). Others are proved similarly.

$$n_1 n_2 T(n_1 n_2) : (t, L) \mapsto \sum_{[L':L]=n_1 n_2} (t, L') \tag{4.13}$$

$$n_1 T(n_1) n_2 T(n_2) : (t, L) \mapsto \sum_{\substack{[L'':L]=n_2 \\ [L':L'']=n_1}} (t, L') \tag{4.14}$$

Let L'/L be an abelian group of order n_1n_2. Since $(n_1, n_2) = 1$, there exists a unique subgroup L'' of L' such that $[L'' : L] = n_2$. (L''/L is the Hall subgroup of L'/L of order n_2). So every (t, L') in the right hand side of (4.13) appears in that of (4.14). The other direction is trivial. Therefore $T(n_1n_2) = T(n_1)T(n_2) = T(n_2)T(n_1)$. ∎

Remark 11. *(3),(4) indicate $T(p^n)$ is a polynomial of $T(p)$ and $T(p,p)$. So we may conclude that the algebra generated by $T(n), [d], T(n,n)$ is commutative. Note also that $T(p)$'s generate $T(n)$.*

Consider $F : \mathfrak{R}_1(N) \to \mathbb{C}$ such that $F(\lambda t, \lambda L) = \lambda^{-k}F(t, L)$. Let $f = F \circ \Phi_N$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and $(d, N) = 1$, we set

$$\begin{aligned}
[d]F(\Phi_N(z)) &= F([d]\left(\frac{1}{N}, \{z, 1\}\right)) = F\left(\frac{d}{N}, \{z, 1\}\right) \\
&= F\left(\frac{cz+d}{N}, \{az+d, cz+d\}\right) \\
&= (cz+d)^{-k}F\left(\frac{1}{N}, \left\{\frac{az+d}{cz+d}, 1\right\}\right) \\
&= (cz+d)^{-k}F \circ \Phi_N(\gamma z) = (cz+d)^{-k}f(\gamma z) \\
&= f|_k\gamma = f|_k[d]. \qquad (4.15)
\end{aligned}$$

Assuming $[n]F = \varepsilon(n)F$, $^\forall(n, N) = 1$, we set

$$\begin{aligned}
n^2T(n,n)F(\Phi_N(z)) &= F\left(n^2T(n,n)\left(\frac{1}{N}, \{z, 1\}\right)\right) = F\left(\frac{1}{N}, \left\{\frac{z}{n}, \frac{1}{n}\right\}\right) \\
&= n^kF\left(\frac{n}{N}, \{z, 1\}\right) = n^kF\left([n]\left(\frac{1}{N}, \{z, 1\}\right)\right) \\
&= n^k[n]F(\Phi_N(z)) = n^k\varepsilon(n)F \circ \Phi_N(z) = n^k\varepsilon(n)f(z).
\end{aligned}$$

Therefore

$$T(n,n)F(\Phi_N(z)) = f|_kT(n,n) \qquad (4.16)$$

where $f \in M_k(\Gamma, \varepsilon)$ and $\Gamma = \Gamma_1(N)$. Finally, we set

$$pT(p)F(\Phi_N(z)) = F\left(pT(p)\left(\frac{1}{N}, \{z, 1\}\right)\right) = F\left(\sum_{[L':L]=p}\left(\frac{1}{N}, L'\right)\right)$$

where $L = \{z, 1\}$. L' are of the form $\left\{\frac{z+b}{p}, 1\right\}$ $(b = 0, 1, 2, \cdots, p-1)$ or $\left\{z, \frac{1}{p}\right\}$.

If $p|N$, then $\frac{1}{N}$ is an N-division point of $\mathbb{C}/L'$, for $L' = \left\{\frac{z+b}{p}, 1\right\}, b = 0, 1, \cdots, p-1$, and not for $L' = \left\{z, \frac{1}{p}\right\}$. So

$$\begin{aligned} pT(p)F(\Phi_N(z)) &= F\left(\sum_{b=0}^{p-1}\left(\frac{1}{N}, \left\{\frac{z+b}{p}, 1\right\}\right)\right) \\ &= \sum_{b=0}^{p-1} F\circ\Phi_N\left(\frac{z+b}{p}\right) \\ &= \sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right). \end{aligned}$$

Thus

$$T(p)F(\Phi_N(z)) = \frac{1}{p}\sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right) = U_p f(z). \tag{4.17}$$

If $p\nmid N$, then

$$\begin{aligned} pT(p)F(\Phi_N(z)) &= F\left(\sum_{b=0}^{p-1}\left(\frac{1}{N}, \left\{\frac{z+b}{p}, 1\right\}\right) + \left(\frac{1}{N}, \left\{z, \frac{1}{p}\right\}\right)\right) \\ &= pU_p f(z) + F\left(\frac{1}{N}, \left\{z, \frac{1}{p}\right\}\right) \\ &= pU_p f(z) + p^k F\left(\frac{p}{N}, \{pz, 1\}\right) \\ &= pU_p f(z) + p^k \varepsilon(p) F\circ\Phi_N(pz) \\ &= pU_p f(z) + p^k \varepsilon(p) f(pz) \\ &= pU_p f(z) + p^k \varepsilon(p) V_p f(z). \end{aligned}$$

Hence

$$\begin{aligned} T(p)F(\Phi_N(z)) &= U_p f(z) + p^{k-1}\varepsilon(p)V_p f(z) \\ &= \sum_{d|p} \varepsilon(d) d^{k-1} V_d \circ U_{p/d} f(z) = f(z)|_k T(p) \end{aligned} \tag{4.18}$$

with $f \in M_k(\Gamma, \varepsilon)$. See (4.9). Therefore $F\circ\Phi_N = f$ enables us to study Hecke operators on f in terms of operator on $\mathfrak{R}_1(N)$. See Remark 11 and the starement below (4.8). We summarize :

Remark 12. *Hecke operators $T(n)$, $T(n,n)$, $[d]$ acting on $M_k(\Gamma,\varepsilon)$, where $\Gamma=\Gamma_1(N)$ and ε is a Dirichlet character : $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, generate a commutative algebra.*

4.5 Euler Products of L-Functions

Let f be a simultaneous eigenform with respect to all $T(n)$, $n \geq 1$, in $M_k(\Gamma,\varepsilon)$ with $\Gamma = \Gamma_1(N)$, normalized to have $a_1 = 1$, where $f(z) = \sum_{m=0}^{\infty} a_n q^n$. Then from Theorem 10 follows $a_n = \lambda_n$, $^\forall n \geq 1$, where $f(z)|_k T(n) = \lambda_n f$. From Theorem 11, we have

(1) $a_{n_1 n_2} = a_{n_1} a_{n_2}$ if $(n_1, n_2) = 1$,

(2) $a_{p^n} = (a_p)^n$ if $p|N$, and

(3) $a_{p^n} = a_{p^{n-1}} \cdot a_p - p^{k-1}\varepsilon(p) a_{p^{n-2}}$.

So we obtain,

Theorem 12. *Let $D(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Then*

$$D(f,s) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p\nmid N}(1 - a_p p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}.$$

(Proof) For $p|N$, $\sum_{m=0}^{\infty} a_{p^m} p^{-ms} = \sum_{m=0}^{\infty} (a_p p^{-s})^m = (1 - a_p p^{-s})^{-1}$. For $p\nmid N$, we prove

$$\left(\sum_{m=0}^{\infty} a_{p^m} T^m\right)\left(1 - a_p T + \varepsilon(p)p^{k-1}T^2\right) = 1.$$

Obviously the constant term is 1. Coefficient of T is $a_p - a_p = 0$. Coefficients of T^n $(n \geq 2)$ are

$$a_{p^n} - a_{p^{n-1}} \cdot a_p + a_{p^{n-2}}\varepsilon(p)p^{k-1} = 0.$$

So substituting $T = p^{-s}$, we have

$$\sum_{m=0}^{\infty} a_{p^m} p^{-sm} = (1 - a_p p^{-s} + \varepsilon(p)p^{k-1-2s}). \qquad \blacksquare$$

We now come back to M_k $(N = 1)$. Let $\gamma_k = (-1)^{k/2}\frac{B_k}{2k}$, k even ≥ 4, and let $f(z) = \gamma_k E_k$. Then

$$D(f,s) = \sum_{n=1}^{\infty} \frac{\sigma_{k-1}(n)}{n^s} = \prod_p \left(1 - \sigma_{k-1}(p)p^{-s} + p^{k-1-2s}\right)^{-1}. \tag{4.19}$$

Moreover,

$$\begin{aligned} D(f,s) &= \sum_{a,d\geq 1} \frac{a^{k-1}}{a^s d^s} = \left(\sum_{a\geq 1} \frac{1}{a^{s-k+1}}\right)\left(\sum_{d\geq 1} \frac{1}{d^s}\right) \\ &= \zeta(s-k+1)\zeta(s) \end{aligned}$$

where $\mathrm{Re}(s) > k$.

For $\Delta \in M_{12}^0$, which is also a simultaneous eigenform of weight 12 with respect to all $T(n)$, $n \geq 1$, with eigenvalues $\lambda(n) = \tau(n)$, we also have an Euler product for $D(\Delta, s)$:

$$\sum_{n=1}^{\infty} \tau(n)n^{-s} = \prod_p \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}.$$

Remark 13. *(1)* $\sigma_{k-1}(n)$ *satisfies* $\sigma_{k-1}(n_1n_2) = \sigma_{k-1}(n_1)\sigma_{k-1}(n_2)$ *for* $(n_1, n_2) = 1$ *and* $\sigma_{k-1}(p^n) = \sigma_{k-1}(p^{n-1})\sigma_{k-1}(p) - p^{k-1}\sigma_{k-1}(p^{n-2})$.

(2) $\tau(n_1n_2) = \tau(n_1)\tau(n_2)$ *for* $(n_1, n_2) = 1$ *and* $\tau(p^n) = \tau(p^{n-1})\tau(p) - p^{11}\tau(p^{n-2})$.

(3) $f(z) = \sum_{n=1}^{\infty} a_n q^n \in M_k^0$ *such that* $f(z)$ *is a simultaneous eigenform with respect to all* $T(n)$ *and* $a_1 = 1$. *Then* $D(f,s) = \prod_p \left(1 - a_p p^{-s} + p^{k-1-s}\right)^{-1}$.

Petersson conjectured : If $(1 - a_pT + p^{k-1}T^2) = (1 - \alpha_pT)(1 - \beta_pT)$, then α_p and β_p are complex conjugates. In other words,

$$|\alpha_p| = |\beta_p| = p^{(k-1)/2} \Rightarrow |a_p| \leq 2p^{(k-1)/2}.$$

This is a generalization of of a Ramanujan conjecture : $|\tau(p)| \leq 2p^{11/2}$. This was proved by Deligne : $|a_n| \leq n^{(k-1)/2}\sigma_0(n)$.

5. Epilogue

5.1 Positive Definite Quadratic Forms

Let $Q = \sum_{1 \le i,j \le m} a_{ij} x_i x_j$ be an integral positive definite quadratic form, *i.e,* $Q = (a_{ij})$ is a semi-integral (diagonal entries and the twice of non-diagonal entries are integers), positive definite $m \times m$ symmetric matrices. We define the theta-series of Q by

$$\begin{aligned} \vartheta(z, Q) &= \sum_{X \in M_{m,1}(\mathbb{Z})} e^{2\pi i\, {}^tXQXz}, \ (z \in \mathfrak{H}) \qquad (5.1) \\ &= \sum_{n=0}^{\infty} r(n, Q) q^n, \ (q = e^{2\pi i z}), \end{aligned}$$

where $r(n, Q) = |\{X \in M_{m,1}(\mathbb{Z}) \mid {}^tXQX = n\}|$. (5.2)

It is known that $\vartheta(z, Q)$ is a modular form of weight $k = \frac{m}{2}$ for $\Gamma_0(q)$ of type χ_Q, which is a Dirichlet character modulo q determined by Q. (See [8]) Here q is the level of Q , the smallest positive integer such that $q(2Q)^{-1}$ is integral with even diagonal entries.

Note that $q = 1$ when Q is even unimodular, whence $8|m$. We define

$$\begin{aligned} \text{the class of } Q &= \{Q' | Q' = {}^tXQX \ \text{ for some } X \in \mathrm{GL}_m(\mathbb{Z})\} \\ &= \mathrm{cls}(Q) \\ \text{the genus of } Q &= \{Q' | Q' = {}^tXQX \ \text{ for some } X \in \mathrm{GL}_m(\mathbb{Z}_p) \ {}^\forall p\} \\ &= \mathrm{gen}(Q) \end{aligned}$$

where $\mathbb{Z}_p$ is the ring of p-adic integers. It is known that

$$\mathrm{gen}(Q) = \{Q' \mid Q' \equiv {}^tXQX \ (\mathrm{mod}\, 8D^3), \ D = \det Q = \det Q'\}.$$

It is well known that the number of classes in the genus is finite. Note that if $Q' \in \mathrm{cls}(Q)$, then $\vartheta(z, Q') = \vartheta(z, Q)$, *i.e,* the theta-series is uniquely determined by $\mathrm{cls}(Q)$. But two distinct classes may give the same theta-series. We set the generic theta-series of Q as follows : Let $Q_1, \cdots, Q_h$ be the representatives of all the distinct classes in the genus of Q.

$$\vartheta(z, [Q]) = \left(\sum_{i=1}^{h} \frac{1}{e_i} \vartheta(z, Q_i) \right) m_Q^{-1}, \ z \in \mathfrak{H} \qquad (5.3)$$

where $e_i = |\{X \in \mathrm{GL}_m(\mathbb{Z}) | Q_i = {}^tXQ_iX\}| < \infty$ and $m_Q = \sum_{i=1}^{h} \frac{1}{e_i}$, which is called the mass of Q.

Fact 3. *(1) $\vartheta(z,[Q])$ is a simultaneous eigenform(normalized) with respect to Hecke operators $T(n)$ for all $n \geq 1$.*

(2) If Q is even unimodular, then $\vartheta(z,[Q]) \in M_{m/2}$. Furthermore, $\vartheta(z,[Q]) = E_{m/2}(z)$.

5.2 Siegel Mass Formula

Let Q be even unimodular so that $\vartheta(z,Q) \in M_k$ where $k = \frac{m}{2}$. Then $\vartheta(z,Q) = E_k + f_Q$, where $f_Q \in M_k^0$. Note that $8|m$.

Siegel proved: Let $Q_1, \cdots, Q_h$ be the full set of representatives of the classes in $\mathrm{gen}(Q)$. Then the weighted average of f_Q's is zero, *i.e.*,

$$\sum_{i=1}^{h} \frac{f_{Q_i}}{e_i} = 0 \tag{5.4}$$

This is, in fact, exactly same as Fact 3-(2) above:

$$\vartheta(z,[Q]) = \sum_{i=1}^{h} (\frac{E_k}{e_i} + \frac{f_{Q_i}}{e_i}) m_Q^{-1} = E_k$$

Finally, we introduce Minkowski-Siegel Mass Formula which reads :

$$m_Q = \frac{B_{m/2}}{m} \prod_{j=1}^{(m/2)-1} \frac{B_{2j}}{4j}. \tag{5.5}$$

5.3 Even Unimodular Lattices

Let Q be an even unimodular lattice in $\mathbb{R}^m$, whence $8|m$.

Case $m = 8$:

$k = \dfrac{m}{2} = 4$ and $\dim M_4 = 1$. $E_4 \in M_4$. Thus $\vartheta(z, Q) = E_4(z)$,
$r(n, Q) = 240\sigma_3(n)$, $^\forall n \geq 1$. $\left(E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n.\right)$

$$\Gamma_8 = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} : \text{ even unimodular.}$$

$e(\Gamma_8) = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$, $m_Q = 2^{-14} \cdot 3^{-5} \cdot 5^{-2} \cdot 7^{-1}$.
Therefore Γ_8 is the only even unimodular lattice in $\mathbb{R}^8$ (Mordell).

Case $m = 16$:

$k = \dfrac{m}{2} = 8$ and $\dim M_8 = 1$. $E_8 \in M_8$. Thus $\vartheta(z, Q) = E_8(z)$,
$r(n, Q) = 480\sigma_7(n)$, $^\forall n \geq 1$. $\left(E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n.\right)$
$\Gamma_8 \oplus \Gamma_8$, Γ_{16}: even unimodular $(\Gamma_8 \oplus \Gamma_8 \not\cong \Gamma_{16})$.
$e(\Gamma_8 \oplus \Gamma_8) = 2^{29} \cdot 3^{10} \cdot 5^4 \cdot 7^2$. $e(\Gamma_{16}) = 2^{15}(16!)$.
$m_Q = 691 \cdot 2^{-30} \cdot 3^{-10} \cdot 5^{-4} \cdot 7^{-2} \cdot 11^{-1} \cdot 13^{-1} = \dfrac{1}{e(\Gamma_8 \oplus \Gamma_8)} + \dfrac{1}{e(\Gamma_{16})}$.
So $\Gamma_8 \oplus \Gamma_8$, Γ_{16} are the only even unimodular lattices in $\mathbb{R}^{16}$ (Witt).

It is easy to see that $\vartheta(z, \Gamma_8 \oplus \Gamma_8) = \vartheta(z, \Gamma_8)^2 = \vartheta(z, \Gamma_{16})$. So we have $E_4(z)^2 = E_8(z)$ and hence $\left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n\right)^2 = \left(1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n\right)$, which yields useful identities between $\sigma_3(n)$ and $\sigma_7(n)$.

Case $m = 24$:

$k = \dfrac{m}{2} = 12$ and $\dim M_{12} = 2$, $E_{12}, \Delta \in M_{12}$. Thus $\vartheta(z, Q) = E_{12} + \beta_Q \Delta(z)$, $r(n, Q) = \dfrac{65520}{691}\sigma_{11}(n) + \beta_Q \tau(n)$ $^\forall n \geq 1$.
$\beta_Q = r(1, Q) - \dfrac{65520}{691}$ since $\tau(1) = 1$. $\beta_Q \neq 0$ because $r(1, Q) \in N$ and

$691 \nmid 65520$.

$$Q = \Lambda \quad : r(1,\Lambda) = 0 \Rightarrow \beta_\Lambda = -\frac{65520}{691}. \ (\Lambda: \text{ Leech lattice}).$$

$$Q = \Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8 \quad : r(1,\Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8) = 720, \ \beta_{\Gamma_8\oplus\Gamma_8\oplus\Gamma_8} = \frac{432000}{691}.$$

$$Q = \Gamma_{24} \quad : r(1,\Gamma_{24}) = 1104, \ \beta_{\Gamma_{24}} = \frac{697344}{691}, \ldots$$

There are 24 distinct classes (Niemeire 1957).
$e(\Lambda) = 2^{22}\cdot 3^9\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 23 = 8{,}315{,}553{,}613{,}086{,}720{,}000.$
$m_Q \approx 8 \times 10^{-15}$.
Let $G = O(\Lambda) = \{X \in \mathrm{GL}_{24}(\mathbb{Z}) : \Lambda = {}^tX\Lambda X\}$. Then $G/\{\pm 1\}$ is a simple group (Conway).

Case $m = 32$**:**

$k = 16$, $\dim M_{32} = 2$, E_{16}, $\Delta\cdot E_4 \in M_{16}$. Thus

$$\vartheta(z,Q) = E_{16} + \beta_Q \Delta\cdot E_{14}.$$

$m_Q \approx 4.03 \times 10^7$. Therefore there are more than 80 million classes !

Case $m = 40$**:**

$m_Q \approx 4.39 \times 10^{51}$. There are more than 8×10^{51} classes !

References

[1] A. Ogg, 'Modular Forms and Dirichlet Series', Benjamin, 1969.

[2] O.T. O'Meara, 'Introduction to Quadratic Forms', Springer-Verlag, 1963.

[3] J.W.S. Cassels, 'Rational Quadratic Forms', Academic Press, 1978.

[4] J.P. Serre, 'A Course in Arithmetic', Springer-Verlag, 1973.

[5] S. Lang, 'Introduction to Modular Forms', Springer-Verlag, 1976.

[6] J.H. Conway and N.J.A. Sloan, 'Sphere Packings, Lattices and Groups', Springer-Verlag, 1988.

[7] E. Hecke, 'Lectures on Dirichlet Series, Modular Functions and Quadratic Forms', Vandenhoek and Ruprecht, 1983.

[8] A.N. Andriarov, 'Quadratic Forms and Hecke Operators', Springer-Verlag, 1987.

[9] G. Shimura, 'Introduction to the Arithmetic Theory of Automorphic Functions', Princeton Univ. Press, 1971.

[10] C.L. Siegel, 'Lectures on the Analytic Theory of Quadratic forms', Princeton Univ. Press, 1949.

An Introduction to Hilbert Modular Forms

Dae San Kim

Department of Mathematics
Seoul Woman's University
Seoul 139 – 774, Korea

Contents

1 Classical Theory of Hilbert Modular Forms.

1.1 Notations and Conventions.

$\mathrm{GL}_2^+(\mathbb{R}) = \{\alpha \in M_2(\mathbb{R}) : \det\alpha > 0\}$ acts transitively on $\mathfrak{H} = \{z = x + iy |\ y > 0\}$ by linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

Similarly, $\mathrm{GL}_2^+(\mathbb{R})^m$ acts componentwise on $\mathfrak{H}^m$. These actions are obviously transitive, and the transformation group is

$$\approx \left(\mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times\right)^m \approx (\mathrm{SL}_2(\mathbb{R})/\{\pm 1\})^m .$$

By convention, for $z = (z_1, \cdots, z_m) \in \mathfrak{H}^m$, $r = (r_1, \cdots, r_m) \in \mathbb{Z}^m$, $t \in \mathbb{C}$, put $z^r = z_1^{r_1} \cdots z_m^{r_m}$, $tz = (tz_1, \cdots, tz_m)$, $r! = r_1! \cdots r_m!$, and $e(w) = e^{2\pi i w}$ for $w \in \mathbb{C}$.

1.2 Automorphisms of $\mathfrak{H}^m$.

Lemma 1.1 ***(Cartan Uniqueness Theorem)*** Let D be a bounded domain, $0 \in D \subseteq \mathbb{C}^m$, $t \cdot D \subseteq D$ for $t \in \mathbb{C}$ with $|t| \leq 1$. If $f : D \to D$ is holomorphic, $f(0) = 0$, $\mathrm{Jac}(f)|_0 =$ identity, then $f =$ identity on D.

Proof. In a neighborhood of 0, we have $f(z) = z + F(z) + \cdots$, where $F = (F_1, \cdots, F_m)$ and is a homogeneous polynomial of degree $p > 1$. Then $f(f(z)) = z + 2F(z) + \cdots$ and in general the k-th iterate $f_k(z) = z + kF(z) + \cdots$. Let $g_k(t) = f_k(tz)$ for $|t| \leq 1$. Then $g_k^{(p)}, i\text{-th component}(0) = kF_i(z)p!$. But by the Cauchy estimate, $|g_k^{(p)}, i\text{-th}(0)| \leq p!M/R^p$, where M depends only on D. Since $R = 1$, we obtain $|kF_i(z)p!| \leq p!M$ or $|kF_i(z)| \leq M$ for all k. Thus $F_i(z) = 0$ and hence f is the identity in a neighborhood of 0. By the identity theorem the same is true for D. ∎

Lemma 1.2 : If $g \in \mathrm{Aut}(D)$ and $g(0) = 0$ for the same D as in Lemma 1.1, then $g(z) = Az$ with $A \in \mathrm{GL}_m(\mathbb{C})$.

Proof. For $t \in \mathbb{C} - \{0\}$, $|t| \leq 1$, put $f(z) = g^{-1}(t^{-1}g(tz))$. Then

$$f : D \to D, \ f(0) = 0, \ \mathrm{Jac}(f)|_0 = \text{identity}.$$

By Lemma 1.1, $g^{-1}(t^{-1}g(tz)) = z$ for all $z \in D$, so that $g(tz) = tg(z)$ for all t, $|t| \leq 1$, $z \in D$. Write $g(z) = \sum_{n=1}^{\infty} G_n(z)$, where G_n is homogeneous of degree n. Then

$$t \sum_{n=1}^{\infty} G_n(z) = \sum_{n=1}^{\infty} G_n(tz).$$

By viewing this as a power series in t, we conclude that $g(z) = G_1(z)$. ∎

Theorem 1.1 If $\mathfrak{D} = \{z \mid |z|<1\}$, then $\mathfrak{D}^m \approx \mathfrak{H}^m$ analytically, and from this we get

$$\mathrm{Aut}(\mathfrak{H}^m) = \left(\mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times\right)^m \cdot \{\text{ permutations on } m \text{ letters}\}$$

(a semidirect product).

Proof. $\mathfrak{D} \approx \mathfrak{H}$ by a fractional linear transformation (*i.e.*, $z \overset{\sigma}{\longmapsto} \frac{z-i}{z+i}$ is such a map of $\mathfrak{D}$ onto $\mathfrak{H}$ and note that its inverse is given by $z \mapsto -i\left(\frac{z+1}{z-1}\right)$) hence also $\mathfrak{D}^m \approx \mathfrak{H}^m$. This induces

$$\mathrm{Aut}(\mathfrak{D}^m) \approx \mathrm{Aut}(\mathfrak{H}^m)$$

and takes $\left(\mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times\right)^m$ to a subgroup $G \subseteq \mathrm{Aut}(\mathfrak{D}^m)$, which is necessarily transitive on $\mathfrak{D}^m$. Let $f \in \mathrm{Aut}(\mathfrak{D}^m)$, $f(0) = a$. By transitivity, there exists $g \in G$ such that $g(a) = 0$. By Lemma 1.2, $g \circ f$ is given by a nonsingular linear map A on $\mathbb{C}^m$, say $A = (a_{ij})$ with respect to standard basis.
Since $A \in \mathrm{Aut}(\mathfrak{D}^m)$,

$$|a_{i1}z_1 + \cdots + a_{im}z_m|<1 \ \text{ for all } \ |z_j|<1.$$

Thus A induces a bijective map of $\overline{\mathfrak{D}}^m$ onto itself and maps $\partial\overline{\mathfrak{D}}^m$ onto itself. Since $|a_{i1}z_1 + \cdots + a_{im}z_m| \leq |a_{i1}| + \cdots + |a_{im}|$ for all $|z_j| \leq 1$ and for $z_1 = \frac{\overline{a}_{i1}}{|a_{i1}|}, \cdots, z_m = \frac{\overline{a}_{im}}{|a_{im}|}$, $|a_{i1}z_1 + \cdots + a_{im}z_m| = |a_{i1}| + \cdots + |a_{im}| \leq 1$, we must have $|a_{i1}| + \cdots + |a_{im}| = 1$. Fix j_0 $(1 \leq j_0 \leq m)$. If $|z_{j_0}| = 1$ and

$z_j = 0$ for $j \neq j_0$, then one of $|a_{1j_0}|, \cdots, |a_{mj_0}|$ must be 1, say $|a_{i_0j_0}| = 1$. Then from $|a_{i_01}| + \cdots + |a_{i_0m}| = 1$ we conclude that $a_{i_0j} = 0$ for $j \neq j_0$. So with some permutation π of coordinates in $\mathbb{C}^m$, $\pi \circ A$ is a diagonal and hence in G (with our choice of σ the automorphism $z \mapsto e^{i\theta}z$ of $\mathfrak{D}$ corresponds to $z \mapsto \frac{\cos\frac{\theta}{2}z + \sin\frac{\theta}{2}}{-\sin\frac{\theta}{2}z + \cos\frac{\theta}{2}}$ of $\mathfrak{H}$). Therefore $gof \in G \cdot \{\text{permutations}\} \Rightarrow f \in G \cdot \{\text{permutations}\} \Rightarrow$ the desired result by lifting back. ∎

1.3 Hilbert Modular Groups and Modular Forms.

Let F be a totally real number field of degree m over $\mathbb{Q}$, with ring of integers $\mathcal{O}$. Fix an ordering of real embeddings $\sigma_1, \cdots, \sigma_m$ of F in $\mathbb{R}$. Via σ_i we have an embedding $\mathrm{GL}_2(F) \to \mathrm{GL}_2(\mathbb{R})^m$ given by $g \mapsto (\sigma_1 g, \cdots, \sigma_m g) = (g_1, \cdots, g_m)$. Let $\mathrm{GL}_2^+(F)$ (respectively, $\mathrm{GL}_2^+(\mathcal{O})$) denote the set of elements of $\mathrm{GL}_2(F)$ (respectively, $\mathrm{GL}_2(\mathcal{O})$) with totally positive determinant. The action of $\mathrm{GL}_2^+(\mathbb{R})^m$ on $\mathfrak{H}^m$ induces that of $\mathrm{GL}_2^+(F)$ on $\mathfrak{H}^m$ via σ_i. The group $\mathrm{GL}_2^+(\mathcal{O})$ is called the full Hilbert modular group.

Definition 1.1 For any non-zero ideal $\mathfrak{n}$ of $\mathcal{O}$, define the principal congruence subgroup of level $\mathfrak{n}$ as

$$\Gamma(\mathfrak{n}) = \left\{\gamma \in \mathrm{GL}_2^+(\mathcal{O}) \mid \gamma \equiv 1_2 \bmod \mathfrak{n}\right\}.$$

A congruence subgroup (of $\mathrm{GL}_2^+(F)$) is a subgroup Γ of $\mathrm{GL}_2^+(F)$ such that $Z(\mathcal{O})\Gamma$ contains some $\Gamma(\mathfrak{n})$ with finite index, where $Z(\mathcal{O}) = \mathcal{O}^\times$ is the center of $\mathrm{GL}_2^+(\mathcal{O})$.

Definition 1.2 For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ and $z \in \mathfrak{H}$, put

$$\mu(g, z) = (\det g)^{-\frac{1}{2}}(cz + d).$$

For $g=(g_1, \cdots, g_m) \in \mathrm{GL}_2^+(\mathbb{R})^m$, $z=(z_1, \cdots, z_m) \in \mathfrak{H}^m$ and $k=(k_1, \cdots, k_m)$ in $\mathbb{Z}^m$, write

$$\mu(g, z)^k = \prod_{j=1}^{m} \mu(g_j, z_j)^{k_j}.$$

For a function on $\mathfrak{H}^m$, define

$$(f|_k g)(z) = f(g(z))\mu(g,z)^{-k}.$$

Then it is immediate to see that $f|_k gh = (f|_k g)|_k h$, for $g, h \in \mathrm{GL}_2^+(\mathbb{R})^m$.

Definition 1.3 For a congruence subgroup Γ, $k \in \mathbb{Z}^m$, $\chi{:}\Gamma \to \mathbb{C}^\times$ a character such that $\chi(\Gamma)$ is a finite group, define

$$\begin{aligned} \mathrm{Wfm}(\Gamma, k, \chi) &= \{f \text{ holomorphic on } \mathfrak{H}^m \mid f|_k\gamma = \chi(\gamma)f,\ \forall\, \gamma \in \Gamma\}, \\ \mathrm{Wfm}(\Gamma, k) &= \{f \text{ holomorphic on } \mathfrak{H}^m \mid f|_k\gamma = f,\ \forall\, \gamma \in \Gamma\}, \\ \mathrm{Wfm}(k) &= \bigcup_{\substack{\text{congruence} \\ \text{subgroups } \Gamma}} \mathrm{Wfm}(\Gamma, k). \end{aligned}$$

Proposition 1.1 Let Γ be a congruence subgroup, and let

$$\Lambda = \left\{ u \in F \;\middle|\; \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in Z(\mathcal{O})\Gamma \right\}.$$

Then $f \in \mathrm{Wfm}(\Gamma, k)$ has a Fourier expansion

$$f(z) = \sum_{\xi \in \Lambda^*} c_\xi \exp(2\pi i Tr(\xi z)),$$

where $\Lambda^* = \{\xi \in F \mid Tr(\xi\Lambda) \subset \mathbb{Z}\}$ is the dual $\mathbb{Z}$-module of Λ. Moreover, the Fourier series is absolutely convergent and uniformly so on compect subsets of $\mathfrak{H}^m$.

Proof. Note that Λ contains some nonzero ideal $\mathfrak{n}$. Since $f(z+u) = f(z)$ for $u \in \Lambda$ and f is smooth as a function of x ($z = x + iy$), f has a Fourier series expansion

$$f(x+iy) = \sum_{\xi \in \Lambda^*} c_\xi(y) \exp(2\pi i Tr(\xi x))$$

which is absolutely convergent and uniformly so for x in some compact subset of $\mathfrak{H}^m$. Since f is holomorphic for $z \in \mathfrak{H}^m$, the Cauchy-Riemann equations

$$i\frac{\partial f}{\partial x_j} = \frac{\partial f}{\partial y_j} \qquad (j = 1, \cdots, m)$$

must be satisfied. For each j, we must have

$$i \sum_{\xi \in \Lambda^*} c_\xi(y)(2\pi i \xi_j)\exp(2\pi i Tr(\xi x)) = \sum_{\xi \in \Lambda^*} \frac{\partial c_\xi(y)}{\partial y_j}\exp(2\pi i Tr(\xi x)).$$

By the uniqueness of Fourier expansions in x,

$$-2\pi \xi_j c_\xi(y) = \frac{\partial c_\xi(y)}{\partial y_j} \implies c_\xi(y) = c_\xi \exp(-2\pi Tr(\xi y))$$

for some constant c_ξ. Thus $f(z) = \sum_{\xi \in \Lambda^*} c_\xi \exp(2\pi i Tr(\xi z))$ and the Fourier series is nicely convergent as asserted. ∎

Definition 1.4 $f \in \mathrm{Wfm}(\Gamma, k)$ is called a holomorphic Hilbert modular form of weight k with respect to Γ if, for every $g \in \mathrm{GL}_2^+(F)$, the Fourier expansion

$$(f|_k g)(z) = \sum_\xi c_\xi(g)\exp(2\pi i Tr(\xi z))$$

has $c_\xi(g) = 0$ unless $\xi = 0$ or $\xi \gg 0$ (totally positive). Here one has to observe that if $f \in \mathrm{Wfm}(\Gamma, k)$ and $g \in \mathrm{GL}_2^+(F)$ then $g^{-1}\Gamma g$ is a congruence subgroup so that $f|_k g \in \mathrm{Wfm}(g^{-1}\Gamma g, k)$. Define

$$\begin{aligned} \mathrm{Mfm}(\Gamma, k) &= \left\{ f \;\middle|\; \begin{array}{c} f \text{ is holomorphic Hilbert modular form} \\ \text{of weight } k \text{ with respect to } \Gamma \end{array} \right\}, \\ \mathrm{Mfm}(k) &= \bigcup_{\substack{\text{congruence} \\ \text{subgroups } \Gamma}} \mathrm{Mfm}(\Gamma, k). \end{aligned}$$

$f \in \mathrm{Mfm}(\Gamma, k)$ is a holomorphic Hilbert modular cuspform of weight k with respect to Γ if, for every $g \in \mathrm{GL}_2^+(F)$, the Fourier expansion

$$(f|_k g)(z) = \sum_\xi c_\xi(g)\exp(2\pi i Tr(\xi z))$$

has $c_\xi(g) = 0$ unless $\xi \gg 0$. $\mathrm{Cfm}(\Gamma, k)$ and $\mathrm{Cfm}(k)$ will denote the obvious $\mathbb{C}$-vector spaces.

Remark 1.1 As contrasted to the case $F = \mathbb{Q}$, the Koecher's principle says that $\mathrm{Mfm}(\Gamma, k) = \mathrm{Wfm}(\Gamma, k)$ for $[F{:}\mathbb{Q}] > 1$.

Theorem 1.2 (Koecher's Principle) Let $m = [F:\mathbb{Q}]>1$, $f \in \mathrm{Wfm}(\Gamma, k, \chi)$. Then in the Fourier expansion of f,

$$f(z) = \sum_{\xi} c(\xi)\exp(2\pi i Tr(\xi z))$$

we have $c(\xi) = 0$ unless $\xi = 0$ or $\xi \gg 0$.
Moreover, $c(0) = 0$ unless $k_1 = k_2 = \cdots = k_m$.

Proof. Note first that Γ contains a subgroup of the form

$$\left\{\tilde{\eta} = \begin{pmatrix} \eta & \\ & \eta^{-1} \end{pmatrix} \middle| \ \eta \in U\right\},$$

where U is a subgroup of $\mathcal{O}^\times$ with finite index. Next we see that for $\eta \in U$

$$\mu(\tilde{\eta}, z)^{-k} = \eta^k, \ \tilde{\eta}(z) = \eta^2 z.$$

Thus $f(\eta^2 z) = \chi(\tilde{\eta})\eta^{-k} f(z) \implies c(\eta^{-2}\xi) = \chi(\tilde{\eta})\eta^{-k}c(\xi) \implies c(0) = 0$, unless $k_1 = k_2 = \cdots = k_m$. (By the unit theorem we can choose $\eta \in U$ such that $|\eta_1|^{k_1} \cdots |\eta_m|^{k_m} \neq 1$). In the notation of the proof of Proposition 1.1, $c_\xi(y) = c(\xi)\exp(-2\pi Tr(\xi y))$ is given by

$$\mathrm{vol}(\mathbb{R}^m/\Lambda)^{-1} \int_{\mathbb{R}^m/\Lambda} f(x+iy)\exp(-2\pi i Tr(\xi x))dx.$$

Suppose that ξ is nonzero and not totally positive, say $\xi_1<0$.
Fix $y_1 = \cdots = y_m = 1$. Then there exists $M > 0$ (independent of ξ) such that $|c(\xi)e^{-2\pi Tr(\xi)}| \leq M$ from the above integral representation of $c_\xi(y)$. Now,

$$\begin{aligned} |c(\xi)| &= |\eta^k c(\eta^{-2}\xi)| \leq M|\eta^k|e^{2\pi Tr(\eta^{-2}\xi)} \\ &= M\prod |\eta_j|^{k_j} e^{2\pi(\eta_1^{-2}\xi_1 + \cdots + \eta_m^{-2}\xi_m)}. \end{aligned}$$

Since $m > 1$, one can choose $\eta \in U$ such that $|\eta_1|<1$, $|\eta_2|, \cdots, |\eta_m| > 1$ by the unit theorem (cf. for example Janusz, Algebraic Number Fields.) Put in η^n for η and let n be large. Then the right hand side $\to 0$ and $c(\xi) = 0$. ∎

Corollary 1.1 Suppose that $[F:\mathbb{Q}] = m > 1$. Then $\mathrm{Wfm}(k) = \mathrm{Mfm}(k)$, and $\mathrm{Wfm}(k) = \mathrm{Cfm}(k)$ unless all k_j's are equal.

Proof. Apply the above theorem to $f|_k g$ for any $g \in GL_2^+(F)$. ∎

1.4 Cusps and Class Numbers.

$\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1 = \left\{ \begin{pmatrix} u \\ v \end{pmatrix} \in \mathbb{C}^2 - \{0\} \right\} / \mathbb{C}^\times$ by matrix multiplication on the left. As usual, we write

$$\mathbb{P}^1 = \mathbb{C} \cup \{i\infty = \text{ the point at infinity}\}.$$

Then the above action is just the linear fractional transformation action on the extended plane. Similarly, $\mathrm{GL}_2(\mathbb{C})^m$ acts on $(\mathbb{P}^1)^m$, componentwise and $\mathfrak{H}^m \subset \mathbb{C}^m \subset (\mathbb{P}^1)^m$.

Definition 1.5 The cusps of $\mathrm{GL}_2^+(F)$ are the points

$$(\sigma_1\alpha, \cdots, \sigma_m\alpha) = (\alpha_1, \cdots, \alpha_m) \in \mathbb{R}^m \subset \partial\mathfrak{H}^m \subset \mathbb{C}^m \subset (\mathbb{P}^1)^m$$

for $\alpha \in F$, plus the point $i\infty = (i\infty, \cdots, i\infty) \in (\mathbb{P}^1)^m$.

Remark 1.2 $\mathrm{GL}_2(F)$ clearly stabilizes the set of cusps. For a subgroup Γ of $\mathrm{GL}_2^+(F)$, we say that two cusps κ_1 and κ_2 are Γ-equivalent if $\kappa_1 = \gamma\kappa_2$ for some $\gamma \in \Gamma$.

Theorem 1.3 Let $\mathrm{SL}_2(\mathcal{O}) \subset \Gamma \subset \mathrm{GL}_2^+(\mathcal{O})$. Then there is a bijection between the ideal class group of F and Γ-equivalent classes of cusps, given by

$$(u\mathcal{O} + v\mathcal{O}) \mapsto \begin{pmatrix} u \\ v \end{pmatrix} \mathbb{C}^\times.$$

In particular, the number of Γ-inequivalent cusps is h_F.

Proof. For any pairs (u, v), $(u', v') \in F^2 - \{0\}$, they are in the same ideal class if and only if $\begin{pmatrix} u \\ v \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}) \begin{pmatrix} u' \\ v' \end{pmatrix} F^\times$. We will show that if $u\mathcal{O} + v\mathcal{O}$ and $u'\mathcal{O} + v'\mathcal{O}$ are in the same ideal class then $\begin{pmatrix} u \\ v \end{pmatrix} \mathbb{C}^\times$ and $\begin{pmatrix} u' \\ v' \end{pmatrix} \mathbb{C}^\times$ are Γ-equivalent. The converse is easy to see. Without loss of generality, we may assume that $u\mathcal{O} + v\mathcal{O} = u'\mathcal{O} + v'\mathcal{O} = \mathfrak{a}$. Put $\alpha = (u, v)$, $\alpha' = (u', v')$. Let $< x, y >= x_1y_1 + x_2y_2$ be the usual pairing on F^2. $< \alpha, \mathcal{O}^2 >= \mathfrak{a} \implies < \alpha, \mathfrak{a}^{-1}\mathcal{O}^2 >= \mathcal{O} \implies \exists\ \gamma \in \mathfrak{a}^{-1}\mathcal{O}^2$ such that $< \alpha, \gamma >= 1$. Since $\alpha \in \mathfrak{a}\mathcal{O}^2$, $1 = < \alpha, \gamma > \in < \mathfrak{a}\mathcal{O}^2, \gamma > \subset < \mathfrak{a}\mathcal{O}^2, \mathfrak{a}^{-1}\mathcal{O}^2 >= \mathcal{O} \implies < \mathfrak{a}\mathcal{O}^2, \gamma > = \mathcal{O}$. Put $M = \{ x \in$

$\mathfrak{a}\mathcal{O}^2 \mid <x,\gamma>=0\}$. Then we claim that $\mathfrak{a}\mathcal{O}^2 = \mathcal{O}\alpha \oplus M$. For $z \in \mathfrak{a}\mathcal{O}^2$, write $z = <z,\gamma>\alpha + (z - <z,\gamma>\alpha)$ and see that $z \in \mathcal{O}\alpha + M$. The rest of claim is trivial. Now, $\mathfrak{a}\mathcal{O}^2 = \mathcal{O}\alpha \oplus M = \mathcal{O}\alpha' \oplus M'$ with M' analogue for α'. According to the structure theorem for finitely generated modules over Dedekind domain, every finitely generated torsionless module over a Dedekind domain R is of the form $R^n \oplus \mathfrak{m}$ for an ideal $\mathfrak{m}$ whose isomorphism class is uniquely determined, and for a uniquely determined $0 \leq n \in \mathbb{Z}$. Thus $M = \mathfrak{m}\beta$, $M' = \mathfrak{m}'\beta'$, $\mathfrak{m} \sim \mathfrak{m}'$ (they are in the same ideal class) for some ideals $\mathfrak{m}$, $\mathfrak{m}'$ of $\mathcal{O}$ and for some $\beta, \beta' \in F^2 - \{0\}$. By adjusting β' we may assume $\mathfrak{m} = \mathfrak{m}'$. Since $\wedge^2 F^2$ is one-dimensional over F, $\alpha \wedge \beta = \alpha' \wedge \beta' \cdot (\text{unit})$. By replacing β' by $\beta' \cdot (\text{unit})$, we have $\alpha \wedge \beta = \alpha' \wedge \beta'$ and $\mathcal{O}\alpha \oplus \mathfrak{m}\beta = \mathfrak{a}\mathcal{O}^2 = \mathcal{O}\alpha' \oplus \mathfrak{m}\beta'$. Define $A \in \mathrm{GL}_2(F)$ by $A\alpha = \alpha'$, $A\beta = \beta'$. Then $A \in \mathrm{SL}_2(F)$ and also $A \in \mathrm{GL}_2(\mathcal{O})$, since both A and A^{-1} send $\mathfrak{a}\mathcal{O}^2$ and hence $\mathcal{O}^2$ to itself. Thus $A \in \mathrm{SL}_2(\mathcal{O})$. ∎

Corollary 1.2 For any congruence group Γ, there are only finitely many Γ-inequivalent cusps. Let $\{\kappa_1, \cdots, \kappa_\nu\}$ be a set of irredundant representatives.

Then $$\mathrm{GL}_2^+(F) = \bigcup_i \Gamma\delta_i P \qquad \text{(disjoint union)},$$

where P is the group of upper triangular matrices in $\mathrm{GL}_2^+(F)$ and $\delta_i \in \mathrm{SL}_2(F)$ is such that $\delta_i(i\infty) = \kappa_i$.

Proof. Assume that $Z(\mathcal{O})\Gamma \supset \Gamma(\mathfrak{n})$ for some nonzero ideal $\mathfrak{n}$. Then there are at most $h_F \nu' \, \Gamma(\mathfrak{n})-$ and hence Γ-inequivalent cusps, where $\nu' = [\mathrm{GL}_2^+(\mathcal{O}) : \Gamma(\mathfrak{n})]$. Let $g \in \mathrm{GL}_2^+(F)$. Then $g(i\infty) = \kappa$ for some cusp $\kappa \implies$ there exist $\gamma \in \Gamma$ and i $(1 \leq i \leq \nu)$ such that $\gamma g(i\infty) = \gamma(\kappa) = \kappa_i \implies \delta_i^{-1}\gamma g(i\infty) = \delta_i^{-1}(\kappa_i) = i\infty$. Since P is the isotropy group of $i\infty$ in $\mathrm{GL}_2^+(F)$,

$$\delta_i^{-1}\gamma g \in P \implies g \in \gamma^{-1}\delta_i P.$$ ∎

Corollary 1.3 Let $f \in \mathrm{Wfm}(\Gamma, k)$ and let

$$(f|_k g)(z) = \sum_\xi c_\xi(g) \exp(2\pi i Tr(\xi z))$$

for $g \in \mathrm{GL}_2^+(F)$. Let $\{\delta_i\}$ be a finite set of representatives for $\Gamma \backslash \mathrm{GL}_2^+(F)/P$. Then f is a cusp form if and only if $c_\xi(g) = 0$ for ξ not totally positive merely for $g \in \{\delta_i\}$.

Proof. Let $\varphi \in \mathrm{Wfm}(\Gamma, k)$ with the Fourier series expansion

$$\varphi(z) = \sum_{\xi} c(\xi)\exp(2\pi i Tr(\xi z)).$$

Then for $p = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in P$,

$$\begin{aligned}(\varphi|_k p)(z) &= \left(\frac{a}{d}\right)^{\frac{k}{2}} \sum_{\xi} c(\xi)\exp\left(2\pi i Tr\left(\xi\left(\frac{az}{d}+\frac{b}{d}\right)\right)\right) \\ &= \sum_{\xi}\left\{\left(\frac{a}{d}\right)^{\frac{k}{2}} c\left(\frac{d}{a}\xi\right)\exp\left(2\pi i Tr\left(\frac{b}{a}\xi\right)\right)\right\}\exp(2\pi i Tr(\xi z)).\end{aligned}$$

Thus the Fourier coefficients of φ vanish for ξ not totally positive $\iff$ those of $\varphi|_k p$ do. For $g \in \mathrm{GL}_2^+(F)$, $g = \gamma\delta_i p$ for some $\gamma \in \Gamma$, $p \in P$ and hence $f|_k g = (f|_k\delta_i)|_k p$. Note the above observation yields the result. ∎

Remark 1.3 Suppose that $[F{:}\mathbb{Q}] = m > 1$. In this case we saw that $\mathrm{Wfm}(\Gamma, k)$
$= \mathrm{Cfm}(\Gamma, k)$ unless all k_j's are equal. Thus Corollary 1.3 is useful only when $m = 1$ (elliptic modular case) or $m > 1$ and equal weight case.

1.5 Siegel sets (An Approximate Fundamental Domain).

Definition 1.6 A standard Siegel set is defined to be a subset of $\mathfrak{H}^m$ of the form

$$S = \{z \in \mathfrak{H}^m \mid \mathrm{Re}(z) \in R,\ \mathrm{Im}(z_j) \geq B,\ j = 1, \cdots, m\},$$

where R is a compact set in $\mathbb{R}^m$ and $B > 0$.

Theorem 1.4 Let Γ be a congruence subgroup. Let $\{\kappa_1, \cdots, \kappa_\nu\}$ be representatives for the Γ-inequivalent cusps and δ_j an element of $\mathrm{SL}_2(F)$ such that $\delta_j(i\infty) = \kappa_j$ for each $j = 1, \cdots, \nu$. Then there exists a standard Siegel set S such that $\mathfrak{H}^m = \Gamma\left(\bigcup_j \delta_j S\right)$.

Proof. We may as well assume that Γ contains $Z(\mathcal{O})$, since $Z(\mathcal{O})$ acts trivially on $\mathfrak{H}^m$. We saw that

$$\mathrm{GL}_2^+(F) = \bigcup_j \Gamma\delta_j p \implies \mathrm{GL}_2^+(F) = \bigcup_i P\delta_i^{-1}\Gamma.$$

Lemma 1.3 For every $z \in \mathfrak{H}^m$, there exist $c, d \in \mathcal{O}$ (not both zero) so that $|\sigma_j(c)z_j + \sigma_j(d)|^2 < Ky_j \ \ (j = 1, \cdots, m)$, where K is a constant such that

$$K > 4D_F^{\frac{1}{m}}/\pi \ \text{ and } \ y_j = \mathrm{Im}(z_j).$$

Proof of Lemma 1.3. Consider the lattice $\Lambda = \mathcal{O}z + \mathcal{O} \subset \mathbb{C}^m$.
Pick a $\mathbb{Z}$-basis $w_1, \cdots, w_m$ of $\mathcal{O}$, so that Λ is generated by $(w_k^{(1)}, \cdots, w_k^{(m)})$ and $(z_1 w_k^{(1)}, \cdots, z_m w_k^{(m)})$ for $k = 1, \cdots, m$. Here $w_k^{(j)} = \sigma_j w_k$. Then

$$\mathrm{vol}(\mathbb{C}^m/\Lambda) = \begin{vmatrix} w_1^{(1)} & \cdots & w_m^{(1)} & & & \\ \vdots & & \vdots & & * & \\ w_1^{(m)} & \cdots & w_m^{(m)} & & & \\ & & & y_1 w_1^{(1)} & \cdots & y_1 w_1^{(m)} \\ & & & \vdots & & \vdots \\ & & & y_m w_1^{(m)} & \cdots & y_m w_m^{(m)} \end{vmatrix}$$

$$= (y_1 \ldots y_m) D_F.$$

For a constant K, the volume of the convex open set

$$V = \{u \in \mathbb{C}^m \mid |u_j|^2 < Ky_j \}$$

is $\pi^m K^m (y_1 \ldots y_m)$. So by Minkowski's theorem if

$$\pi^m K^m (y_1 \ldots y_m) > 2^{2m} D_F (y_1 \ldots y_m) \ i.e., \ K > 4D_F^{\frac{1}{m}}/\pi$$

then there exist $c, d \in \mathcal{O}$ (not both zero) such that

$$|\sigma_j(c)z_j + \sigma_j(d)|^2 < Ky_j, \ j = 1, \cdots, m. \qquad \blacksquare$$

Take $a, b \in F$ so that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F)$. Then

$$\mathrm{Im}((gz)_j) = \frac{\mathrm{Im}(z_j)}{|\sigma_j(c)z_j + \sigma_j(d)|^2} > \frac{1}{K}.$$

There exist $p = \begin{pmatrix} p_{11} & p_{12} \\ 0 & p_{22} \end{pmatrix} \in P$, $\gamma \in \Gamma$, and some i, such that $g = p\delta_i^{-1}\gamma$, which implies that $(c \ d) = p_{22}(c_i \ d_i)\gamma$ with $\delta_i^{-1} = \begin{pmatrix} * & * \\ c_i & d_i \end{pmatrix}$.

Lemma 1.4 There is some nonzero ideal $\mathfrak{n}$ of $\mathcal{O}$ (depending on Γ) such that entries of $\gamma \in \Gamma$ lie in $\mathfrak{n}^{-1}$.

Proof of Lemma 1.4. For some ideal $\mathfrak{m}$, Γ contains $\Gamma(\mathfrak{m})$ with finite index. If $\{\gamma_j\}$ is a finite set of coset representatives for $\Gamma/\Gamma(\mathfrak{m})$ and $\mathfrak{n}$ is a nonzero ideal of $\mathcal{O}$ such that all the entries of every γ_j lie in $\mathfrak{n}^{-1}$, then such an $\mathfrak{n}$ is a desired one. ∎

From $p_{22}(c_i\ d_i)\gamma = (c\ d)$ and the Lemma 1.4, we obtain

$$\begin{aligned} & p_{22}(c_i\mathcal{O} + d_i\mathcal{O}) \subset \mathfrak{n}^{-1}(c\mathcal{O} + d\mathcal{O}) \\ \Longrightarrow\ & |\mathrm{Norm}_{F/\mathbb{Q}} p_{22}| N(c_i\mathcal{O} + d_i\mathcal{O}) \geq N\mathfrak{n}^{-1} N(c\mathcal{O} + d\mathcal{O}) \\ \Longrightarrow\ & |\mathrm{Norm}_{F/\mathbb{Q}} p_{22}|^{-1} \leq N(c_i\mathcal{O} + d_i\mathcal{O}) N\mathfrak{n}/N(c\mathcal{O} + d\mathcal{O}) \\ & \leq N(c_i\mathcal{O} + d_i\mathcal{O}) N\mathfrak{n}. \end{aligned}$$

Put $A = \max_i N(c_i\mathcal{O} + d_i\mathcal{O}) N\mathfrak{n}$. Then $|\mathrm{Norm}_{F/\mathbb{Q}} p_{22}|^{-1} \leq A$. ∎

Lemma 1.5 There exist $c, c' > 0$ (depending only on $\mathcal{O}$) such that for every $a \in F$ there exists $\eta \in \mathcal{O}^\times$ such that

$$c|\mathrm{Norm}_{F/\mathbb{Q}} a|^{\frac{1}{m}} \leq |\sigma_i(\eta a)| \leq c'|\mathrm{Norm}_{F/\mathbb{Q}} a|^{\frac{1}{m}}.$$

Proof of Lemma 1.5. Take independent units $\varepsilon_1, \cdots, \varepsilon_{m-1} \in \mathcal{O}^\times$ and consider the system of equations

$$\sum_{k=1}^{m-1} x_k \log |\varepsilon_k^{(\nu)}| = \log \left| \frac{(Na)^{\frac{1}{m}}}{a^{(\nu)}} \right| \qquad for\ \nu = 1, \cdots, m.$$

Clearly, the last equation is dependent on the $(m-1)$ previous ones and the absolute value of the determinant of the coefficient matrix of the first $(m-1)$ equations is the regulator of F. Thus the system has a unique solution $x_1, \cdots, x_{m-1}$. Choose $y_k \in \mathbb{Z}$ so that $|x_k - y_k| \leq \frac{1}{2}$, for $k = 1, \cdots, m-1$. Then,

$$\left| \sum_k y_k \log \left|\varepsilon_k^{(\nu)}\right| - \log \left| \frac{(Na)^{\frac{1}{m}}}{a^{(\nu)}} \right| \right| \leq \sum_k |y_k - x_k| \left| \log \left|\varepsilon_k^{(\nu)}\right| \right| \leq \frac{1}{2} \sum_k \left| \log \left|\varepsilon_k^{(\nu)}\right| \right|,$$

for $\nu = 1, \cdots, m$. Put $M = \max_\nu \frac{1}{2} \sum_k \left| \log \left| \varepsilon_k^{(\nu)} \right| \right|$. Then the inequalities hold with $c = e^{-M}$, $c' = e^M$, $\eta = \varepsilon_1^{y_1} \cdots \varepsilon_{m-1}^{y_{m-1}} \in \mathcal{O}^\times$. ∎

By applying Lemma 1.5 with $a = p_{22}$,

$$|\sigma_j(\eta p_{22})|^{-1} \leq c^{-1} |\mathrm{Norm}_{F/\mathbb{Q}} p_{22}|^{-\frac{1}{m}} \leq c^{-1} A^{\frac{1}{m}}$$

with $\tilde{\eta} = \begin{pmatrix} \eta & \\ & \eta \end{pmatrix} \in Z(\mathcal{O})$, replacing p by $p\tilde{\eta}$ and γ by $\gamma\tilde{\eta}^{-1}$ we may assume that $|\sigma_j(p_{22})|^{-1} \leq c^{-1} A^{\frac{1}{m}}$. Combining this with

$$K^{-1} < \mathrm{Im}((gz)_j) = \mathrm{Im}((p\delta_i^{-1}\gamma z)_j) = \mathrm{Im}((\delta_i^{-1}\gamma z)_j)/\sigma_j(p_{22})^2, \ (j = 1, \cdots, m),$$

we get

$$\mathrm{Im}((\delta_i^{-1}\gamma z)_j) > K^{-1}\sigma_j(p_{22})^2 \geq K^{-1} c^2 A^{-\frac{2}{m}}$$

for $j = 1, \cdots, m$. Note that if $\delta_i^{-1} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ then

$$\delta_i \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \delta_i^{-1} = \begin{pmatrix} 1 + c_i d_i u & d_i^2 u \\ -c_i^2 u & 1 - c_i d_i u \end{pmatrix}.$$

So we may choose an ideal $\mathfrak{n}$ of $\mathcal{O}$ sufficiently small so that $\Gamma(\mathfrak{n}) \subset \Gamma$ and $\delta_i \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \delta_i^{-1} \in \Gamma$ for all $u \in \mathfrak{n}$ and for all i. Let R be a compact subset of $\mathbb{R}^m$, so that $R + \mathfrak{n} = \mathbb{R}^m$. Put $\tilde{u} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \Gamma(\mathfrak{n}) \subset \Gamma$, for $u \in \mathfrak{n}$. Choose $u \in \mathfrak{n}$, so that

$$(\tilde{u}\delta_i^{-1}\gamma)z \in S = \left\{ z \in \mathfrak{H}^m \mid \mathrm{Im}(z_j) > K^{-1} c^2 A^{-\frac{2}{m}}, \ \mathrm{Re}(z) \in R \right\}.$$

Here one should note that $\mathrm{Im}(\delta_i^{-1}\gamma)z = \mathrm{Im}(\tilde{u}\delta_i^{-1}\gamma)z$. Since $\delta_i \tilde{u} \delta_i^{-1} \in \Gamma$,

$$\tilde{u}\delta_i^{-1} = \delta_i^{-1}\gamma', \text{ for some } \gamma' \in \Gamma \implies (\delta_i^{-1}\gamma'\gamma)z \in S \implies z \in \Gamma(\bigcup_i \delta_i S). \quad ∎$$

1.6 Finite Dimensionality of Spaces of Cuspforms.

Theorem 1.5 Let Γ be a congruence subgroup, $k = (k_1, \ldots, k_m) \in \mathbb{Z}^m$. Then $\dim_{\mathbb{C}} \mathrm{Cfm}(\Gamma, k)$ is finite. Moreover, $\mathrm{Mfm}(\Gamma, k) = 0$ if some $k_i < 0$ or some $k_i = 0$ and some $k_j > 0$, and $\mathrm{Mfm}(\Gamma, 0) = \mathbb{C}$.

Corollary 1 of Proof : For a fixed congruence subgroup Γ and weight k, and a cuspform $f(z) = \sum_{\xi} c(\xi)\exp(2\pi i Tr(\xi z)) \in \mathrm{Cfm}(\Gamma, k)$, there is a constant $c_1 > 0$ such that $|c(\xi)| \leq c_1 \xi^{\frac{k}{2}}$.

Corollary 2 of Proof : Given a cuspform f of weight k, there exists a constant $c_2 > 0$ so that for any $x + iy = z \in \mathfrak{H}^m$, $y^{k/2}|f(z)| \leq c_2$.

Corollary 3 of Proof : Given a Siegel set S and a cuspform f of weight k, there are constants $c_3, c_4 > 0$ so that for $z = x + iy \in S$,

$$y^{k/2}|f(z)| \leq c_4 \exp(-c_3 y^{\frac{1}{m}}).$$

Lemma 1.6 Take $\alpha, c > 0$.

(i) $\sup_{y>0} y^{\alpha}\exp(-cy) = \left(\frac{\alpha}{ec}\right)^{\alpha}$.

(ii) For $y > 0$, $y^{\alpha} \leq \left(\frac{\alpha}{ec}\right)^{\alpha} \exp(cy)$.

(iii) For $y_1, \ldots, y_m > 0$,

$$\inf\{\sum_i \xi_i y_i \mid \xi_1, \ldots, \xi_m > 0,\ \prod_i \xi_i \geq n > 0\} = mn^{\frac{1}{m}} \left(\prod_i y_i\right)^{\frac{1}{m}}.$$

For the proof of Theorem 1.5, the following ingrediants will be needed. Let $\{\kappa_1, \ldots, \kappa_\nu\}$ be the set of Γ-inequivalent cusps, and choose $\delta_i \in \mathrm{SL}_2(F)$ so that $\delta_i(i\infty) = \kappa_i$ with $\delta_1 = 1_2$. Let $f \in \mathrm{Cfm}(\Gamma, k)$. If for each i, Λ_i is the lattice of translations in x leaving $f|_k\delta_i$ invarient, Λ_i^* the dual lattice with respect to Tr, and Λ_i^+ the set of totally positive elements of Λ_i^*, then by Koecher's principle

$$(f|_k\delta_i)(z) = \sum_{\xi \in \Lambda_i^+} c_i(\xi)\exp(2\pi i Tr(\xi z)).$$

Let S be a Siegel set for Γ so that $\mathfrak{H}^m = \Gamma(\bigcup_i \delta_i S)$, where

$$S = \{z \in \mathfrak{H}^m \mid \mathrm{Im}(z_i) \geq \eta > 0,\ \mathrm{Re}(z) \text{ is in a fixed compact subset of } \mathbb{R}^m\}.$$

Lemma 1.7 Assume that $f \in \mathrm{Cfm}(\Gamma, k)$ is such that $c_i(\xi) = 0$ for all indices i and $N\xi = \prod_i \xi_i \leq n(\geq 0)$. Then

$$\sup\{y^{\frac{k}{2}}|f(z)| \mid z \in \mathfrak{H}^m\} = \sup\{y^{\frac{k}{2}}|f(z)| \mid z \in \bigcup_i \delta_i S\}$$

is finite and the supremum is attained.

Proof. Note first that $y^{\frac{k}{2}}|f(z)|$ is Γ-invariant and hence that the asserted equality holds. Put $d = \sup\{1, k_1, \ldots, k_m\}$. For any $\xi = (\xi_1, \ldots, \xi_m)$ with all $\xi_i > 0$, $N\xi \geq q(> 0)$, and $x + iy \in S$,

$$\begin{aligned}
\prod_i y_i^{\frac{k_i}{2}} &= \eta^{\sum \frac{k_i}{2}} \prod_i \left(\frac{y_i}{\eta}\right)^{\frac{k_i}{2}} \leq \eta^{\sum \frac{k_i}{2}} \prod_i \left(\frac{y_i}{\eta}\right)^{\frac{d}{2}} \\
&\leq \eta^{\sum \frac{k_i}{2}} \prod_i \left(\frac{d}{2e\pi\xi_i\eta}\right)^{\frac{d}{2}} \times \exp(\pi Tr(\xi y)) \\
&\leq \eta^{\sum \frac{k_i}{2}} \left(\frac{d}{2e\pi\eta}\right)^{\frac{dm}{2}} q^{-\frac{d}{2}} \exp(\pi Tr(\xi y))
\end{aligned}$$

(by applying (ii) of Lemma 1.6 with $y = \frac{y_i}{\eta}$, $\alpha = \frac{d}{2}$, $c = \pi\xi_i\eta$).
By assumption in the Fourier expansion of $f|_k\delta_i$ only those coefficients $c_i(\xi)$ with $\xi \in \Lambda_i^+$, $N\xi > n$ appear and there exists $\varepsilon > 0$ such that $N\xi \geq n + \varepsilon$ for such ξ's. By the above estimate, taking $z \in S$,

$$\begin{aligned}
&\mathrm{Im}(\delta_i z)^{\frac{k}{2}}|f(\delta_i z)| = y^{\frac{k}{2}}|(f|_k\delta_i)(z)| \\
\leq\ & y^{\frac{k}{2}} \sum_{\substack{\xi \in \Lambda_i^+ \\ N\xi \geq n+\varepsilon}} |c_i(\xi)| \exp(-2\pi Tr(\xi y)) \\
\leq\ & \eta^{\sum \frac{k_i}{2}} \left(\frac{d}{2e\pi\eta}\right)^{\frac{dm}{2}} (n+\varepsilon)^{-\frac{d}{2}} \sum_{\xi} |c_i(\xi)| \exp(-\pi Tr(\xi y)),
\end{aligned}$$

which is convergent as being the series of the absolute values of $(f|_k\delta_i)\left(\frac{z}{2}\right)$. Since each term goes to zero as $y_i \to 0$ for $y_i \geq \eta > 0$, the series itself tends to zero by the dominated convergence theorem for series. Thus the supremum is finite and is attained. This also shows the Corollary 2 of proof. ∎

Lemma 1.8 $M = \sup\left\{ \exp\left(\pi m n^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}}\right) \times |f(z)| \;\middle|\; z = x + iy \in S \right\}$ is finite and is attained.

Proof. As in the proof of Lemma 1.7,

$$f(z) = \sum_{\substack{\xi \in \Lambda_i^+ \\ N\xi \geq n+\varepsilon}} c_1(\xi) \exp(2\pi i \mathrm{Tr}(\xi z)) \quad \text{for some } \varepsilon > 0.$$

For any $\xi \in \Lambda_i^+$ with $N\xi \geq n + \varepsilon$, by (iii) of Lemma 1.6

$$\begin{aligned} m n^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}} &= \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}} \times m(n+\varepsilon)^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}} \\ &\leq \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}} Tr(\xi y). \end{aligned}$$

Thus

$$\begin{aligned} & \exp(\pi m n^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}}) |f(z)| \\ \leq & \sum_\xi |c_1(\xi)| \exp\left(\pi \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}} Tr(\xi y)\right) \exp(-2\pi Tr(\xi y)) \\ = & \sum_\xi |c_1(\xi)| \exp\left(-\pi \left\{2 - \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}}\right\} Tr(\xi y)\right), \end{aligned}$$

which is convergent as being the series of absolute values of the terms of the Fourier series at $\frac{1}{2}\pi \left\{2 - \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}}\right\} z \in \mathfrak{H}^m$. To finish up the proof, apply the same reasoning as in the proof of the Lemma 1.7. ∎

Corollary of Lemma 1.7, 1.8 : There are constants $c_3, c_4 > 0$ such that

$$y^{\frac{k}{2}} |f(z)| \leq c_4 \exp(-c_3 y^{\frac{1}{m}}) \text{ for } z = x + iy \in S.$$

Proof. By the proof of Lemma 1.7, for $z \in S$,

$$y^{\frac{k}{2}} |f(z)| \leq c' \sum_\xi |c_1(\xi)| \exp(-\pi Tr(\xi y)) \qquad \text{for some } c' > 0.$$

Then by the proof of Lemma 1.8,

$$\begin{aligned} & \exp\left(\pi m n^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}}\right) |f(z)| y^{\frac{k}{2}} \\ \leq\ & c' \sum_{\xi} |c_1(\xi)| \exp\left(\pi \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}} Tr(\xi y)\right) \exp(-\pi Tr(\xi y)) \\ \leq\ & c' \sum_{\xi} |c_1(\xi)| \exp\left(-\pi \left\{1 - \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}}\right\} Tr(\xi y)\right) \end{aligned}$$

from which the result follows. ∎

Proof of Theorem 1.5. By Lemma 1.7, there exist i and $z_0 = x_0 + iy_0 \in S$ such that

$$y^{k/2}|f(z)| \leq \mathrm{Im}(\delta_i z_0)^{k/2} \times |f(\delta_i z_0)| = y_0^{k/2} |(f|_k \delta_i)(z_0)|$$

for $z \in \mathfrak{H}^m$. By applying Lemma 1.8 to $f|_k\delta_i$ instead of f we may assume that for any $z \in \mathfrak{H}^m$,

$$|f(z)| \leq y^{-\frac{k}{2}} y_0^{\frac{k}{2}} M \exp(-\pi m n^{\frac{1}{m}} \prod_i y_{0i}^{\frac{1}{m}}).$$

Note that

$$\begin{aligned} m \prod_i y_{0i}^{\frac{1}{m}} &= \prod_i y_{0i}^{\frac{1}{m}} + \cdots + \prod_i y_{0i}^{\frac{1}{m}} \\ &\geq \eta^{\frac{m-1}{m}} y_{01}^{\frac{1}{m}} + \cdots + \eta^{\frac{m-1}{m}} y_{0m}^{\frac{1}{m}} \\ &= \eta^{\frac{m-1}{m}} (y_{01}^{\frac{1}{m}} + \cdots + y_{0m}^{\frac{1}{m}}). \end{aligned}$$

Thus

$$(*) \qquad |f(z)| \leq y^{-\frac{k}{2}} y_0^{\frac{k}{2}} M \exp(-\pi (n\eta^{m-1})^{\frac{1}{m}} \sum y_{0i}^{\frac{1}{m}}).$$

Now,

$$\begin{aligned} & |c_1(\xi)| \\ =\ & \exp(2\pi Tr(\xi y)) \left| \mathrm{vol}(\mathbb{R}^m/\Lambda_1)^{-1} \int_{\mathbb{R}^m/\Lambda_1} \exp(-2\pi Tr(\xi x)) f(x+iy) dx \right| \\ (**)\quad \leq\ & \exp(2\pi Tr(\xi y)) \sup\{|f(x+iy)| \mid x \in \mathbb{R}^m/\Lambda_1\} \\ \leq\ & \exp(2\pi Tr(\xi y)) y^{-\frac{k}{2}} y_0^{\frac{k}{2}} M \times \exp(-\pi (n\eta^{m-1})^{\frac{1}{m}} \sum y_{0i}^{\frac{1}{m}}). \end{aligned}$$

If some $k_i < 0$, then by letting $y_i \to 0+$ we get $c_1(\xi)$ for every ξ *i.e.*, $\mathrm{Cfm}(\Gamma, k) = 0$. We will use the fact that there exist not identically zero cuspforms for some suffciently small congruence group. The proof will be given in section 1.9. Let $\varphi \in \mathrm{Mfm}(\Gamma, k)$ with some $k_i < 0$, and let f be some cuspform not identically zero. Then $\varphi^n f$ is a cuspform with some negative weight component for large enough n and hence $\varphi^n f = 0 \implies \varphi = 0$. By replacing y by $\frac{1}{\xi}$ in $(**)$,

$$\left|c_1(\xi)\xi^{-\frac{k}{2}}\right| \leq \exp(2\pi m) y_0^{\frac{k}{2}} M \times \exp\left(-\pi(n\eta^{m-1})^{\frac{1}{m}} \sum y_{0i}^{\frac{1}{m}}\right),$$

which proves the Corollary 1 of proof. If $k = 0$ and $\varphi \in \mathrm{Mfm}(\Gamma, 0)$, then granting the assertion of the theorem for $k > 0$, $\varphi^n f \in \mathrm{Cfm}(\Gamma \bigcap \Gamma', k')$ for any not identically zero $f \in \mathrm{Cfm}(\Gamma', k')$ and every $0 \leq n \in \mathbb{Z}$. Since these can not be linearly independent, there is a nontrivial relation

$$\sum_n \alpha_n \varphi^n f = 0 \Longrightarrow \sum_n \alpha_n \varphi^n = 0$$

$\Longrightarrow \varphi$ is algebraic over $\mathbb{C} \Longrightarrow \varphi$ is a constant. If some $k_i = 0$ and some $k_j > 0$, then f is a cuspform and $|f(z)|y^{\frac{k}{2}}$ attains its maximum at a certain point $z^{(0)} \in \mathfrak{H}^m$ by Lemma 1.7. We may assume $k_1 = 0$.

$$\begin{aligned} & |f(z_1, z_2^{(0)}, \cdots, z_m^{(0)})| y_1^{\frac{k_1}{2}} {y_2^{(0)}}^{\frac{k_2}{2}} \cdots {y_m^{(0)}}^{\frac{k_m}{2}} \\ \leq\ & |f(z_1^{(0)}, z_2^{(0)}, \cdots, z_m^{(0)})| {y_1^{(0)}}^{\frac{k_1}{2}} {y_2^{(0)}}^{\frac{k_2}{2}} \cdots {y_m^{(0)}}^{\frac{k_m}{2}} \end{aligned}$$

$$\Longrightarrow \qquad |f(z_1, z_2^{(0)}, \cdots, z_m^{(0)})| \leq |f(z_1^{(0)}, z_2^{(0)}, \cdots, z_m^{(0)})| \qquad \text{for all } z_1 \in \mathfrak{H}.$$

Thus $z_1 \mapsto f(z_1, z_2^{(0)}, \cdots, z_m^{(0)})$ is constant by maximum modulus principle. Let Λ be the lattice of translation in x and let $a \in \Lambda$. Then

$$\begin{aligned} f(z_1^{(0)}, \cdots, z_m^{(0)}) &= f(z_1, z_2^{(0)}, \cdots, z_m^{(0)}) \\ &= f(z_1 + a_1, z_2^{(0)} + a_2, \cdots, z_m^{(0)} + a_m) \\ &= f(z_1, z_2^{(0)} + a_2, \cdots, z_m^{(0)} + a_m). \end{aligned}$$

Since $\Lambda \to \mathbb{R}^{m-1}$ given by $a \mapsto (a_2, \cdots, a_m)$ has dense image, f only depends on the imaginary part of z. Since f is holomorphic, it is constant and hence zero. Finally, we consider the case that every $k_i > 0$. From $(*)$ and using (i)

of Lemma 1.6,

$$\begin{aligned}|f(z)| &\leq y^{-\frac{k}{2}} M y_0^{\frac{k}{2}} \exp(-\pi(n\eta^{m-1})^{\frac{1}{m}} \sum y_{0i}^{\frac{1}{m}}) \\ &\leq y^{-\frac{k}{2}} M \prod_i \sup\Big\{t^{mk_i/2}\exp(-\pi(n\eta^{m-1})^{\frac{1}{m}} t) \mid t>0\Big\} \\ &\leq y^{-\frac{k}{2}} M \prod_i \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{n\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{mk_i/2}.\end{aligned}$$

This yields

$$\begin{aligned}|c_1(\xi)| &\leq \exp(2\pi Tr(\xi y))\left|\mathrm{vol}(\mathbb{R}^m/\Lambda_1)^{-1}\int_{\mathbb{R}^m/\Lambda_1}\exp(-2\pi i Tr(\xi x))f(x+iy)dx\right| \\ &\leq \exp(2\pi Tr(\xi y)) y^{-\frac{k}{2}} M \prod_i \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{n\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{mk_i/2}.\end{aligned}$$

$$(***) \qquad |c_1(\xi)| \leq M \prod_i \left(\frac{4\pi e\xi_i}{k_i}\right)^{k_i/2} \times \prod_i \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{n\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{mk_i/2},$$

by minimizing over $\{(y_1,\cdots,y_m) \mid y_j>0\}$ ((i) of Lemma 1.6). Put

$$M' = \prod_i \left(\frac{4\pi e}{k_i}\right)^{k_i/2} \times \prod_i \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{n\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{mk_i/2}.$$

Let $w = u+iv$ be the point in S where

$$M = \sup\Big\{\exp(\pi m n^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}}) \times |f(z)| \mid z = x+iy \in S\Big\}$$

is attained. Then

$$\begin{aligned}|f(w)| &= M\exp(-\pi m n^{\frac{1}{m}} \prod_i v_i^{\frac{1}{m}}) \\ &\leq \sum_\xi |c_1(\xi)|\exp(-2\pi Tr(\xi v)) \\ &\leq MM' \sum_\xi \prod_i \xi_i^{\frac{k_i}{2}} \exp(-2\pi Tr(\xi v)) \qquad \text{by } (***).\end{aligned}$$

By (ii) of Lemma 1.6, $\prod_i \xi_i^{\frac{k_i}{2}} \leq \left\{\prod_i (k_i/\pi e v_i)^{k_i/2}\right\} \exp(\frac{1}{2}\pi Tr(\xi v))$.
As in the proof of Lemma 1.8, there exists $\varepsilon > 0$ such that

$$mn^{\frac{1}{m}} \prod_i y_i^{\frac{1}{m}} \leq \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}} Tr(\xi y)$$

for $\xi \in \Lambda_1^+$ with $N\xi > n$. Hence

$$M\exp(-\pi m n^{\frac{1}{m}} \prod_i v_i^{\frac{1}{m}}) \leq MM' \sum_\xi \left\{\prod_i (k_i/\pi e v_i)^{k_i/2}\right\} \exp(-\frac{3}{2}\pi Tr(\xi v)).$$

Then we have

$$\begin{aligned} 1 &\leq M' \left\{\prod_i (k_i/\pi e v_i)^{k_i/2}\right\} \sum_\xi \exp\left(-\pi \left\{\frac{3}{2} - \left(\frac{n}{n+\varepsilon}\right)^{\frac{1}{m}}\right\} Tr(\xi v)\right) \\ &\leq M' \left\{\prod_i (k_i/\pi e v_i)^{k_i/2}\right\} \sum_\xi \exp\left(-\frac{1}{2}\pi\eta Tr(\xi)\right) \\ &\leq M' \left\{\prod_i (k_i/\pi e v_i)^{k_i/2}\right\} \sigma, \end{aligned}$$

where $\sigma = \sum_\xi \exp\left(-\frac{1}{2}\pi\eta Tr(\xi)\right) < \infty$ and depends only on Γ. By using the expression for M',

$$\begin{aligned} 1 &\leq \sigma \prod_i \left(\frac{4}{v_i}\right)^{\frac{k_i}{2}} \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{\frac{mk_i}{2}} \times \left(n^{\sum k_i/2}\right)^{-1} \\ &\leq \sigma \prod_i \left(\frac{4}{\eta}\right)^{\frac{k_i}{2}} \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{\frac{mk_i}{2}} \times \left(n^{\sum k_i/2}\right)^{-1}. \\ \Longrightarrow \qquad n^{\sum k_i/2} &\leq \sigma \prod_i \left(\frac{4}{\eta}\right)^{\frac{k_i}{2}} \left\{\frac{mk_i}{2\pi e}\left(\frac{1}{\eta^{m-1}}\right)^{\frac{1}{m}}\right\}^{\frac{mk_i}{2}}, \end{aligned}$$

where the right hand side depends only on Γ and k, not on n nor on f. Thus there is a constant n' (depending only on Γ and k) such that $c_i(\xi) = 0$ for all i with $\xi \in \Lambda_i^+$ $N\xi \leq n' \Longrightarrow f = 0$ identically. Since $c_i(\xi)$ depends only

on ξ modulo a subgroup U of $\mathcal{O}^\times$ of finite index and $\{\xi \in \Lambda_i^+ \mid N\xi \leq n'\}/U$ is finite, there are only finitely many vanishing conditions on the Fourier coefficients of f which assure that f is identically zero. Now, elementary linear algebra consideration completes the proof. ∎

1.7 Quotient Space $X_\Gamma = \Gamma\backslash(\mathfrak{H}^m)^*$

Put $(\mathfrak{H}^m)^* = \mathfrak{H}^m \cup F \cup \{i\infty\} = \mathfrak{H}^m \cup \{\text{ cusps of } \mathrm{GL}_2^+(F)\}$. Then $(\mathfrak{H}^m)^*$ carries a unique topology with the following properties;

(a) The topology induced on $\mathfrak{H}^m$ is the usual one.

(b) $\mathfrak{H}^m$ is an open dense subset of $(\mathfrak{H}^m)^*$.

(c) If κ is a cusp and $g \in \mathrm{GL}_2^+(F)$ is such that $g\kappa = i\infty$, then the sets $g^{-1}(U_M) \cup \{\kappa\}$, $M > 0$, with $U_M = \{z \in \mathfrak{H}^m \mid N(\mathrm{Im}(z)) = \prod_{j=1}^{m} \mathrm{Im}(z_j) > M\}$ form a basis for the neighborhood of κ.

Remark 1.4 (a) The system of sets $g^{-1}(U_M) \cup \{\kappa\}$, $M > 0$ does not depend on the choice of g.

(b) Since $\mathrm{GL}_2^+(F)$ acts on the set of cusps, Γ acts on $(\mathfrak{H}^m)^*$ for any congruence subgroup Γ.

Consider now the quotient space $X_\Gamma = \Gamma\backslash(\mathfrak{H}^m)^*$, equipped with the quotient topology.

Theorem 1.6 For any congruence subgroup Γ, the quotient space X_Γ is a locally compact Hausdorff space. The canonical mapping

$$\Gamma_{i\infty}\backslash U_M \bigcup \{i\infty\} \to \Gamma\backslash(\mathfrak{H}^m)^*$$

is an open imbedding for sufficiently large $M > 0$.

This system is a neighborhood basis of the class of $i\infty$.

Remark 1.5 For any $g \in \mathrm{GL}_2^+(F)$, the transformation $z \mapsto gz$ induces a homeomorphism $X_\Gamma \tilde{\to} X_{g\Gamma g^{-1}}$. Thus we may restrict our attention to the local structure of X_Γ at the cusp $i\infty$.

Lemma 1.9 Given a compact set $K \subseteq \mathfrak{H}^m$, κ a cusp of Γ, there exists a neighborhood U of κ such that $\Gamma U \cap K = \emptyset$.

Proof. We may assume that $\kappa = i\infty$. There are constants $A, B > 0$ such that $A<N(\mathrm{Im}(z))<B$ for all $z \in K$. Since Γ is a congruence subgroup, $\{N(\det g) : g \in \Gamma\}$ is a finite set and hence

$$\sup\{N(\det g) : \ g \in \Gamma\} = \alpha > 0$$

For the same reason, there is a constant c_Γ such that

$$\inf\left\{|Nc| \ \middle| \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \ c \neq 0\right\} \geq c_\Gamma.$$

Then for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ with $c \neq 0$ and $z \in \mathfrak{H}^m$,

$$\begin{aligned} N(\mathrm{Im}(\gamma z)) &= N(\det\gamma)N(\mathrm{Im}(z))/|N(cz+d)|^2 \\ &\leq N(\det\gamma)|Nc|^{-2}N(\mathrm{Im}(z))^{-1} \\ &\leq \alpha c_\Gamma^{-1}N(\mathrm{Im}(z))^{-1}. \end{aligned}$$

Put $M = \max(\alpha B, \ \alpha c_\Gamma^{-2}/A)$. Let $z \in K$. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ with $c = 0$, then

$$N(\mathrm{Im}(\gamma z)) = N(\det\gamma)N(\mathrm{Im}(z)) \leq \alpha N(\mathrm{Im}(z)) \leq \alpha B.$$

On the other hand, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ with $c \neq 0$, then $N(\mathrm{Im}(\gamma z)) \leq \alpha c_\Gamma^{-2}A^{-1}$. Thus if $U = \{z \in \mathfrak{H}^m \mid N(\mathrm{Im}(z))>M\} \cup \{i\infty\}$, then $\Gamma U \cap K = \emptyset$. ∎

Lemma 1.10 For Γ-inequivalent cusps κ_2, κ_2 of Γ, there exist neighborhoods U_1, U_2 of κ_2, κ_2, respectively, such that $\Gamma U_1 \cap U_2 = \emptyset$.

Proof. We may assume that $\kappa_1 = i\infty$. For $\mathcal{U}$ with $[\mathcal{O}^\times : \mathcal{U}]<\infty$, there exist $c, c' > 0$ (depending only on $\mathcal{U}$) such that for every $a \in F$ there exists $\eta \in \mathcal{U}$ such that

$$c|\mathrm{Norm}_{F/\mathbb{Q}}(a)|^{\frac{1}{m}} \leq |(\eta a)^{(j)}| \leq c'|\mathrm{Norm}_{F/\mathbb{Q}}(a)|^{\frac{1}{m}}.$$

This can be proved as in Lemma 1.5 by taking independent units in $\mathcal{U}$. Since F is dense in $\mathbb{R}^m$ by the approximation theorem,the above inequality says that given $z \in \mathfrak{H}^m$ there exists $\begin{pmatrix} \varepsilon & \\ & \varepsilon^{-1} \end{pmatrix} \in Z(\mathcal{O})\Gamma$ $(\varepsilon \in \mathcal{O}^\times)$ such that

$$cN(\mathrm{Im}(z))^{\frac{1}{m}} \leq \mathrm{Im}(\varepsilon z)^{(j)} \leq c'N(\mathrm{Im}(z))^{\frac{1}{m}}, \quad \textit{for all } j.$$

Let P be a fundamental domain for $\mathbb{R}^m/\mathfrak{b}$, where $\mathfrak{b}$ is an ideal of F such that $Z(\mathcal{O})\Gamma \supseteq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \ b \in \mathfrak{b} \right\}$. Note that $\overline{P}$ is compact. Put

$$K = \{z \in \mathfrak{H}^m \mid \mathrm{Re}(z) \in \overline{P}\ ,\ N(\mathrm{Im}(z)) = 1, \text{ and } c \leq \mathrm{Im}(z^{(j)}) \leq c',\ \forall j\}.$$

Then K is compact and by Lemma 1.9, there are connected neighborhoods U_1 of $i\infty$ and U_2 of κ_2 such that $\Gamma U_1 \bigcap K = \Gamma U_2 \bigcap K = \emptyset$. Note also that $\Gamma \cdot K \supseteq \{z \in \mathfrak{H}^m \mid N(\mathrm{Im}(z)) = 1\}$, from which U_1 and U_2 are disjoint. Since $N(\mathrm{Im}(z))$ is a continuous function of z on $\mathbb{C}^m$,

$$U_1 - \{i\infty\} \subseteq \{z \in \mathfrak{H}^m \mid N(\mathrm{Im}(z)) > 1\},$$

$$U_2 - \{\kappa_2\} \subseteq \{z \in \mathfrak{H}^m \mid N(\mathrm{Im}(z)) < 1\}.$$

Assume now that $z_0 \in \gamma U_2 \bigcap U_1$ for some $\gamma \in \Gamma$. Then $N(\mathrm{Im}(z_0)) > 1$. Since γU_2 is connected, $\gamma\kappa_2 \neq i\infty$ is a cusp with $N(\mathrm{Im}(\gamma\kappa_2)) = 0$, there exists $z_1 \in \gamma U_2$ such that $N(\mathrm{Im}(z_1)) = 1$. But this implies that

$$z_1 \in \gamma U_2 \bigcap \Gamma K \Longrightarrow \Gamma U_2 \bigcap K \neq \emptyset,$$

a contradiction. Thus $\Gamma U_1 \bigcap U_2 = \emptyset$. ∎

Lemma 1.11 The space $\Gamma_{i\infty}\backslash\overline{U}_M \cup \{i\infty\}$ is compact for $M > 0$.

Proof. First we must show that $\Gamma_{i\infty}$ acts on $\overline{U}_M \cup \{i\infty\}$. Put

$$\begin{aligned} t &= \{a \in \mathbb{R}^m \mid z \mapsto z + a \text{ lies in } \Gamma\}, \\ \Lambda &= \{\varepsilon \in (\mathbb{R}_+)^m \mid z \mapsto \varepsilon z + b \text{ lies in } \Gamma \text{ for some } b \in \mathbb{R}^m\} \end{aligned}$$

Then $$\Lambda \cong \mathbb{Z}^{m-1},\ t \cong \mathbb{Z}^m.$$

Clearly, Λ acts on t by $(\varepsilon, a) \mapsto \varepsilon a = (\varepsilon_1 a_1, \cdots, \varepsilon_m a_m)$. The linear map $\mathbb{R}^m \to \mathbb{R}^m$ $(a \mapsto \varepsilon a)$ has determinant $N\varepsilon$, and the matrix of the linear map with respect to a basis of the lattice is integral. So $N\varepsilon = 1$. This implies that $\Gamma_{i\infty}$ acts on $\overline{U}_M \cup \{i\infty\}$. Secondly, we will show that $\Gamma_{i\infty}\backslash\overline{U}_M \cup \{i\infty\}$ is compact. A subset P of an n-dimensional real vector space is called a parallelotope if there exists a basis $a_1, \cdots, a_m$ with the property

$$P = \{a \mid a = \sum t_j a_j,\ 0 \le t_j \le 1,\ 1 \le j \le n\}.$$

If P is a fundamental parallelotope for t and Q that for $\log\Lambda$ in the space $\{v \in \mathbb{R}^m \mid Tr(v) = v_1 + \cdots + v_m = 0\}$, then $\Gamma_{i\infty} \cdot V = \overline{U}_M$, where

$$V = \left\{ z \in \overline{U}_M \,\middle|\, x \in P,\ \log \frac{y}{\sqrt[m]{Ny}} \in Q \right\}.$$

Let $[\sqrt[m]{c}, \infty]$ denote a compact interval in the extended real axis. Since the following map is continuous, the image contains $V \bigcup \{i\infty\}$, $\Gamma_{i\infty}\backslash\overline{U}_M \cup \{i\infty\}$ is compact. The map is $[\sqrt[m]{M}, \infty] \times P \times Q \to \overline{U}_M \cup \{i\infty\}$ given by

$$(t, x, \log y) \mapsto \begin{cases} x + ity & \text{if } t < \infty \\ i\infty & \text{if } t = \infty \end{cases}. \qquad \blacksquare$$

Proof of Theorem 1.6. As $\Gamma\backslash\mathfrak{H}^m$ is Hausdorff [See the Chapter 1 of [S1]], any two non-cusps can be separated. If κ is a cusp and $z_0 \in \mathfrak{H}^m$, then choosing a compact neighborhood K of z_0 in $\mathfrak{H}^m$ we can find a neighborhood U of κ such that $\Gamma U \bigcap K = \emptyset$ by Lemma 1.9. So κ and z_0 can be separated. Any two inequivalent cusps can be separated by Lemma 1.10. Then X_Γ is Hausdorff. X_Γ is also locally compact, since $\Gamma\backslash\mathfrak{H}^m$ is also locally compact and each class of cusps has a compact neighborhood by Lemma 1.11.

$$\Gamma_{i\infty}\backslash U_M \cup \{i\infty\} \to \Gamma\backslash(\mathfrak{H}^m)^*$$

is clearly continuous and open. For injectivity,we have to show that $\Gamma_{i\infty}\backslash U_M \to \Gamma\backslash\mathfrak{H}^m$ is injective for M sufficiently large. Namely,

$$N(\mathrm{Im}(z)) > M,\ \ N(\mathrm{Im}(\gamma z)) > M,\ \ \gamma \in \Gamma \quad \Longrightarrow \quad \gamma \in \Gamma_{i\infty},$$

which follows from the proof of Lemma 1.9. Namely, if $M = \sqrt{\alpha}/c_\Gamma, \gamma \in \Gamma \setminus \Gamma_{i\infty}, z \in \mathfrak{H}^m$ with $N(\mathrm{Im}(z)) > M$, then

$$N(\mathrm{Im}(\gamma z)) \le \alpha c_\Gamma^{-2} N(\mathrm{Im}(z))^{-1} < \alpha c_\Gamma^{-2}(c_\Gamma/\sqrt{\alpha}) = \sqrt{\alpha}/c_\Gamma \qquad i.e.,$$

$$\Gamma_{i\infty} = \{\gamma \in \Gamma \mid \gamma U_M \bigcap U_M \neq \emptyset\} \ \ with\ M = \sqrt{\alpha}/c_\Gamma. \qquad \blacksquare$$

Remark 1.6 $\Gamma\backslash(\mathfrak{H}^m)^* = X_\Gamma$ is a complex analytic space in a natural way. With an imbedding into some $\mathbb{P}^N$, it becomes a normal projective variety. To accomplish this imbedding, let $k = (k, k, \cdots, k)$, and let $\{f_0, \cdots, f_N\}$ be a basis of $\mathrm{Mfm}(\Gamma, k)$. then the map $\mathfrak{H}^m \to \mathbb{P}^N$ given by $z \mapsto (f_0(z), \cdots, f_N(z))$ is well-defined if not all f_j's are zero at any point. Further, this induces $\Gamma\backslash\mathfrak{H}^m \to \mathbb{P}^N \quad (\overline{z} \mapsto (f_0(z), \cdots, f_N(z)))$, because under Γ each $f_j(z)$ changes by the same factor.

Theorem 1.7 Given any congruence subgroup Γ, there exists B such that if $k > B$, $k \in 2\mathbb{Z}$, then $\Gamma\backslash(\mathfrak{H}^m)^* \hookrightarrow \mathbb{P}^N$ is biregular.

Proof. See [B]. ∎

Remark 1.7 If $m = 1$, then we get a compact Riemann surface *i.e.*, a non-singular variety. But for $m > 1$, any fixed points in $\mathfrak{H}^m$ (= elliptic fixed points) or any cusps, give singularities. For details, the reader is referred to [F, pp. 10-11,14-18,30-32].

1.8 Volume Computation of $\mathrm{SL}_2(\mathcal{O})\backslash\mathfrak{H}^m$.

$\mathrm{d}\mu = \prod_{j=1}^{m} \frac{dx_j \wedge dy_j}{y_j^2}$ is a $\mathrm{SL}_2(\mathbb{R})^m$-invariant measure on $\mathfrak{H}^m$, which induces a measure on $\mathrm{SL}_2(\mathcal{O})\backslash\mathfrak{H}^m$, also denoted by $\mathrm{d}\mu$.

Theorem 1.8 The volume of $\mathrm{SL}_2(\mathcal{O})\backslash\mathfrak{H}^m$ with respect to μ is

$$\int_{SL_2(\mathcal{O})\backslash\mathfrak{H}^m} d\mu = 2\pi^{-m} D^{\frac{3}{2}} \zeta_F(2),$$

where D is the absolute value of the absolute discriminant of F.

Lemma 1.12 (a) Let $\mathfrak{m}$ be a non-zero fractional ideal of F. For each ideal class of F, choose an integral ideal $\mathfrak{a}_i$ in the class, and let $\alpha_i, \beta_i \in \mathcal{O}$ be generators for $\mathfrak{a}_i$. Then $(\mathfrak{m}^2 - \{0\})/\mathrm{SL}_2(\mathcal{O})$ has irredundant representatives $(\alpha_i, \beta_i)\lambda$ where $0 \neq \lambda \in \mathfrak{m}\mathfrak{a}_i^{-1}/\mathcal{O}^\times$. Moreover, $\mathfrak{m}^2 - \{0\} = \bigcup_{i,\lambda} \lambda(\alpha_i, \beta_i)(\Gamma_i\backslash\Gamma)$, where $\Gamma = \mathrm{SL}_2(\mathcal{O})$, $\Gamma_i = \{\gamma \in \Gamma \mid (\alpha_i, \beta_i)\gamma = (\alpha_i, \beta_i)\}$, and the right hand side consists of distinct elements.

(b) There exist $p_i, q_i \in \mathfrak{a}_i^{-1}$ such that $g_i = \begin{pmatrix} p_i & q_i \\ \alpha_i & \beta_i \end{pmatrix} \in \mathrm{SL}_2(F)$.

(c) $g_i \Gamma_i g_i^{-1} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathfrak{a}_i^{-2} \right\}$.

Proof. (a). $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto a\mathcal{O} + b\mathcal{O}$ of $F^2 - \{0\}$ to fractional ideals of F gives a one-to-one correspondence between $\mathfrak{m}^2 - \{0\}/\mathrm{SL}_2(\mathcal{O})$ and the fractional ideals contained in $\mathfrak{m}$. The rest of (a) is clear from this.
(b). Since $\alpha_i\mathcal{O} + \beta_i\mathcal{O} = \mathfrak{a}_i$, $\alpha_i\mathfrak{a}_i^{-1} + \beta_i\mathfrak{a}_i^{-1} = \mathcal{O} \Longrightarrow \exists p_i, q_i \in \mathfrak{a}_i^{-1}$ such that $\beta_i p_i - \alpha_i q_i = 1$.
(c). Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_i$. Then

$$\begin{pmatrix} p_i & q_i \\ \alpha_i & \beta_i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \beta_i & -q_i \\ -\alpha_i & p_i \end{pmatrix}$$
$$= \begin{pmatrix} p_i a + q_i c & p_i b + q_i d \\ \alpha_i & \beta_i \end{pmatrix} \begin{pmatrix} \beta_i & -q_i \\ -\alpha_i & p_i \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix},$$

where $u \in \mathfrak{a}_i^{-2}$, and one notes that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_i \Longrightarrow (\alpha_i, \beta_i) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (\alpha_i, \beta_i)$$

and hence the $(1,1)$-enrty is

$$(p_i, q_i) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \beta_i \\ -\alpha_i \end{pmatrix} = (p_i, q_i) \begin{pmatrix} \beta_i \\ -\alpha_i \end{pmatrix} = 1.$$

On the other hand,

$$\gamma = \begin{pmatrix} \beta_i & -q_i \\ -\alpha_i & p_i \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p_i & q_i \\ \alpha_i & \beta_i \end{pmatrix} = \begin{pmatrix} 1 + \alpha_i\beta_i u & \beta_i^2 u \\ -\alpha_i^2 u & 1 - \alpha_i\beta_i u \end{pmatrix} \in \Gamma.$$

And

$$\begin{pmatrix} p_i & q_i \\ \alpha_i & \beta_i \end{pmatrix} \gamma = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p_i & q_i \\ \alpha_i & \beta_i \end{pmatrix} \Longrightarrow (\alpha_i, \beta_i)\gamma = (\alpha_i, \beta_i) \Rightarrow \gamma \in \Gamma_i. \quad \blacksquare$$

Proof of Theorem 1.8. Let φ be an $SO(2)^m$ -invariant Schwartz function on $(\mathbb{R}^2)^m$. For each $z \in \mathfrak{H}^m$, choose $g_z \in SL_2(\mathbb{R})^m$ so that $g_z(i) = z$. Here g_z is determined right-modulo $SO(2)^m$. Let $\mathfrak{m}$ be a nonzreo fractional ideal of F. Define

$$(*) \qquad Z(\varphi;\mathfrak{m}) = \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{0\neq\xi\in\mathfrak{m}} \varphi(\xi g_z) d\mu(z).$$

We will make use of all the items in Lemma 1.12. In addition, we will put $(\alpha_0, \beta_0) = (0, 1)$ for a particular index. On the other hand,

$$\begin{aligned} Z(\varphi;\mathfrak{m}) &= 2\sum_i \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\lambda\in\mathfrak{m}\mathfrak{a}_i^{-1}/\mathcal{O}^\times} \varphi((0,\lambda)g_i g_z) d\mu(z) \\ &= 2\sum_i \int_{g_i\Gamma_i g_i^{-1}\backslash\mathfrak{H}^m} \sum_{\lambda} \varphi((0,\lambda)g_z) d\mu(z), \end{aligned}$$

by replacing z by $g_i^{-1}(z)$. (Here a factor of 2 occurs, since $\pm 1_2$ acts trivially on $\mathfrak{H}^m$, and $-1_2 \notin \Gamma_i$.) By taking $g_z = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & 0 \\ 0 & y^{-\frac{1}{2}} \end{pmatrix}$,

$$Z(\varphi;\mathfrak{m}) = 2\sum_i \mathrm{vol}(\mathbb{R}^m/\mathfrak{a}_i^{-2}) \times \sum_{\lambda\in\mathfrak{m}\mathfrak{a}_i^{-1}/\mathcal{O}^\times} \int Ny^{-1}\varphi(0,\lambda y^{-\frac{1}{2}}) dy/Ny,$$

where the integral is over $(0,\infty)^m$, and $Ny = y_1 \cdots y_m$.
By changing variables, $y \to \lambda^2 y$,

$$Z(\varphi;\mathfrak{m}) = 2\sum_i \mathrm{vol}(\mathbb{R}^m/\mathfrak{a}_i^{-2}) \times \sum_{\lambda\in\mathfrak{m}\mathfrak{a}_i^{-1}/\mathcal{O}^\times} N\lambda^{-2} \int Ny^{-1}\varphi(0,y^{-\frac{1}{2}}) dy/Ny.$$

(Here we use the fact that $SO(2)^m$-invariance of φ implies

$$\varphi(\cdots, \pm x_i, \cdots) = \varphi(\cdots, x_i, \cdots).)$$

Since $\mathrm{vol}(\mathbb{R}^m/\mathfrak{a}_i^{-2}) = D^{\frac{1}{2}} N\mathfrak{a}_i^{-2}$,

$$\begin{aligned} &\sum_i \mathrm{vol}(\mathbb{R}^m/\mathfrak{a}_i^{-2}) \times \sum_* N\lambda^{-2} \\ &= D^{\frac{1}{2}} \sum_i \sum_{**} N\mathfrak{a}^{-2} = D^{\frac{1}{2}} \sum_{0\neq\mathfrak{a}\subseteq\mathfrak{m}} N\mathfrak{a}^{-2} = D^{\frac{1}{2}} N\mathfrak{m}^{-2}\zeta_F(2), \end{aligned}$$

where $\sum_{*}$ is taken over all nonzero $\lambda \in \mathfrak{m}\mathfrak{a}_i^{-1}/\mathcal{O}^\times$ and $\sum_{**}$ is taken over all nonzero $\mathfrak{a} \subseteq \mathfrak{m}$, $\mathfrak{a} \sim \mathfrak{a}_i$. Thus

$$Z(\varphi;\mathfrak{m}) = 2D^{\frac{1}{2}} N\mathfrak{m}^{-2}\zeta_F(2) \int Ny\varphi(0,y^{\frac{1}{2}})dy/Ny.$$

On the other hand, by the Poisson summation formula,

$$\begin{aligned} & Z(\varphi;\mathfrak{m}) \\ = & \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\xi\in\mathfrak{m}^2} \varphi(\xi g_z)d\mu(z) - \varphi(0)\int_{\Gamma\backslash\mathfrak{H}^m} d\mu(z) \\ = & \ \mathrm{vol}(\mathbb{R}^{2m}/\mathfrak{m}^2)^{-1} \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\xi\in(\mathfrak{m}^*)^2} \widehat{\varphi}(\xi g_z^{-t})d\mu(z) - \varphi(0)\int_{\Gamma\backslash\mathfrak{H}^m} d\mu(z) \\ = & \ \mathrm{vol}(\mathbb{R}^{2m}/\mathfrak{m}^2)^{-1} \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{0\neq\xi\in(\mathfrak{m}^*)^2} \widehat{\varphi}(\xi g_z^{-t})d\mu(z) \\ & +[\mathrm{vol}(\mathbb{R}^m/\mathfrak{m}^2)^{-1}\widehat{\varphi}(0) - \varphi(0)]\int_{\Gamma\backslash\mathfrak{H}^m} d\mu(z), \end{aligned}$$

where $\mathfrak{m}^* = \{\alpha \in F \mid \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\mathfrak{m}) \subseteq \mathbb{Z}\}$.

Note that for $g_z = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}} \end{pmatrix}$, $g_z^{-t}(i) = -z^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z$.

Replacing z by $-z^{-1}$ *i.e.*, replacing z by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} z$,

$$\begin{aligned} Z(\varphi;\mathfrak{m}) \ = \ & \mathrm{vol}(\mathbb{R}^{2m}/\mathfrak{m}^2)^{-1} Z(\widehat{\varphi};\mathfrak{m}^*) \\ & +[\mathrm{vol}(\mathbb{R}^{2m}/\mathfrak{m}^2)^{-1}\widehat{\varphi}(0) - \varphi(0)]\int_{\Gamma\backslash\mathfrak{H}^m} d\mu(z). \end{aligned}$$

By taking $\mathfrak{m} = \mathcal{O}$ and combining these two calculations

$$\begin{aligned} & 2D^{\frac{1}{2}}\zeta_F(2)\int_{(0,\infty)^m} Ny\varphi(0,y^{\frac{1}{2}})dy/Ny \\ = \ & 2D^{\frac{3}{2}}\zeta_F(2)\int_{(0,\infty)^m} Ny\widehat{\varphi}(0,y^{\frac{1}{2}})dy/Ny + [D^{-1}\widehat{\varphi}(0) - \varphi(0)]\mathrm{vol}(\Gamma\backslash\mathfrak{H}^m). \end{aligned}$$

Now, we have to take an $\mathrm{SO}(2)^m$-invariant Schwartz function φ on $\mathbb{R}^{2m}$, with $D^{-1}\widehat{\varphi}(0) \neq \varphi(0)$, with $t > 0$, $t \neq D^{-\frac{1}{m}}$, put $\varphi(x) = \exp(-\pi t\|x\|^2)$. Then $\widehat{\varphi}(x) = t^{-m}\varphi(t^{-1}x)$, and the above equality is

$$2D^{\frac{1}{2}}\zeta_F(2)(\pi t)^{-m} = 2D^{\frac{3}{2}}\zeta_F(2)\pi^{-m} + [D^{-1}t^{-m} - 1]\mathrm{vol}(\Gamma\backslash\mathfrak{H}^m).$$

This implies that $\mathrm{vol}(\Gamma\backslash\mathfrak{H}^m) = 2D^{\frac{3}{2}}\pi^{-m}\zeta_F(2)$. ∎

1.9 Eisenstein Series.

Definition 1.7 Let $\mathfrak{m}$ be a nonzero fractional ideal of F, and $1<k \in \mathbb{Z}$. The inhomogeneous holomorphic Eisenstein series of weight $2k = (2k, \cdots, 2k)$, attached to $\mathfrak{m}$, is defined to be

$$\begin{aligned} E(z;\mathfrak{m},2k) &= \overset{*}{\sum}(cz+d)^{-2k} \quad \text{(a multi-index notation)} \\ &= \overset{*}{\sum} N(cz+d)^{-2k}, \end{aligned}$$

where $\sum^*$ is taken over $(c,d) \in \{(\alpha,\beta) \in \mathfrak{m}^2 \mid \alpha\mathcal{O}+\beta\mathcal{O} = \mathfrak{m}\}/\mathcal{O}^\times$. The homogeneous holomorphic Eisenstein series of weight $2k = (2k, \cdots, 2k)$, attached to $\mathfrak{m}$, is defined to be

$$E^*(z;\mathfrak{m},2k) = \overset{**}{\sum}(cz+d)^{-2k} = \overset{**}{\sum} N(cz+d)^{-2k},$$

where $\sum^{**}$ is taken over $(c,d) \in \mathfrak{m}^2 - \{0\}/\mathcal{O}^\times$.

Proposition 1.2 $E(z;\mathfrak{m},2k)$ and $E^*(z;\mathfrak{m},2k)$ are holomorphic on $\mathfrak{H}^m$ for $2k > 2$, and are Hilbert modular forms of weight $2k$ for any congruence subgroup Γ with $\mathrm{GL}_2^+(\mathcal{O}) \supset \Gamma \supset SL_2(\mathcal{O})$.

Proof. Since the defining series for E is a subseries of that for E^*, it will suffice to consider E^* only. Consider $\sum^{**}|cz+d|^{-r}$ for $0<r \in \mathbb{R}$. Take a compact subset $K \subseteq \mathfrak{H}^m$. Then there exists $M > 0$ such that for all $z \in K$ and j, $|c_j z_j + d_j| \geq M(c_j^2+d_j^2)^{\frac{1}{2}}$, and hence $|cz+d|^{-r} \leq M^{-rm}N(c^2+d^2)^{-r/2}$. Let $L = F(i)$. Then

$$\sum{}^*|cz+d|^{-r} \leq M^{-rm}\sum{}^* N_{L/\mathbb{Q}}(ci+d)^{-r/2}.$$

Claim: The convergence of the latter sum is equivalent to that of $\sum_{\substack{\mathfrak{a}\ integral \\ ideal\ of L}} N\mathfrak{a}^{-r/2}$. Since the class number of L is finite, the convergence of $\sum_{\mathfrak{a}\ integral} N\mathfrak{a}^{-r/2}$ is equivalent to that of $\sum_{\substack{\mathfrak{a}\ principal \\ integral}} N\mathfrak{a}^{-r/2}$. Since $[\mathcal{O}_L^\times:\mathcal{O}_F^\times]<\infty$ by the Dirichlet unit theorem, we get the desired equivalence. Since $\zeta_L(r/2)$ is absolutely convergent precisely for $r > 2$, $\sum^*(cz+d)^{-r}$ is absolutely convergent for $r > 2$, and hence

it, being a uniformly convergent sum of holomorphic functions on compacta, is holomorphic. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathcal{O})$. Note that

$$\mu(\gamma, z)^{2k} = \prod_j \mu(\gamma_j, z_j)^{2k} = N(\det \gamma)^{-k}(cz+d)^{2k} = (cz+d)^{2k}.$$

Now,

$$\begin{aligned} E^*(\gamma z; \mathfrak{m}, 2k)\mu(\gamma, z)^{-2k} &= \sum_{p,q}^{**} \left(p\frac{az+b}{cz+d} + q\right)^{-2k} (cz+d)^{-2k} \\ &= \sum^{**}[(pa+qc)z + (pb+qd)]^{-2k} \\ &= \sum^{**}(pz+q)^{-2k} \end{aligned}$$

If $[F{:}\mathbb{Q}] > 1$, by Koecher's principle it is a Hilbert modular form. The case $F = \mathbb{Q}$ is classical. ∎

Proposition 1.3 For a congruence subgroup Γ with

$$\mathrm{GL}_2^+(\mathcal{O}) \supset \Gamma \supset \mathrm{SL}_2(\mathcal{O}), \quad 2k > 2,$$

define $\mathrm{Eis}(\Gamma, 2k)$ to be the subspace of $Mfm(\Gamma, 2k)$ spanned by all of the above Eisenstein series. Let $\{\mathfrak{m}_i \mid i = 1, \cdots, h_F\}$ be any set of representatives for the ideal classes of F. Then both

$$\{E(z; \mathfrak{m}_i, 2k) \mid i = 1, \cdots, h_F\} \quad \text{and} \quad \{E^*(z; \mathfrak{m}_i, 2k) \mid i = 1, \cdots, h_F\}$$

are basis for $\mathrm{Eis}(\Gamma, 2k)$.

Lemma 1.13 Let $w_1, \cdots, w_h$ be the ideal class characters of F. Put

$$\widetilde{E} = \begin{pmatrix} N\mathfrak{m}_1^{2k} E(\mathfrak{m}_1) \\ \vdots \\ N\mathfrak{m}_h^{2k} E(\mathfrak{m}_h) \end{pmatrix}, \qquad \widetilde{E}^* = \begin{pmatrix} N\mathfrak{m}_1^{2k} E^*(\mathfrak{m}_1) \\ \vdots \\ N\mathfrak{m}_h^{2k} E^*(\mathfrak{m}_h) \end{pmatrix},$$

$\Lambda(2k) = \mathrm{diag}[L(2k, w_1), \cdots, L(2k, w_h)]$, and $\Omega = \left(\frac{1}{\sqrt{h}} w_j(\mathfrak{m}_i)\right)$. Then we have the following fundamental relations;

$$\widetilde{E}^* = \Omega\Lambda(2k)\Omega^{-1}\widetilde{E}, \quad \Omega\overline{\Omega}^t = I.$$

Proof. For any non-zero fractional ideal $\mathfrak{a}$,

$$\begin{aligned} E^*(\mathfrak{a}) &= \sum_{\mathfrak{m}\subseteq\mathfrak{a}} E(\mathfrak{m}) = \sum_i \sum_{\substack{\mathfrak{m}\subseteq\mathfrak{a}\\ \mathfrak{m}\sim\mathfrak{m}_i}} E(\mathfrak{m}) \\ &= \sum_i \sum_{\substack{\alpha\in\mathfrak{a}\mathfrak{m}_i^{-1}/\mathcal{O}^\times\\ \alpha\neq 0}} E(\alpha\mathfrak{m}_i) = \sum_i \sum_\alpha N\alpha^{-2k} E(\mathfrak{m}_i) \\ &= \sum_i E(\mathfrak{m}_i)\zeta(2k;\mathfrak{a}\mathfrak{m}_i^{-1}), \end{aligned}$$

where $\zeta(\ ;\mathfrak{n})$ is the partial zeta function $\zeta(s;\mathfrak{n}) = \sum_{\substack{\alpha\in\mathfrak{n}/\mathcal{O}^\times\\ \alpha\neq 0}} |N(\alpha)|^{-s}$.

If $L(s,w) = \sum_{\mathfrak{m}\subseteq\mathcal{O}} w(\mathfrak{m})N\mathfrak{m}^{-s}$, then we see that

$$\zeta(s;\mathfrak{n}) = h^{-1}\sum_w w(\mathfrak{n})N\mathfrak{n}^{-s}L(s,w).$$

Thus

$$N\mathfrak{a}^{2k}E^*(\mathfrak{a}) = h^{-1}\sum_{i,w} w(\mathfrak{a}\mathfrak{m}_i^{-1})L(2k,w)N\mathfrak{m}_i^{2k}E(\mathfrak{m}_i)$$

$$\Longrightarrow \quad N\mathfrak{m}_l^{2k}E^*(\mathfrak{m}_l) = h^{-1}\sum_{i,j} w_j(\mathfrak{m}_l\mathfrak{m}_i^{-1})L(2k,w_j)N\mathfrak{m}_i^{2k}E(\mathfrak{m}_i)$$

This implies that $\widetilde{E}^* = \Omega\Lambda(2k)\Omega^{-1}\widetilde{E}$ and $\Omega\overline{\Omega}^t = I$. ∎

Lemma 1.14 For $\delta = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2^+(F)$, let

$$(E|_{2k}\delta)(z) = \sum_\xi c_\xi \exp(2\pi i \mathrm{Tr}(\xi z)).$$

Then $c_0 = 0$ if $\mathfrak{m}$ is not in the same ideal class as $p\mathcal{O} + r\mathcal{O}$, and $c_0 \neq 0$ otherwise, where $E = E(\ ;\mathfrak{m},2k)$.

Proof. Clearly, for $z = (i\lambda,\cdots,i\lambda)$ with $\lambda > 0$, $\lim_{\lambda\to\infty}(E|_{2k}\delta)(z) = c_0$. Because $c_\xi = 0$ unless $\xi = 0$ or $\xi \gg 0$. Now,

$$\begin{aligned} (E|_{2k}\delta)(z) &= \sum_{c,d}{}^{*} N(c(pz+q)(rz+s)^{-1}+d)^{-2k}(rz+s)^{-2k} \times N(\det\delta)^k \\ &= N(\det\delta)^k \sum N(c(pz+q)+d(rz+s))^{-2k} \\ &= N(\det\delta)^k \sum N((cp+dr)z+(cq+ds))^{-2k}. \end{aligned}$$

Now,

$$\lim_{\lambda\to\infty} N((cp+dr)i\lambda+(cq+ds))^{-2k} = \begin{cases} 0 & \text{, if } cp+dr\neq 0, \\ N(cq+ds)^{-2k}>0 & \text{, if } cp+dr=0. \end{cases}$$

By direct calculation and the Theorem 1.3, $cp+dr=0 \iff c\mathcal{O}+d\mathcal{O}=\mathfrak{m}$ and $p\mathcal{O}+r\mathcal{O}$ are in the same ideal class. ∎

Proof of Proposition 1.3. For $\alpha\in F^\times$,

$$E(\alpha\mathfrak{a}) = N\alpha^{-2k}E(\mathfrak{a}),\quad E^*(\alpha\mathfrak{a}) = N\alpha^{-2k}E^*(\mathfrak{a}),$$

so that $\{E(\mathfrak{m}_i)\}$ and $\{E^*(\mathfrak{m}_i)\}$ respectively span the space spanned by

$$\{E(\mathfrak{n}) \mid \mathfrak{n} \text{ is a nonzero fractional ideal of } F\}$$

and that spanned by

$$\{E^*(\mathfrak{n}) \mid \mathfrak{n} \text{ is a nonzero fractional ideal of } F\}.$$

Since $k>1$, the matrices appearing in the fundamental relation of Lemma 1.13 are nonsingular, and hence $\{E(\mathfrak{m}_i)\}$ and $\{E^*(\mathfrak{m}_i)\}$ generate the same space. It only remains to see that $\{E(\mathfrak{m}_i)\}$ is linearly independent. Each $g\in \mathrm{GL}_2^+(F)$ gives rise to the linear functional on $\mathrm{Mfm}(\Gamma,2k)$, given by $L_g f=$ the 0-th Fourier coefficient of $f|_{2k}g$. Let $\mathfrak{m}_i = p_i\mathcal{O}+r_i\mathcal{O}$, and choose $q_i, s_i\in F$ so that $\delta_i = \begin{pmatrix} p_i & q_i \\ r_i & s_i \end{pmatrix} \in \mathrm{GL}_2^+(F)$. Then

$$\begin{aligned} &\sum_{i=1}^{h}\alpha_i E(\mathfrak{m}_i)=0 \\ \Longrightarrow\quad & L_{\delta_j}\Big(\sum_{i=1}^{h}\alpha_i E(\mathfrak{m}_i)\Big) = \sum_{i=1}^{h}\alpha_i L_{\delta_j}(E(\mathfrak{m}_i)) = \alpha_j L_{\delta_j}(E(\mathfrak{m}_j)) = 0 \\ \Longrightarrow\quad & \alpha_j = 0, \end{aligned}$$

by Lemma 1.14. ∎

(Corollary of Lemmas). For a congruence subgroup Γ with $GL_2^+(\mathcal{O})\supset\Gamma\supset \mathrm{SL}_2(\mathcal{O})$, $f\in\mathrm{Mfm}(\Gamma,2k)$, there exists an $E\in\mathrm{Eis}(\Gamma,2k)$ such that $f-E\in \mathrm{Cfm}(\Gamma,2k)$.

Proof. By the Theorem 1.3 and its corollary, there are δ_j $(j = 1, \cdots, h_F)$ of $\mathrm{GL}_2^+(F)$ such that $\{\delta_j(i\infty)\}$ is the set of Γ-inequivalent cusps. If $\delta_j = \begin{pmatrix} p_j & q_j \\ r_j & s_j \end{pmatrix}$, then $\begin{pmatrix} p_j \\ q_j \end{pmatrix} \in (\mathbb{P}^1)^m$ is $\delta_j(i\infty)$ and $\{\mathfrak{m}_j = p_j\mathcal{O} + q_j\mathcal{O}\}$ is a collection of representatives for the ideal classes. Moreover, $f \in \mathrm{Cfm}(\Gamma, 2k) \iff L_{\delta_j} f =$ 0-th Fourier coefficient of $f|_{2k}\delta_j$ is zero for all j. Put

$$E_i = E(\ ; \mathfrak{m}_i, 2k), \quad E = \sum_i L_{\delta_i} f (L_{\delta_i} E_i)^{-1} E_i.$$

Then for all j, $L_{\delta_j}(f - E) = L_{\delta_j} f - L_{\delta_j} f = 0$ *i.e.*, $f - E \in \mathrm{Cfm}(\Gamma, 2k)$. ∎

Proposition 1.4 ***(The Fourier expansion at Infinity)***

$$E^*(z; \mathfrak{m}, 2k) = \sum_{\alpha \in \mathfrak{m} - \{0\}/\mathcal{O}^\times} N\alpha^{-2k} + D^{\frac{1}{2}} N\mathfrak{m}^{-1} [(-2\pi i)^{2k}/\Gamma(2k)]^m \times \sum_{0 \ll \xi \in \mathcal{O}^*} \sigma_{2k-1}(\xi; \mathfrak{m}) \exp(2\pi i Tr(\xi z)),$$

where D is the absolute discriminant of F, and

$$\sigma_{2k-1}(\xi; \mathfrak{m}) = \sum_{\substack{\delta \in \mathfrak{m}^*/\mathcal{O}^\times \\ \xi/\delta \in \mathfrak{m}}} |N_{F/\mathbb{Q}}\delta|^{2k-1}.$$

Lemma 1.15 For $\mathrm{Re}(s) > 0$, $Im(z) > 0$, $z = x + iy$,

$$(*) \quad \int_{\mathbb{R}} z^{-s} \exp(-2\pi i t x) dx = \begin{cases} [(-2\pi i)^s/\Gamma(s)] t^{s-1} \exp(-2\pi t y) & , t > 0 \\ 0 & , t \leq 0 \end{cases}$$

Proof. By Fourier inversion formula, it is enough to see that

$$\int_{\mathbb{R}} f(t) \exp(2\pi i t x) dt = (x + iy)^{-s},$$

where $f(t)$ is as in $(*)$.

$$\begin{aligned} \int_{\mathbb{R}} f(t) \exp(2\pi i t x) dt &= [(-2\pi i)^s/\Gamma(s)] \int_0^\infty t^{s-1} \exp(2\pi i t z) dt \\ &= [(-2\pi i)^s/\Gamma(s)][(-2\pi i)z]^{-s} \Gamma(s) = z^{-s}. \end{aligned}$$ ∎

Proof of Proposition 1.4.

$$E^*(z;\mathfrak{m},2k) = \sum^{**} N(cz+d)^{-2k} = \sum_{c=0} N(cz+d)^{-2k} + \sum_{c\neq 0} N(cz+d)^{-2k}$$
$$= \sum_{\alpha\in\mathfrak{m}-\{0\}/\mathcal{O}^\times} N\alpha^{-2k} + \sum_{c\in\mathfrak{m}-\{0\}/\mathcal{O}^\times} Nc^{-2k}\Big\{\sum_{d\in\mathfrak{m}} N\Big(z+\frac{d}{c}\Big)^{-2k}\Big\}.$$

Since $E^*(z;\mathfrak{m},2k)$ is a modular form of weight $2k$ for $\mathrm{GL}_2^+(\mathcal{O})$, its Fourier coefficients can be indexed by $\mathcal{O}^*$. For $\xi\in\mathcal{O}^*$, the ξ-th Fourier coefficient of $\Big\{\sum_{d\in\mathfrak{m}} N\Big(z+\frac{d}{c}\Big)^{-2k}\Big\}$ is

$$D^{-\frac{1}{2}}\int_{\mathbb{R}^m/\mathcal{O}} \exp(-2\pi i\mathrm{Tr}(\xi x))\Big\{\sum_{d\in\mathfrak{m}} N\Big(z+\frac{d}{c}\Big)^{-2k}\Big\}dx$$
$$= D^{-\frac{1}{2}}\int_{\mathbb{R}^m} \exp(-2\pi i\mathrm{Tr}(\xi x))\Big\{\sum_{d\in\mathfrak{m}/c\mathcal{O}} N\Big(z+\frac{d}{c}\Big)^{-2k}\Big\}dx$$
$$= D^{-\frac{1}{2}}\sum_{d\in\mathfrak{m}/c\mathcal{O}} \exp\Big(2\pi i\mathrm{Tr}\Big(\xi\frac{d}{c}\Big)\Big)\int_{\mathbb{R}^m} \exp(-2\pi i\mathrm{Tr}(\xi x))N(z)^{-2k}dx,$$

where by Lemma 1.15, the integral is

$$\begin{cases} [(-2\pi i)^{2k}/\Gamma(2k)]^m N\xi^{2k-1}\exp(-2\pi Tr(\xi y)) & ,\ \xi\gg 0 \\ 0 & ,\ \text{otherwise.}\end{cases}$$

Moreover, the sum is $\begin{cases} 0 & ,\ \xi/c\notin\mathfrak{m}^*=\mathfrak{m}^{-1}\mathcal{O}^* \\ |Nc|N\mathfrak{m}^{-1} & ,\ \xi/c\in\mathfrak{m}^*.\end{cases}$
For $\xi\in\mathcal{O}^*$ totally positive, the ξ-th Fourier coefficient is

$$D^{-\frac{1}{2}}N\mathfrak{m}^{-1}[(-2\pi i)^{-2k}/\Gamma(2k)]^m N\xi^{2k-1}\exp(-2\pi Tr(\xi y))\sum_{\substack{0\neq c\in\mathfrak{m}/\mathcal{O}^\times \\ \xi\in c\mathfrak{m}^*}} |Nc|^{1-2k}$$
$$= D^{-\frac{1}{2}}N\mathfrak{m}^{-1}[(-2\pi i)^{-2k}/\Gamma(2k)]^m\exp(-2\pi Tr(\xi y))\sum_{\substack{\xi/c\in\mathfrak{m}^*/\mathcal{O}^\times \\ \xi/(\xi/c)\in\mathfrak{m}}}\Big|N\Big(\frac{\xi}{c}\Big)\Big|^{2k-1}$$
$$= D^{-\frac{1}{2}}N\mathfrak{m}^{-1}[(-2\pi i)^{-2k}/\Gamma(2k)]^m\exp(-2\pi Tr(\xi y))\sum_{\substack{0\neq\delta\in\mathfrak{m}^*/\mathcal{O}^\times \\ \xi\in\delta\mathfrak{m}}}|N\delta|^{2k-1}$$
$$= D^{-\frac{1}{2}}N\mathfrak{m}^{-1}[(-2\pi i)^{-2k}/\Gamma(2k)]^m\exp(-2\pi Tr(\xi y))\sigma_{2k-1}(\xi;\mathfrak{m}).$$

Therefore,

$$E^*(z;\mathfrak{m},2k) = \zeta(2k;\mathfrak{m}) + D^{-\frac{1}{2}}N\mathfrak{m}^{-1}[(-2\pi i)^{-2k}/\Gamma(2k)]^m \times \sum_{0\ll\xi\in\mathcal{O}^*} \sigma_{2k-1}(\xi;\mathfrak{m})\exp(2\pi i Tr(\xi z)). \quad \blacksquare$$

We generalize the previous considerations to any congruence subgroup Γ.

Definition 1.8 Let Γ be a congruence subgroup, $2<k\in\mathbb{Z}$.
For $\alpha\in \mathrm{GL}_2^+(F)$, define an Eisenstein series of weight $(k,\cdots,k)$ by

$$E_\alpha(z) = \sum_{\gamma\in(\alpha P\alpha^{-1}\cap\Gamma)\backslash\Gamma} \mu(\alpha^{-1}\gamma,z)^{-k}.$$

Remark 1.8 (a) E_α is well defined, if it is convergent. As we saw in the proof of Lemma 1.11, for any congruence subgroup Γ', $N\left(\frac{a}{d}\right)=1$, if $\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}\in\Gamma'$. If $\delta\in\alpha P\alpha^{-1}\bigcap\Gamma$, then $\begin{pmatrix} a & b\\ 0 & d\end{pmatrix} = \alpha^{-1}\delta\alpha \in P\bigcap\alpha^{-1}\Gamma\alpha$ and

$$\begin{aligned}\mu(\alpha^{-1}\delta\gamma,z)^{-k} &= \mu(\alpha^{-1}\delta\alpha,\alpha^{-1}\gamma z)^{-k}\mu(\alpha^{-1}\gamma,z)^{-k}\\ &= N\left(\frac{a}{d}\right)^{\frac{k}{2}}\mu(\alpha^{-1}\gamma,z)^{-k} = \mu(\alpha^{-1}\gamma,z)^{-k}.\end{aligned}$$

(b) E_α is absolutely convergent for $k>2$.

(c) $E_\alpha\in \mathrm{Mfm}(\Gamma,k)$. It is so by Koecher's principle for $m>1$, and the case $m=1$ is classical.

Proposition 1.5 For $\delta\in \mathrm{GL}_2^+(F)$, let $(E_\alpha|_k\delta)(z) = \sum_\xi c_\xi \exp(2\pi i Tr(\xi z))$. Then $c_0=0$ if $\Gamma\alpha P\neq\Gamma\delta P$ and $c_0\neq 0$ otherwise. If $\Gamma\alpha P=\Gamma\beta P$, then $E_\alpha = cE_\beta$ for some $c>0$. In particular, none of these Eisenstein series are identically zero.

Corollary 1.4 There exist cusp forms which are not identically zero.

Proof of Proposition 1.5. Note that

$$(E_\alpha|_k\delta)(z) = \sum_\gamma \mu(\alpha^{-1}\gamma,\delta z)^{-k}\mu(\delta,z)^{-k} = \sum_\gamma \mu(\alpha^{-1}\gamma\delta,z)^{-k}.$$

For $z = (i\lambda, \cdots, i\lambda)$, $\lambda > 0$, $\lim_{\lambda\to\infty}(E_\alpha|_k)(z) = c_0$, since $c_\xi = 0$ unless $\xi = 0$ or ξ is totally positive. For $\gamma \in \mathrm{GL}_2^+(F)$, $\lim_{\lambda\to\infty}\mu(\gamma, z)^{-k} = 0 \iff \gamma \notin P$. Thus $c_0 = 0$ if $\alpha^{-1}\gamma\delta \notin P$ for all γ *i.e.*, $\delta \notin \Gamma\alpha P$. On the other hand, if $\delta \in \gamma_1^{-1}\alpha P$ and $\delta \in \gamma_2^{-1}\alpha P$ for $\gamma_1, \gamma_2 \in \Gamma$, then for some $p \in P$, $\gamma_1^{-1}\alpha p = \gamma_2^{-1}\alpha$ *i.e.*, $\gamma_1\gamma_2^{-1} \in \Gamma\bigcap\alpha P\alpha^{-1}$ *i.e.*, $(\Gamma\bigcap\alpha P\alpha^{-1})\gamma_1 = (\Gamma\bigcap\alpha P\alpha^{-1})\gamma_2$. This means that if $\Gamma\delta P = \Gamma\alpha P$ then there is precisely one term of $(E_\alpha|_k\delta)(z)$ which does not vanish as $\lambda \to \infty$. Thus $c_0 \neq 0$ in this case. Assume that $\Gamma\alpha P = \Gamma\beta P$. Then there exist $\delta \in \Gamma$, $p \in P$ such that $\delta\alpha p = \beta$. Then

$$\begin{aligned} E_\beta(z) &= \sum_{\gamma\in(\beta P\beta^{-1}\bigcap\Gamma)\backslash\Gamma} \mu(\beta^{-1}\gamma, z)^{-k} = \sum \mu(p^{-1}\alpha^{-1}\delta^{-1}\gamma, z)^{-k} \\ &= N\Big(\frac{a}{d}\Big)^{\frac{k}{2}} \sum \mu(\alpha^{-1}\delta^{-1}\gamma, z)^{-k} = N\Big(\frac{a}{d}\Big)^{\frac{k}{2}} E_\alpha(z), \end{aligned}$$

since $(\beta P\beta^{-1}\bigcap\Gamma)a \mapsto (\alpha P\alpha^{-1}\bigcap\Gamma)\delta^{-1}a$ gives a one-to-one correspondence between $(\beta P\beta^{-1}\bigcap\Gamma)\backslash\Gamma = (\delta\alpha P\alpha^{-1}\delta^{-1}\bigcap\Gamma)\backslash\Gamma$ and $(\alpha P\alpha^{-1}\bigcap\Gamma)\backslash\Gamma$. ∎

Proof of Corollary 1.4. If $\Gamma = \Gamma(\mathfrak{n})$ with a proper ideal $\mathfrak{n}$ of $\mathcal{O}$, then 0 and $i\infty$ are inequivalent cusps. Let E_α and E_β be two Eisenstein series of weight $(4, \cdots, 4)$ for Γ, associated with distinct double cosets $\Gamma\alpha P$, $\Gamma\beta P$. Then $f = E_\alpha E_\beta$ is a cuspform for Γ of weight $(8, \cdots, 8)$. ∎

Theorem 1.9 Let Γ be a congruence subgroup, and $2<k \in \mathbb{Z}$. For any choice of representatives $\{g_i\}$ for $\Gamma\backslash\mathrm{GL}_2^+(F)/P$,

$$E_i(z) = \sum_{\gamma\in(g_iPg_i^{-1}\bigcap\Gamma)\backslash\Gamma} \mu(g_i^{-1}\gamma, z)^{-k}$$

form a basis of Eis(Γ, k)=the space spanned over $\mathbb{C}$ by all E_α.

$$\mathrm{Mfm}(\Gamma, k) = \mathrm{Eis}(\Gamma, k) \oplus \mathrm{Cfm}(\Gamma, k).$$

1.10 Petersson Inner Product.

Definition 1.9 Let $k \in \mathbb{Z}^m$, Γ a congruence subgroup.
For $f_1, f_2 \in \mathrm{Mfm}(\Gamma, k)$, define

$$<f_1, f_2> = \int_{\Gamma\backslash\mathfrak{H}^m} f_1(z)\overline{f_2(z)}y^k y^{-2}dxdy.$$

Proposition 1.6 If at least one of f_1 and f_2 is a cuspform, then the integral defining $<f_1, f_2>$ is absolutely convergent. With this inner product $\mathrm{Cfm}(\Gamma, k)$ is a finite dimensional Hilbert space.

Proof. It is easy to see that $f_1(z)\overline{f_2(z)}\mathrm{Im}(z)^k$ is Γ-invariant as a function of $z \in \mathfrak{H}^m$. Let S be a standard Siegel set and $\{\delta_i\}$ a finite set of elements of $\mathrm{GL}_2^+(F)$, so that $\mathfrak{H}^m = \Gamma\Big(\bigcup_i \delta_i S\Big)$. Put $\varphi(z) = \sum_i \sum_{\gamma\in\Gamma} \psi(\delta_i^{-1}\gamma z)$ for $z \in \mathfrak{H}^m$, with the characteristic function ψ of S. Then $\varphi \geq 1$ on all of $\mathfrak{H}^m$. The integral for $<f_1, f_2>$ is dominated by

$$\begin{aligned}
&\int_{\Gamma\backslash\mathfrak{H}^m} \varphi(z)|f_1(z)f_2(z)|y^k y^{-2}dxdy \\
&= \sum_i \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\gamma\in\Gamma} \psi(\delta_i^{-1}\gamma z)|f_1(\gamma z)f_2(\gamma z)|\mathrm{Im}(\gamma z)^k y^{-2}dxdy \\
&= \sum_i \int_{\mathfrak{H}^m} \psi(\delta_i^{-1} z)|f_1(z)f_2(z)|y^k y^{-2}dxdy \\
&= \sum_i \int_{\delta_i S} |f_1(z)f_2(z)|y^k y^{-2}dxdy \\
&= \sum_i \int_{S} |f_1(\delta_i z)f_2(\delta_i z)|\mathrm{Im}(\delta_i z)^k y^{-2}dxdy \\
&= \sum_i \int_{S} |(f_1|_k\delta_i)(z)(f_2|_k\delta_i)(z)|y^k y^{-2}dxdy \ .
\end{aligned}$$

Suppose that f_1 is a cuspform and fix i. Then there exist $c, C > 0$ such that

$$y^{\frac{k}{2}}|(f_1|_k\delta_i)(z)| \leq C\exp(-cy^{\frac{1}{m}}),$$

$$y^{\frac{k}{2}}|(f_2|_k\delta_i)(z) - c_0| \leq C\exp(-cy^{\frac{1}{m}}),$$

where c_0 is the 0-th Fourier coefficient of $f_2|_k\delta_i$. From these, the result follows. ∎

Proposition 1.7 If $f \in \mathrm{Cfm}(\Gamma, k)$ and $E \in \mathrm{Eis}(\Gamma, k)$, then $<f, E>= 0$.

Proof. It suffices to prove the assertion for $E = E_\alpha$, since $\mathrm{Eis}(\Gamma, k)$ is spanned by E_α. Note that

$$<f, E_\alpha> \ = \ \int_{\Gamma\backslash\mathfrak{H}^m} f(z) \overline{\sum_{\gamma\in\alpha P\alpha^{-1}\cap\Gamma\backslash\Gamma} \mu(\alpha^{-1}\gamma, z)^{-k}}\mathrm{Im}(z)^k y^{-2}dxdy$$

$$
\begin{aligned}
&= \int_{\Gamma\backslash\mathfrak{H}^m} f(z)\overline{\sum_{\gamma\in P\cap\alpha^{-1}\Gamma\alpha\backslash\alpha^{-1}\Gamma\alpha}\mu(\gamma\alpha^{-1},z)^{-k}}\mathrm{Im}(z)^k y^{-2}dxdy \\
&= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathfrak{H}^m} f(\alpha z)\overline{\sum_{\gamma\in P\cap\alpha^{-1}\Gamma\alpha\backslash\alpha^{-1}\Gamma\alpha}\mu(\gamma\alpha^{-1},\alpha z)^{-k}}\mathrm{Im}(\alpha z)^k y^{-2}dxdy \\
&= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathfrak{H}^m} f(\alpha z)\overline{\mu(\alpha,z)^k}\mathrm{Im}(\alpha z)^k\overline{\sum_{\gamma\in P\cap\alpha^{-1}\Gamma\alpha\backslash\alpha^{-1}\Gamma\alpha}\mu(\gamma,z)^{-k}}y^{-2}dxdy \\
&= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathfrak{H}^m} f(\alpha z)\mu(\alpha,z)^{-k}(\mathrm{Im}(z))^k\overline{\sum_{\gamma\in P\cap\alpha^{-1}\Gamma\alpha\backslash\alpha^{-1}\Gamma\alpha}\mu(\gamma,z)^{-k}}y^{-2}dxdy \\
&= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathfrak{H}^m} (f|_k\alpha)(z)\overline{\sum_{\gamma\in P\cap\alpha^{-1}\Gamma\alpha\backslash\alpha^{-1}\Gamma\alpha}\mu(\gamma,z)^{-k}}(\mathrm{Im}(z))^k y^{-2}dxdy\ .
\end{aligned}
$$

Thus by replacing Γ and f by $\alpha^{-1}\Gamma\alpha$ and $f|_k\alpha$, we may assume that $\alpha = 1$. Moreover, we may assume that $\Gamma = \Gamma(\mathfrak{n})$. Then

$$
\begin{aligned}
< f, E > &= \int_{\Gamma\backslash\mathfrak{H}^m} f(z)\overline{\sum_{\gamma\in P\cap\Gamma\backslash\Gamma}\mu(\gamma,z)^{-k}}y^k y^{-2}dxdy \\
&= \int_{\Gamma\backslash\mathfrak{H}^m}\sum_{\gamma\in P\cap\Gamma\backslash\Gamma} f(\gamma z)\mu(\gamma,z)^k\mathrm{Im}(\gamma z)^k y^{-2}dxdy \\
&= \int_{P\cap\Gamma\backslash\mathfrak{H}^m} f(z)y^k y^{-2}dxdy\ .
\end{aligned}
$$

Let $U = \{\alpha \in \mathcal{O}_+^\times : \alpha \equiv 1 \pmod{\mathfrak{n}}\}$, $T = (0,\infty)^m$. Then

$$
\int_{P\cap\Gamma\backslash\mathfrak{H}^m} f(z)y^k y^{-2}dxdy = \int_{T\backslash U}\left(\int_{\mathbb{R}^m/\mathfrak{n}} f(z)dx\right)y^k y^{-2}dy,
$$

since $P\cap\Gamma\backslash\mathfrak{H}^m$ has a bijective correspondence with $\mathbb{R}^m/\mathfrak{n}\times T/U$ in an obvious manner. Now, the inner integral $\int_{\mathbb{R}^m/\mathfrak{n}} f(z)dx$ is clearly zero, since

$$
f(z) = \sum_{\substack{\xi\in n^* \\ \xi\gg 0}} c_\xi \exp(2\pi i\mathrm{Tr}(\xi z))
$$

is a cuspform. ∎

1.11 Poincare Series.

Lemma 1.16 Let $\{f_i\}$ be a sequence of holomorphic functions on an open subset U of $\mathbb{C}^n$. Then $\{f_i\}$ converges uniformly on a compact set C of U if and only if it converges in the L^1-sense on C (with Lebesgue measure).

Definition 1.10 For a congruence subgroup $\Gamma \supset \Gamma(\mathfrak{n})$, a totally positive element $\nu \in \mathfrak{n}^*$, and for $k = (k_1, \cdots, k_m)$, define the ν-th Poincare series of weight k with respect to Γ as

$$P(z; k, \nu) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \mu(\gamma, z)^{-k} \exp(2\pi i Tr(\nu(\gamma z))),$$

where $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \Gamma \right\}$.

Proposition 1.8 If all $k_j > 2$, then the above series is absolutely and uniformly convergent on compact subsets of $\mathfrak{H}^m$ and defines a cuspform.

Proof. For convergence, it is enough to show that

$$(*) \qquad \int_{\Gamma \backslash \mathfrak{H}^m} y^{\frac{k}{2}} \sum_{\gamma} |\mu(\gamma, z)^{-k} \exp(2\pi i Tr(\nu(\gamma z)))| y^{-2} dx dy < \infty$$

in view of Lemma 1.16.
(Here one should observe that $y^{\frac{k}{2}} \sum_{\gamma} |\mu(\gamma, z)^{-k} \exp(2\pi i Tr(\nu(\gamma z)))|$ is Γ-invariant.)

$$\begin{aligned}
\text{Now, } (*) \text{ is } & \int_{\Gamma \backslash \mathfrak{H}^m} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} (\mathrm{Im}(z))^{\frac{k}{2}} |\mu(\gamma, z)|^{-k} |\exp(2\pi i \mathrm{Tr}(\nu(\gamma z)))| y^{-2} dx dy \\
&= \int_{\Gamma \backslash \mathfrak{H}^m} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} (\mathrm{Im}(\gamma z))^{\frac{k}{2}} |\exp(2\pi i Tr(\nu(\gamma z)))| y^{-2} dx dy \\
&= \int_{\Gamma_\infty \backslash \mathfrak{H}^m} (\mathrm{Im}(z))^{\frac{k}{2}} |\exp(2\pi i Tr(\nu z))| y^{-2} dx dy \\
&= \int_{\mathbb{R}^m / \Lambda} dx \int_{(0,\infty)^m} y^{\frac{k}{2}} |\exp(-2\pi Tr(\nu y))| y^{-2} dy \\
&= \mathrm{vol}(\mathbb{R}^m / \Lambda) \prod_{j=1}^{m} \int_0^\infty y_j^{\frac{k_j}{2} - 1} \exp(-2\pi \nu_j y_j) y_j^{-1} dy_j,
\end{aligned}$$

where $\Lambda = \left\{ x \in \mathbb{R}^m \,\middle|\, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \Gamma_\infty \right\}$.

Here each integral is absolutely convergent if and only if $\frac{k_j}{2}-1>0$ *i.e.*, $k_j>2$.

$$\text{Note that} \quad \begin{aligned} P(\gamma' z;k,\nu) &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma,\gamma' z)^{-k}\exp(2\pi i\mathrm{Tr}(\nu(\gamma\gamma' z))) \\ &= \mu(\gamma',z)^k \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma\gamma',z)^{-k}\exp(2\pi i\mathrm{Tr}(\nu(\gamma\gamma' z))) \\ &= \mu(\gamma',z)^k P(z;k,\nu). \end{aligned}$$

Thus $P(\ ;k,\nu)\in \mathrm{Mfm}(\Gamma,k)$ by Koecher's principle for $m>1$ and by classical result for $m=1$. To show that $P(\ ;k,\nu)\in \mathrm{Cfm}(\Gamma,k)$, it is enough to see that for every $g\in GL_2^+(F)$, $\lim_{\lambda\to\infty}(f|_k g)(i\lambda)=0$. Note that

$$(*) \qquad \begin{aligned} (f|_k g)(i\lambda) &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma,g(i\lambda))^{-k}\exp(2\pi i Tr(\nu(\gamma g(i\lambda))))\mu(g,i\lambda)^{-k} \\ &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma g,i\lambda)^{-k}\exp(2\pi i Tr(\nu(\gamma g(i\lambda)))). \end{aligned}$$

For $\alpha\in GL_2^+(F)$ with $\alpha=\begin{pmatrix} a & b \\ c & d\end{pmatrix}$,

$$\begin{aligned} &|\mu(\alpha,i\lambda)^{-k}\exp(2\pi i Tr(\nu(\alpha(i\lambda))))| \\ &= (\det\alpha)^{\frac{k}{2}}|ci\lambda+d|^{-k}\exp(-2\pi(\det\alpha)\lambda/|ci\lambda+d|^2). \end{aligned}$$

So if γg is not upper triangular, $\mu(\gamma g,i\lambda)^{-k}\to 0$ as $\lambda\to\infty$. If it is, then the exponential term tends to 0 as $\lambda\to\infty$. In either case, the convergence is monotone and therefore $(*)$ tends to 0 by the monotone convergence theorem. ∎

Proposition 1.9 Let $k_j>2$ for $j=1,\cdots,m$, $f(z)=\sum_\xi c_\xi\exp(2\pi i Tr(\xi z))\in \mathrm{Cfm}(\Gamma,k)$, and $P(\ ;k,\nu)$ as before. Then

$$< f,P(\ ;k,\nu)>= c_\nu \nu^{1-k}\mathrm{vol}(\mathbb{R}^m/\Lambda)\prod_{j=1}^m (4\pi)^{1-k_j}\Gamma(k_j-1),$$

where $\Lambda=\left\{x\in\mathbb{R}^m \,\middle|\, \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\in\Gamma\right\}$.

Proof.

$$\begin{aligned}
< f, P(\ ;k,\nu) > &= \int_{\Gamma\backslash\mathfrak{H}^m} f(z) \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \overline{\mu(\gamma,z)^{-k}\exp(2\pi i\mathrm{Tr}(\nu(\gamma z)))} y^k y^{-2} dxdy \\
&= \int_{\Gamma\backslash\mathfrak{H}^m} f(z) \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \overline{\mu(\gamma,z)^{-k}\exp(2\pi i\mathrm{Tr}(\nu(\gamma z)))} |\mu(\gamma,z)|^{2k} \\
&\qquad \times (\mathrm{Im}(\gamma z))^k y^{-2} dxdy \\
&= \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} f(\gamma z)\overline{\exp(2\pi i Tr(\nu(\gamma z)))} (\mathrm{Im}(\gamma z))^k y^{-2} dxdy \\
&= \int_{\Gamma_\infty\backslash\mathfrak{H}^m} \sum_{\xi} c_\xi \exp(2\pi i\mathrm{Tr}(\xi z - \nu\overline{z})) y^k y^{-2} dxdy \\
&= \int_{(0,\infty)^m} \int_{\mathbb{R}^m/\Lambda} \sum_{\xi} c_\xi \exp(2\pi i\mathrm{Tr}(\xi z - \nu\overline{z})) dx\, y^k y^{-2} dy \\
&= c_\nu \mathrm{vol}(\mathbb{R}^m/\Lambda) \prod_{j=1}^m \int_0^\infty \exp(-4\pi\nu_j y_j) y_j^{k_j-1} dy_j \big/ y_j \\
&= c_\nu \mathrm{vol}(\mathbb{R}^m/\Lambda) \prod_{j=1}^m (4\pi\nu_j)^{1-k_j} \Gamma(k_j - 1). \qquad \blacksquare
\end{aligned}$$

Corollary 1.5 The Poincare series span the space of cuspforms.

Proof. The orthogonal complement of the space spanned by Poincare series is 0. ∎

1.12 Reproducing Kernel for Cuspforms.

Theorem 1.10 Let Γ be a congruence subgroup, $k = (k_1, \cdots, k_m) \in \mathbb{Z}^m$. For $z, w \in \mathfrak{H}^m$, define

$$Q(z,w) = \sum_{\gamma\in\Gamma} \mu(\gamma,z)^{-k} (\gamma z + w)^{-k}.$$

If every $k_j > 2$, then this series is absolutely and uniformly convergent for (z,w) in compact subsets of $\mathfrak{H}^m \times \mathfrak{H}^m$. For each $z, w \in \mathfrak{H}^m$, $Q(\ ,w) \in \mathrm{Cfm}(\Gamma, k)$ and $Q(z,\ ) \in \mathrm{Cfm}(\Gamma^\natural, k)$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\natural = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$ and $\Gamma^\natural = \{\gamma^\natural \mid \gamma \in \Gamma\}$. Also,

$$< f, Q(\ ,-\overline{w}) >= \prod_{j=1}^m \left\{ 4\pi \left(\frac{i}{2}\right)^{k_j} \frac{1}{(k_j - 1)} \right\} \times f(w).$$

Proof. As in the case of Poincare series, for convergence of this series it is enough to show that

$$\int_{\Gamma\backslash\mathfrak{H}^m} y^{\frac{k}{2}} \sum_{\gamma\in\Gamma} |\mu(\gamma,z)^{-k}(\gamma z+w)^{-k}| y^{-2}dxdy < \infty.$$

(Here one notes that $y^{\frac{k}{2}} \sum_{\gamma\in\Gamma} |\mu(\gamma,z)^{-k}(\gamma z+w)^{-k}|$ is Γ-invariant.)

$$\begin{aligned} &= \int_{\Gamma\backslash\mathfrak{H}^m} \sum_{\gamma\in\Gamma} (\mathrm{Im}(\gamma z))^{\frac{k}{2}} |(\gamma z+w)^{-k}| y^{-2}dxdy \\ &= \int_{\mathfrak{H}^m} y^{\frac{k}{2}} |z+w|^{-k} y^{-2}dxdy \\ &= \prod_{j=1}^{m} \int_{\mathfrak{H}} y_j^{\frac{k_j}{2}} |z_j+w_j|^{-k_j} y_j^{-2}dx_j dy_j. \end{aligned}$$ ∎

Lemma 1.17 $\int_{\mathfrak{H}} y^{\frac{k}{2}} |z+w|^{-k} y^{-2}dxdy$ is convergent for $k>2$, where $x+iy = z$, $u+iv = w \in \mathfrak{H}$.

Proof. Replacing x by $x-u$ and then x by $x(y+v)$, the given integral is

$$\int_{\mathbb{R}} (x^2+1)^{-\frac{k}{2}} dx \int_0^\infty (y+v)^{1-k} y^{\frac{k}{2}-2} dy.$$

The first integral is clearly convergent for $k>2$. In the second integral , by replacing y by yv we get

$$(*) \qquad v^{-\frac{k}{2}} \int_0^\infty \frac{y^{\frac{k}{2}-1}}{(1+y)^{k-1}} \frac{dy}{y}.$$

Recall that the Beta function is defined by

$$\begin{aligned} B(x,y) &= \int_0^1 t^{x-1}(1-t)^{y-1}dt \qquad (\mathrm{Re}(x), \mathrm{Re}(y) > 0) \\ &= \int_0^\infty \frac{u^x}{(1+u)^{x+y}} \frac{du}{u} \qquad (\text{by putting } u = t/(1-t)). \end{aligned}$$

Also, we have

$$B(x,y) = \Gamma(x)\Gamma(y)/\Gamma(x+y),$$

which is convergent for $\mathrm{Re}(x), \mathrm{Re}(y) > 0$. Thus

$$(*) = v^{-\frac{k}{2}} B\left(\frac{k}{2} - 1, \frac{k}{2}\right)$$

is convergent for $\frac{k}{2} - 1 > 0$. ∎

This shows that the series defining $Q(z, w)$ is uniformly and absolutely convergent on compact subsets.

$$< f, Q(\ \ , -\overline{w}) >= \int_{\mathfrak{H}^m} f(z)(\overline{z} - w)^{-k} y^{k-2} dx dy.$$

Consider the integral

$$(**) \qquad \int_{\mathfrak{H}} \exp(2\pi i \xi_j z)(x - iy - w_j)^{-k_j} y^{k_j - 2} dx dy.$$

The integral in x is

$$\int_{\mathbb{R}} \exp(2\pi i \xi_j x)(x - iy - w_j)^{-k_j} dx = \frac{(2\pi i)^{k_j} \xi_j^{k_j - 1}}{\Gamma(k_j)} \exp(2\pi i \xi_j w_j) \exp(-2\pi \xi_j y)$$

by Lemma 1.15. Thus

$$\begin{aligned}
(**) &= \frac{(2\pi i)^{k_j} \xi_j^{k_j - 1}}{\Gamma(k_j)} \exp(2\pi i \xi_j w_j) \int_0^\infty \exp(-4\pi \xi_j y) y^{k_j - 1} \frac{dy}{y} \\
&= \frac{(2\pi i)^{k_j} \xi_j^{k_j - 1} \Gamma(k_j - 1)}{\Gamma(k_j)(4\pi \xi_j)^{k_j - 1}} \exp(2\pi i \xi_j w_j) \\
&= (4\pi)\left(\frac{i}{2}\right)^{k_j} \frac{1}{(k_j - 1)} \exp(2\pi i \xi_j w_j).
\end{aligned}$$

This implies that

$$< f, Q(\ \ , -\overline{w}) >= \prod_{j=1}^{m} \left\{ 4\pi \left(\frac{i}{2}\right)^{k_j} \frac{1}{(k_j - 1)} \right\} \times f(w).$$

Note that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

$$\mu(\gamma, z)(\gamma z + w) = (\det \gamma)^{-\frac{1}{2}} (cz + d) \left[\frac{az + b}{cz + d} + w \right]$$

$$= (\det\gamma)^{-\frac{1}{2}}(cw+a)\left[\frac{dw+b}{cw+a}+z\right]$$
$$= \mu(\gamma^\natural, w)(\gamma^\natural w + z).$$

Thus if $Q(\ \ , w) \in \mathrm{Cfm}(\Gamma, k)$, then $\sum_{\gamma\in\Gamma} \mu(\gamma^\natural, w)^{-k}(\gamma^\natural w + z)^{-k}$ is a cuspform in w with respect to $\Gamma^\natural$ and therefore $Q(z, \ ) \in \mathrm{Cfm}(\Gamma^\natural, k)$.
Put $\Gamma_\infty = \left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \in \Gamma\right\}$, $\Lambda = \left\{x \middle| \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \in \Gamma\right\}$. Then

$$\begin{aligned} Q(z,w) &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\sum_{\delta\in\Gamma_\infty} \mu(\delta\gamma, z)^{-k}(\delta\gamma z + w)^{-k} \\ &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma, z)^{-k} \sum_{\delta\in\Gamma_\infty} (\delta\gamma z + w)^{-k} \\ &= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma, z)^{-k} \sum_{\lambda\in\Lambda} (\gamma z + w + \lambda)^{-k}. \end{aligned}$$

By Poisson summation formula and Lemma 1.15,

$$\begin{aligned} \sum_{\lambda\in\Lambda}(\gamma z + w + \lambda)^{-k} &= \mathrm{vol}(\mathbb{R}^m/\Lambda)^{-1} \sum_{\substack{\xi\in\Lambda^* \\ \xi\gg 0}} \prod_j \left[(-2\pi i)^{k_j}/\Gamma(k_j)\right] \xi^{k-1} \\ &\qquad \times \exp(2\pi i \mathrm{Tr}(\xi(\gamma z + w))). \end{aligned}$$

Thus

$$\begin{aligned} Q(z,w) &= \mathrm{vol}(\mathbb{R}^m/\Lambda)^{-1} \prod_j \left[\frac{(-2\pi i)^{k_j}}{\Gamma(k_j)}\right] \sum_\xi \xi^{k-1}\exp(2\pi i \mathrm{Tr}(\xi w)) \\ &\qquad \times \Big\{ \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \mu(\gamma, z)^{-k} \exp(2\pi i \mathrm{Tr}(\xi(\gamma z))) \Big\} \\ &= \mathrm{vol}(\mathbb{R}^m/\Lambda)^{-1} \prod_j \left[\frac{(-2\pi i)^{k_j}}{\Gamma(k_j)}\right] \\ &\qquad \times \sum_\xi \xi^{k-1}\exp(2\pi i \mathrm{Tr}(\xi w)) P(z; k, \xi) \end{aligned}$$

is a cuspform in z. ∎

1.13 Analytic Properties of Eisenstein Series.

Define for $k \in \mathbb{Z}$, $k > 2$, $z \in \mathfrak{H}^m$, $s \in \mathbb{C}$,

$$\begin{aligned} & E_k(z) = \sum^*(cz+d)^{-k} && \text{(a multi-index notation)} \\ (*) \quad & E_k(z,s) = \sum^*(cz+d)^{-k}|cz+d|^{-s} && \text{(a multi-index notation)} \end{aligned}$$

where $\sum^*$ is over $(c,d) \in \mathcal{O}^2 - \{0\}/\mathcal{O}_+^\times$.

Remark 1.9 (a) The same method applies to $E_k(z)$ to show that E_k is holomorphic on $\mathfrak{H}^m$ for $k \in \mathbb{Z}$, $k > 2$ and that it is a Hilbert modular form of weight k for any congruence subgroup Γ with $\mathrm{GL}_2^+(\mathcal{O}) \supset \Gamma \supset \mathrm{SL}_2(\mathcal{O})$.

(b) The second term in $(*)$ will be used as a convergence factor, using $s \to 0$, for example.

To obtain the Fourier expansion one may use, in the order of generality ;

(1) Partial fraction expansion of $\cot \pi z$.

(2) Lipschitz formula.

(3) Confluent hypergeometric functions (a special case gives Bessel functions).

(1). Let $m = 1$. Recall that $-\sum_{n\in\mathbb{Z}}(z+n)^{-2} = -\frac{\pi^2}{\sin^2 \pi t} = \frac{d}{dt}(\pi \cot \pi z)$.

Also, $\pi \cot \pi z = \pi i \frac{e^{2\pi i z}+1}{e^{2\pi i z}-1} = \pi i \frac{q+1}{q-1} = \pi i(1 - 2\sum_{n=0}^{\infty} q^n)$, with $q = e^{2\pi i z}$.

Differentiating both of the above succesively

$$(-1)^{k-1}(k-1)! \sum_{n\in\mathbb{Z}}(z+n)^{-k} = -(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n,$$

for $k \geq 2$. Let k be even and $k > 2$. Then

$$\begin{aligned} E_k(z) &= \sum^*(mz+n)^{-k} = 2\sum_{n=1}^{\infty} n^{-k} + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}(mz+n)^{-k} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1} q^{mn} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \end{aligned}$$

where $\sigma_{k-1}(n) = \sum_{\substack{d|n \\ d>0}} d^{k-1}$.

(2). Note that $\Gamma(s) \sum_{n\in\mathbb{Z}} (-2\pi i(z+n))^{-s}$ is well-defined for $z \in \mathfrak{H}$, $Re(s) > 1$, by specifying a branch of $w^{-s} = e^{-s\log w}$. Put

$$\hat{f}(x) = \int_{\mathbb{R}^m} f(t) e^{-2\pi i <t,x>} dt,$$

where $<t,x> = \sum t_j x_j$, f continuous, and $f \in L^1(\mathbb{R}^m)$.

Theorem 1.11 (a) $\hat{f} \in L^1(\mathbb{R}^m) \Rightarrow f(x) = \int_{\mathbb{R}^m} \hat{f}(t) e^{2\pi i <t,x>} dt$ almost everywhere.

(b) If f is continuous, $f = O(|x|^{-m-\alpha})$ for some $\alpha > 0$ as $|x| \to \infty$ (and hence $f \in L^1(\mathbb{R}^m)$ and $\hat{f}$ is meaningful) and $|\hat{f}| = O(|x|^{-m-\beta})$ for some $\beta > 0$, then

$$\sum_{a\in\mathbb{Z}^m} f(x+a) = \sum_{b\in\mathbb{Z}^m} \hat{f}(b) e^{2\pi i <b,x>}.$$

In particular, we have the Poisson summation formula

$$\sum_{a\in\mathbb{Z}^m} f(a) = \sum_{b\in\mathbb{Z}^m} \hat{f}(b). \qquad \blacksquare$$

Example 1.1 Let $f(x) = \begin{cases} x^{s-1} e^{2\pi i x z} & , \text{ if } x > 0 \\ 0 & , \text{ if } x \le 0, \end{cases}$ where $\mathrm{Im}(z) > 0$, $\mathrm{Re}(s) > 1$. Then

$$\hat{f}(t) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i t x} dx = \int_0^{\infty} x^{s-1} e^{2\pi i x(z-t)} dx = \Gamma(s) [-2\pi i(z-t)]^{-s}$$

and we get the Lipschitz formula

$$\sum_{n=1}^{\infty} n^{s-1} e^{2\pi i n z} = \Gamma(s) \sum_{n\in\mathbb{Z}} [-2\pi i(z+n)]^{-s},$$

which can be used as before to get the Fourier expansion of $E_k(z)$.

Remark 1.10 By Fourier inversion formula

$$\int_{-\infty}^{\infty} \Gamma(s)\,[-2\pi i(z-t)]^{-s}\, e^{2\pi i x t} dt = \begin{cases} x^{s-1}e^{2\pi i x z} & , \text{ if } x > 0 \\ 0 & , \text{ if } x \leq 0. \end{cases}$$

Put $v = 2\pi i(t-z)$. Then

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} v^{-s} e^{vx} dv = \begin{cases} x^{s-1}/\Gamma(s) & , \quad x > 0 \\ 0 & , \quad x \leq 0, \end{cases}$$

at least for $\mathrm{Re}(s) > 0,\ c > 0$.

(3). (Confluent Hypergeometric Functions)
We will give the Fourier expansion for $\sum^*(mz+n)^{-\alpha}(m\overline{z}+n)^{-\beta}$, where $\sum^*$ is taken over $(m,n) \in \mathbb{Z}^2 - \{(0,0)\}$.

Theorem 1.12 (Mellin Inversion Formula)

$$G(s) = \int_0^{\infty} F(x)x^{s-1}dx \text{ if and only if } F(x) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} G(s)x^{-s}ds$$

for $x \in \mathbb{R},\ s \in \mathbb{C}$, and F such that the integral converges nicely.

Proof. Let $x = e^u,\ s = 2\pi(c+it)$ for fixed $c \in \mathbb{R},\ G(s) = \Phi(t)$. Then

$$\Phi(t) = G(s) = \int_{-\infty}^{\infty} F(e^u)e^{2\pi u(c+it)}du = \int_{-\infty}^{\infty} F(e^u)e^{2\pi uc}e^{2\pi itu}du$$

and hence by Fourier inversion formula

$$F(e^u)e^{2\pi uc} = \int_{-\infty}^{\infty} G(2\pi(c+it))e^{-2\pi iut}dt$$

and thus

$$F(x) = F(e^u) = \int_{-\infty}^{\infty} G(2\pi(c+it))e^{-2\pi(c+it)u}dt = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} G(s)x^{-s}ds$$

where $\sigma = 2\pi c = \mathrm{Re}(s)$. ∎

Remark 1.11 Note that Mellin inversion formula is just a Fourier inversion formula in different coordinates.

Example 1.2 (a) Let $F(x) = e^{-x}$. Then $\Gamma(s) = \int_0^\infty e^{-x}x^{s-1}dx$, $\mathrm{Re}(s) > 0$, so that $e^{-x} = \dfrac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \Gamma(s)x^{-s}ds$, $\sigma > 0$.

(b) Let $f(x) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$. Then $f(iy) = \sum_{n=0}^{\infty} a_n e^{-2\pi n y}$, so that

$$\begin{aligned}\int_0^\infty [f(iy) - a_0]\, y^{s-1}dy &= \sum_{n=1}^{\infty} a_n \int_0^\infty e^{-2\pi n y}y^{s-1}dy \\ &= \Gamma(s)(2\pi)^{-s}\sum_{n=1}^{\infty} a_n n^{-s}.\end{aligned}$$

Then by Mellin inversion formula

$$f(iy) - a_0 = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} R(s)y^{-s}ds,$$

where $R(s) = \Gamma(s)(2\pi)^{-s}L(f,s)$ (Riemann).

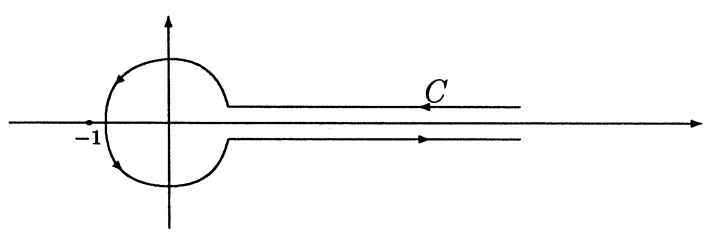
For the following discussion, one is referred to Shimula's papers [S2,S3]. For $y > 0$, $\alpha, \beta \in \mathbb{C}$, put

$$\sigma(y,\alpha,\beta) = \int_0^\infty (u+1)^{\alpha-1}u^{\beta-1}e^{-yu}du = y^{-\beta}\int_0^\infty \left(1+\frac{t}{y}\right)^{\alpha-1}t^{\beta-1}e^{-t}dt.$$

This is convergent for $\mathrm{Re}(\beta) > 0$ and $\sigma(y,1,\beta) = y^{-\beta}\Gamma(\beta)$. It can be shown that

$$(e^{2\pi i\beta} - 1)\sigma(y,\alpha,\beta) = y^{-\beta}\int_\infty^{(0+)} \left(1+\frac{t}{y}\right)^{\alpha-1}t^{\beta-1}e^{-t}dt,$$

where $\int_\infty^{(0+)}$ denotes $\int_C$ with the Hankel contour C.



This shows that $(e^{2\pi i\beta}-1)\sigma(y,\alpha,\beta)$ can be analytically continued to a function holomorphic for all $(\alpha,\beta)\in\mathbb{C}^2$ and

$$y^{\beta}\Gamma(\beta)^{-1}\sigma(y,\alpha,\beta)=\frac{e^{-\pi i\beta}}{2\pi i}\Gamma(1-\beta)\int_{\infty}^{(0+)}(1+y^{-1}t)^{\alpha-1}t^{\beta-1}e^{-t}dt.$$

Recall here that $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$.

Example 1.3 $(e^{2\pi i\beta}-1)\Gamma(\beta)=\int_{\infty}^{(0+)}u^{\beta-1}e^{-u}du.$

Lemma 1.18 Let α,β be complex numbers such that $\mathrm{Re}(\alpha)>0$, $\mathrm{Re}(\beta)>0$, $Re(\alpha+\beta)>1$. Then for $x+iy=z\in\mathfrak{H}$,

$$\sum_{m=-\infty}^{\infty}(z+m)^{-\alpha}(\overline{z}+m)^{-\beta}=\sum_{n=-\infty}^{\infty}\tau_n(y,\alpha,\beta)e^{2\pi inx},$$

where $\tau_n(y,\alpha,\beta)$ is given by

$$i^{\alpha-\beta}(2\pi)^{-\alpha-\beta}\Gamma(\alpha)\Gamma(\beta)\tau_n(y,\alpha,\beta)=\begin{cases}n^{\alpha+\beta-1}e^{-2\pi ny}\sigma(4\pi ny,\alpha,\beta) & \text{if } n>0,\\ |n|^{\alpha+\beta-1}e^{-2\pi|n|y}\sigma(4\pi|n|y,\beta,\alpha) & \text{if } n<0,\\ \Gamma(\alpha+\beta-1)(4\pi y)^{1-\alpha-\beta} & \text{if } n=0.\end{cases}$$

Proof. Put $f(x)=z^{-\alpha}\overline{z}^{-\beta}$ for $x+iy=z$ with a fixed y. By the Poisson summation formula, for $Re(\alpha+\beta)>1$,

$$\sum_{m\in\mathbb{Z}}(z+m)^{-\alpha}(\overline{z}+m)^{-\beta}=\sum_{m\in\mathbb{Z}}f(x+m)=\sum_{n\in\mathbb{Z}}\widehat{f}(n)e^{2\pi inx},$$

where $\widehat{f}(t)=\int_{-\infty}^{\infty}z^{-\alpha}\overline{z}^{-\beta}e^{-2\pi itx}dx$. Putting $v=i\overline{z}=y+ix$,

$$\begin{aligned}\widehat{f}(t) &= i^{\beta-\alpha-1}e^{2\pi ty}\int_{y-i\infty}^{y+i\infty}v^{-\beta}(2y-v)^{-\alpha}e^{-2\pi tv}dv\\ &= i^{\beta-\alpha-1}e^{2\pi ty}\Gamma(\alpha)^{-1}\int_{y-i\infty}^{y+i\infty}v^{-\beta}e^{-2\pi tv}\left\{\int_0^{\infty}e^{-\xi(2y-v)}\xi^{\alpha-1}d\xi\right\}dv\end{aligned}$$

(for $\mathrm{Re}(\alpha)>0$)

$$= i^{\beta-\alpha-1}e^{2\pi ty}\Gamma(\alpha)^{-1}\int_0^{\infty}\xi^{\alpha-1}e^{-2y\xi}\left\{\int_{y-i\infty}^{y+i\infty}v^{-\beta}e^{(\xi-2\pi t)v}dv\right\}d\xi.$$

By Remark 1.10, for $\mathrm{Re}(\beta) > 0$,

$$\int_{y-i\infty}^{y+i\infty} v^{-\beta} e^{\lambda v} dv = \begin{cases} 2\pi i \lambda^{\beta-1} \Gamma(\beta)^{-1} & \text{if } \lambda > 0, \\ 0 & \text{if } \lambda \leq 0. \end{cases}$$

Putting $\xi = 2\pi p$ and $u = \max(0, t)$,

$$(*) \quad \widehat{f}(t) = (2\pi)^{\alpha+\beta} i^{\beta-\alpha} e^{2\pi t y} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} \int_u^\infty p^{\alpha-1} (p-t)^{\beta-1} e^{-4\pi p y} dp,$$

which holds for $\mathrm{Re}(\alpha) > 0$, $\mathrm{Re}(\beta) > 0$ and $\mathrm{Re}(\alpha+\beta) > 1$.
For $t > 0$, put $p - t = tq$. Then $(*)$ is

$$\begin{aligned} & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} e^{-2\pi t y} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} t^{\alpha+\beta-1} \int_0^\infty (1+q)^{\alpha-1} q^{\beta-1} e^{-4\pi t y q} dq \\ = \; & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} e^{-2\pi t y} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} t^{\alpha+\beta-1} \sigma(4\pi t y, \alpha, \beta). \end{aligned}$$

For $t < 0$, put $p = |t|q$. Then $(*)$ is

$$\begin{aligned} & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} e^{-2\pi |t| y} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} |t|^{\alpha+\beta-1} \int_0^\infty (1+q)^{\beta-1} q^{\alpha-1} e^{-4\pi |t| y q} dq \\ = \; & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} e^{-2\pi |t| y} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} |t|^{\alpha+\beta-1} \sigma(4\pi |t| y, \beta, \alpha). \end{aligned}$$

For $t = 0$, $(*)$ is

$$\begin{aligned} & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} \int_0^\infty p^{\alpha+\beta-2} e^{-4\pi y p} dp \\ = \; & (2\pi)^{\alpha+\beta} i^{\beta-\alpha} \Gamma(\alpha)^{-1} \Gamma(\beta)^{-1} (4\pi y)^{-(\alpha+\beta-1)} \Gamma(\alpha+\beta-1). \end{aligned}$$

■

Lemma 1.19 The function $y^\beta \Gamma(\beta)^{-1} \sigma(y, \alpha, \beta)$ is invariant under the transformation $\alpha \mapsto 1-\beta$, $\beta \mapsto 1-\alpha$.

Proof. Consider the Mellin transform of $\sigma(y, \alpha, \beta)$:

$$\begin{aligned} \int_0^\infty \sigma(y, \alpha, \beta) y^{s-1} dy &= \int_0^\infty \int_0^\infty (u+1)^{\alpha-1} u^{\beta-1} e^{-yu} y^{s-1} dy du \\ &= \Gamma(s) \int_0^\infty (u+1)^{\alpha-1} u^{\beta-s-1} du \\ &= \Gamma(s) \Gamma(\beta-s) \Gamma(1-\alpha-\beta+s) / \Gamma(1-\alpha), \end{aligned}$$

for $\mathrm{Re}(s) > 0$, $\mathrm{Re}(\beta - s) > 0$ and $\mathrm{Re}(1-\alpha-\beta+s) > 0$.
(Recall here that for $\mathrm{Re}(x)$, $\mathrm{Re}(y) > 0$,

$$B(x, y) = \int_0^\infty u^{x-1} (1+u)^{-x-y} du = \Gamma(x)\Gamma(y)/\Gamma(x+y). \;)$$

By Mellin inversion formula

$$\Gamma(1-\alpha)\sigma(y,\alpha,\beta)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\Gamma(s)\Gamma(\beta-s)\Gamma(1-\alpha-\beta+s)y^{-s}ds,$$

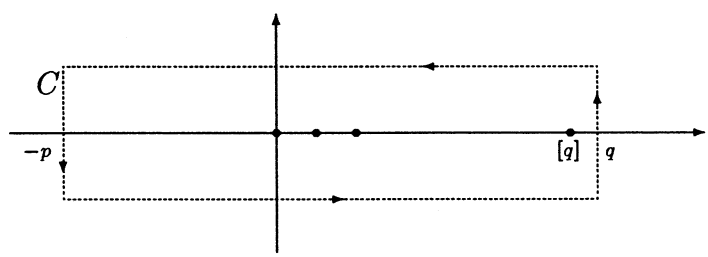
for $c>0$ with $\mathrm{Re}(\alpha+\beta-1)<c<\mathrm{Re}(\beta)$. Put $S=s-\beta$. Then we get

$$y^{\beta}\Gamma(\beta)^{-1}\sigma(y,\alpha,\beta)=\frac{1}{2\pi i}\int_{-p-i\infty}^{-p+i\infty}\frac{\Gamma(-S)\Gamma(S+\beta)\Gamma(S+1-\alpha)}{\Gamma(1-\alpha)\Gamma(\beta)}y^{-S}dS,$$

if $0<p<\min\{\mathrm{Re}(1-\alpha),\ \mathrm{Re}(\beta)\}$ $(-p=c-\mathrm{Re}(\beta))$. Such a number p can be found whenever $\mathrm{Re}(\beta)>0$, $\mathrm{Re}(1-\alpha)>0$. Thus $y^{\beta}\Gamma(\beta)^{-1}\sigma(y,\alpha,\beta)$ is symmetric under $\alpha\mapsto 1-\beta$, $\beta\mapsto 1-\alpha$ with the restriction $\mathrm{Re}(\beta)>0$ and $\mathrm{Re}(1-\alpha)>0$. To get rid of this restriction, define

$$\Phi(y,\alpha,\beta)=\frac{1}{2\pi i}\int_{q-i\infty}^{q+i\infty}\frac{\Gamma(-s)\Gamma(s+\beta)\Gamma(s+1-\alpha)}{\Gamma(\beta)\Gamma(1-\alpha)}y^{-s}ds,$$

for $q>0$, $q\notin\mathbb{Z}$. Using Stirling's formula one shows that the above integral is convergent. Choose q so that $\mathrm{Re}(\beta)>-q$ and $\mathrm{Re}(1-\alpha)>-q$.



The contour integral of

$$(*)\qquad \Gamma(-s)\Gamma(s+\beta)\Gamma(s+1-\alpha)y^{-\beta}/\Gamma(\beta)\Gamma(1-\alpha)$$

over C gives

$$\Phi-y^{\beta}\Gamma(\beta)^{-1}\sigma(y,\alpha,\beta)=\sum\text{ Residues between }\ \mathrm{Re}=-p\text{ and }\mathrm{Re}=q.$$

The only nonholomorphic part of $(*)$ is $\Gamma(-s)$, and

$$\begin{aligned}\Gamma(m+1-s) &= (m-s)(m-1-s)\cdots(1-s)(-s)\Gamma(-s)\\ \Longrightarrow\quad \operatorname*{Res}_{s=m}(\Gamma(-s)) &= \lim_{\lambda\to m}(s-m)\Gamma(-s)=(-1)^{m-1}/m!.\end{aligned}$$

Thus the sum of the residues is

$$\sum_{m=0}^{[q]} \frac{(-1)^{m-1}}{m!} y^{-m} \frac{\Gamma(m+1-\alpha)\Gamma(m+\beta)}{\Gamma(\beta)\Gamma(1-\alpha)}$$

and hence

$$y^{\beta}\Gamma(\beta)^{-1}\sigma(y,\alpha,\beta) = \sum_{m=0}^{[q]} \frac{\Gamma(m+1-\alpha)\Gamma(m+\beta)}{\Gamma(1-\alpha)\Gamma(\beta)} \frac{(-y)^{-m}}{m!} + \frac{1}{2\pi i}\int_{q-i\infty}^{q+i\infty} \frac{\Gamma(-s)\Gamma(s+1-\alpha)\Gamma(s+\beta)}{\Gamma(1-\alpha)\Gamma(\beta)} y^{-s} ds$$

for $\mathrm{Re}(\beta) > -q$ and $\mathrm{Re}(1-\alpha) > -q$. Thus for given α, β we simply choose q large enough and get our result. ∎

2 Automorphic Forms on Classical Domains.

2.1 The Four Families of Classical Domains and Groups Acting on Them.

Type I :

$$\begin{aligned} D = D(p,q) &= \{z \mid p \times q \text{ complex matrix with } 1_q - z^*z \gg 0\ \}, \\ G = U(p,q) &= \{g \in \mathrm{GL}_{p+q}(\mathbb{C}) \mid g^*Hg = H\ \}, \end{aligned}$$

where $H = \begin{pmatrix} -1_p & 0 \\ 0 & 1_q \end{pmatrix}$ and $A \gg 0$ means that A is positive definite (Hermitian). For a matrix v of suitable size, put $H\{v\} = v^*Hv$.

Remark 2.1 (a) $z \in D(p,q) \iff H\left\{\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\} \gg 0.$

(b) For $g \in \mathrm{GL}_{p+q}(\mathbb{C})$, $g \in U(p,q) \iff H\{g\} = H.$

Write each element $g \in U(p,q)$ by using a block decomposition $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a is $p \times p$, b is $p \times q$, c is $q \times p$ and d is $q \times q$. Then G acts on D by a linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az+b)(cz+d)^{-1}.$$

Indeed, first for $z \in D$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$,

$$\begin{aligned} H\left\{\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\} &= H\left\{g\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\} = H\left\{\begin{pmatrix} az+b \\ cz+d \end{pmatrix}\right\} \\ &= (cz+d)^*(cz+d) - (az+b)^*(az+b). \end{aligned}$$

Then $(cz+d)^*(cz+d) \gg 0$, since $H\left\{\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\}$ is positive definite and $(az+b)^*(az+b)$ is positive semi-definite. This implies $(cz+d) \in \mathrm{GL}_q(\mathbb{C})$. Secondly,

$$\begin{aligned} H\left\{\begin{pmatrix} g(z) \\ 1_q \end{pmatrix}\right\} &= ((cz+d)^{-1})^* H\left\{g\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\}(cz+d)^{-1} \\ &= ((cz+d)^{-1})^* H\left\{\begin{pmatrix} z \\ 1_q \end{pmatrix}\right\}(cz+d)^{-1} \gg 0. \end{aligned}$$

Then $g(z) \in D(p,q)$. The isotropy group of the point $0 \in D$ is

$$K = \left\{ \begin{pmatrix} k_1 & \\ & k_2 \end{pmatrix} \middle| \; k_1 \in U(p),\ k_2 \in U(q) \right\}.$$

To see this, note that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K \Longrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}(0) = bd^{-1} = 0$ and

$$H\{g\} = H \iff \begin{cases} a^*a - c^*c = 1_p \\ d^*d - b^*b = 1_q \\ a^*b = c^*d \end{cases}.$$

From these notations, $b = 0$, $c = 0$, $a^*a = 1_p$, $d^*d = 1_q$ *i.e.*, $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ with $a \in U(p)$, $b \in U(q)$. Finally, we demonstrate that the action of G on D is transtive so that D is diffeomorphic to $U(p,q)\big/U(p) \times U(q)$. For any $z \in D$, put

$$\gamma_z = \begin{pmatrix} (1_p - zz^*)^{-\frac{1}{2}} & z(1_q - z^*z)^{-\frac{1}{2}} \\ (1_q - z^*z)^{-\frac{1}{2}} z^* & (1_q - z^*z)^{-\frac{1}{2}} \end{pmatrix}.$$

Then $\gamma_z \in G$ and $\gamma_z(0) = z$.

Remark 2.2 (a) One easily shows that for $z \in D$,

$$z^*z(1_q - zz^*)^{-1} = (1_q - z^*z)^{-1}z^*z.$$

By using this we see that $1_p - zz^* = (1_p + z(1_q - z^*z)^{-1}z^*)^{-1}$ and hence that $1_p - zz^* \gg 0$. Thus $D(p,q)$ is also given by

$$D(p,q) = \{z \mid p \times q \text{ complex matrix with } \; 1_p - zz^* \gg 0\}.$$

(b) $z(1_q - z^*z)^{\frac{1}{2}} = (1_p - zz^*)^{\frac{1}{2}}z$ is needed to show that $\gamma_z \in G$, whose proof is left to the reader.

In the following, note that the groups and domains of Types II and III are subgroups and subdomains of Type I groups and domains.

Type II:

$$D = \{z \in D(n,n) \mid z^t = -z\}, \quad G = \{g \in U(n,n) \mid g^tEg = E\},$$

where $E = \begin{pmatrix} 0_n & 1_n \\ 1_n & 0_n \end{pmatrix}$. For a matrix of suitable size, let us put $E[v] = v^tEv$.

Remark 2.3 Note that $z^t = -z \iff E\left[\begin{pmatrix} z \\ 1_n \end{pmatrix}\right] = 0.$

G acts on D by linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az+b)(cz+d)^{-1}.$$

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $z \in D$. Then $G(z) \in D(n,n)$ and

$$\begin{aligned} E\left[\begin{pmatrix} g(z) \\ 1_n \end{pmatrix}\right] &= (cz+d)^{-t} E\left[g\begin{pmatrix} z \\ 1_n \end{pmatrix}\right](cz+d)^{-1} \\ &= (cz+d)^{-t}\, E\left[\begin{pmatrix} z \\ 1_n \end{pmatrix}\right](cz+d)^{-1} \\ &= 0. \end{aligned}$$

Thus $g(z) \in D$.

Remark 2.4 (a) Note that $g \in U(p,q) \iff g^{-1} = H^{-1}g^*H$ *i.e.*, writing $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have $g^{-1} = \begin{pmatrix} a^* & -c^* \\ -b^* & d^* \end{pmatrix}$.

(b) Thus for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(n,n)$,

$$g \in G \iff g^{-1} = Eg^tE = \begin{pmatrix} d^t & b^t \\ c^t & a^t \end{pmatrix} \iff d = \bar{a},\ c = -\bar{b} \quad i.e.,$$

$$G = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \middle|\ \bar{a}^t a - b^t\bar{b} = 1_n,\ \ \bar{a}^t b = -b^t\bar{a} \right\}.$$

The isotropy group of $0 \in D$ is $K = \left\{ \begin{pmatrix} k & \\ & k^{-t} \end{pmatrix} \middle|\ k \in U(n) \right\}$. The action of G on D is transitive. To show this, note first that

$$\begin{aligned} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in G &\iff \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}^{-1} = \begin{pmatrix} \bar{a}^t & b^t \\ -\bar{b}^t & a^t \end{pmatrix} \in G \\ &\iff a\bar{a}^t - b\bar{b}^t = 1_n,\ \ ab^t = -ba^t. \end{aligned}$$

For any $z \in D$, find $A \in \mathrm{GL}_n(\mathbb{C})$ so that $A(1_n - z\bar{z}^t)\overline{A^t} = 1_n$. Then

$$g = \begin{pmatrix} A & -Az \\ \bar{A}z & \bar{A} \end{pmatrix} \in G \quad \text{and} \quad g(z) = 0.$$

Therefore D is diffeomorphic to G/K.

Type III:

$$D = \{z \in D(n,n) \mid z^t = z\}, \qquad G = \{g \in U(n,n) \mid g^t J g = J\},$$

where $J = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$. Then G acts on D by linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az+b)(cz+d)^{-1}.$$

$$G = \left\{ \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix} \middle| \, \bar{a}^t a - b^t \bar{b} = 1_n, \ \bar{a}^t b = b^t \bar{a} \right\}.$$

The isotropy group of $0 \in D$ is

$$K = \left\{ \begin{pmatrix} k & \\ & k^{-t} \end{pmatrix} \middle| \, k \in U(n) \right\}.$$

The action of G on D is transitive and hence D is diffeomorphic to G/K.

Type IV:

$$\begin{aligned} D &= \{z \mid 2 \times q \text{ real matrix with } 1_q - {}^t z z \gg 0\}, \\ G &= \mathrm{SO}_0(2,q) = \text{ the identity component of} \\ &\qquad \left\{ g \in \mathrm{SL}_{2+q}(\mathbb{R}) \middle| \, g^t \begin{pmatrix} -1_2 & \\ & 1_q \end{pmatrix} g = \begin{pmatrix} -1_2 & \\ & 1_q \end{pmatrix} \right\}. \end{aligned}$$

G acts on D by linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az+b)(cz+d)^{-1},$$

where a is 2×2, d is $q \times q$, etc. The isotropy group of $0 \in D$ is

$$K = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} \middle| \, a \in \mathrm{SO}(2), \ b \in \mathrm{SO}(q) \right\}.$$

The action of G on K is transitive, which can be shown as in the Type I case. Thus D is diffeomorphic to G/K.

2.2 Cayley Transforms and Unbounded Models of The Classical Domains.

Recall that

$$\mathrm{SU}(1,1) = \mathrm{U}(1,1) \cap \mathrm{SL}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix} \middle| \, |a|^2 - |b|^2 = 1 \right\}$$

acts on the unit disk $D = \{z \in \mathbb{C} : |z| < 1\}$ as a linear fractional transformations. Put $c = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$. Then the Cayley map $D \to \mathfrak{H}$ given by the linear fractional transformation

$$z \mapsto c(z) = (z+i)(iz+1)^{-1}$$

is a diffeomorphism and $c\mathrm{SU}(1,1)c^{-1} = \mathrm{SL}_2(\mathbb{R})$. This has generalizations to the classical domains.

Type III:
Put

$$\begin{aligned}
c &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1_n & i1_n \\ i1_n & 1_n \end{pmatrix} \in \mathrm{GL}_{2n}(\mathbb{C}), \\
D_n &= \{z \in D(n,n) \mid z^t = z\}, \\
G_n &= \left\{ g \in \mathrm{SU}(n,n) \middle| g^t \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix} g = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix} \right\}, \\
\mathfrak{H}_n &= \left\{ z \in \mathrm{M}_n(\mathbb{C}) \middle| z^t = z, \ (z - \bar{z})/2i \gg 0 \right\}, \\
\mathrm{Sp}(n,\mathbb{R}) &= \left\{ g \in \mathrm{GL}_{2n}(\mathbb{R}) \middle| g^t \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix} g = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix} \right\},
\end{aligned}$$

where $\mathfrak{H}_n$ is called the Siegel upper half plane of genus n. Just as in the classical case the map $D_n \to \mathfrak{H}_n$ given by the linear fractional transformation $z \mapsto c(z) = (z + i1_n)(iz + 1_n)^{-1}$ is a diffeomorphism and $cG_nc^{-1} = \mathrm{Sp}(n,\mathbb{R})$. Further, for $g \in G_n$, $z \in D_n$, $c(g(z)) = (cgc^{-1})(c(z))$. First, we have to verify that $(iz + 1_n)$ is nonsingular for $z \in D_n$. Assume that $(iz + 1_n)v = 0$ for some $v \in \mathbb{C}^n$ *i.e.*,

$$\begin{aligned}
zv = iv &\Rightarrow \bar{z}\bar{v} = -i\bar{v} \text{ and } v^t z = iv^t \\
&\Rightarrow v^t(1_n - z\bar{z})\bar{v} = v^t\bar{v} - v^t\bar{v} = 0 \\
&\Rightarrow v = 0,
\end{aligned}$$

since $1_n - z\bar{z} \gg 0$ and thus $iz + 1_n$ is non-singular. Next, note that for $z \in D_n$,

$$c(z)^t = (iz + 1_n)^{-1}(z + i1_n) = (z + i1_n)(iz + 1_n)^{-1} = c(z).$$

Finally, from the identity $\begin{pmatrix} -1_n & \\ & 1_n \end{pmatrix} \left\{ c^{-1} \begin{pmatrix} z \\ 1_n \end{pmatrix} \right\} = (z - z^*)/i$, we get

$$\begin{aligned} (c(z) - c(z)^*)/i &= \begin{pmatrix} -1_n & \\ & 1_n \end{pmatrix} \left\{ c^{-1} \begin{pmatrix} c(z) \\ 1_n \end{pmatrix} \right\} \\ &= \begin{pmatrix} -1_n & \\ & 1_n \end{pmatrix} \left\{ \begin{pmatrix} z \\ 1_n \end{pmatrix} (-iz + 1_n) \right\} \gg 0, \end{aligned}$$

for $z \in D_n$. Also, we see $cG_nc^{-1} = \mathrm{Sp}(n, \mathbb{R})$ easily. Since the analogous things can also be proved for the inverse map $\mathfrak{H}_n \to D_n$ $(z \mapsto (z - i1_n)(-iz + 1_n)^{-1})$, we are done with this type.

Remark 2.5 (a) $\mathfrak{H}_n$ is a Siegel domain of first kind, which is also called a "tube domain". We explain this briefly in the following. Let U be a vector space over $\mathbb{R}$ of positive dimension. A nondegenerate open convex cone in U is a non-empty open set Ω of U satisfying :

$$x, y \in \Omega \iff \lambda x + \mu y \in \Omega$$

for any positive real numbers λ, μ and, in addition, not containing any straight line. Then a Siegel domain of first kind is

$$\mathcal{S}(\Omega) = U + i\Omega = \{ u \in U_{\mathbb{C}} \mid \mathrm{Im}(u) \in \Omega \},$$

for such a nondegenerate open convex cone Ω in U (with vertex at the origin).

(b)
1. Let Ω_1 be the set of all real positive definite symmetric matrices of size n. Then Ω_1 is a cone in $\mathrm{Symm}(n, \mathbb{R}) \cong \mathbb{R}^{\frac{n(n+1)}{2}}$, where $\mathrm{Symm}(n, \mathbb{R})$ is the real vector space of all $n \times n$ real symmetric matrices. Thus $\mathcal{S}(\Omega_1) = \mathfrak{H}_n$.
2. Let Ω_2 be the set of all complex positive definite Hermitian matrices of size n. Then Ω_2 is a cone in $\mathrm{Herm}(n, \mathbb{C}) \cong \mathbb{R}^{n^2}$, where $\mathrm{Herm}(n, \mathbb{C})$ is the real vector space consisting of all $n \times n$ complex Hermitian matrices. As we will explain in a moment, $\mathcal{S}(\Omega_2) = \mathcal{J}_n$ is the Hermitian upper half space.

Type I (A special case) :
Define the Hermitian upper half space

$$\mathcal{J}_n = \{z \in \mathrm{M}_n(\mathbb{C}) \mid (z - z^*)/2i \gg 0 \}.$$

Let $U_n = \{g \in \mathrm{GL}_{2n}(\mathbb{C}) \mid g^*Hg = H \}$ with $H = \begin{pmatrix} 0_n & -i1_n \\ i1_n & 0_n \end{pmatrix}$. Then U_n acts on $\mathcal{J}_n$ by linear fractional transformations, $U_n = cU(n,n)c^{-1}$ (with the same c as in the above), $c(D(n,n)) = \mathcal{J}_n$, and the Cayley map $D(n,n) \to \mathcal{J}_n$, $(z \mapsto c(z))$ is a diffeomorphism and is equivariant with respect to $U(n,n)$ and U_n.

Type I (General case) :
Consider the domain $D(p,q)$ and the group $U(p,q)$ for $p \geq q$ (without loss of generality). Put

$$c = \begin{pmatrix} \frac{1}{\sqrt{2}}1_q & 0 & \frac{1}{\sqrt{2}}i1_q \\ 0 & 1_{p-q} & 0 \\ \frac{1}{\sqrt{2}}i1_q & 0 & \frac{1}{\sqrt{2}}1_q \end{pmatrix} \in \mathrm{GL}_{p+q}(\mathbb{C}).$$

Use the coordinates (z,u) for $\begin{pmatrix} z \\ u \end{pmatrix} \in M_{p,q}(\mathbb{C})$, where z is $q \times q$ and u is $(p-q) \times q$. For

$$H = \begin{pmatrix} 0_q & 0 & -i1_q \\ 0 & 1_{p-q} & 0 \\ i1_q & 0 & 0_q \end{pmatrix},$$

define

$$U_{p,q} = \{g \in \mathrm{GL}_{p+q}(\mathbb{C}) \mid g^*Hg = H\}.$$

Then one verifies that $z \mapsto c(z)$ gives a diffeomorphism

$$D(p,q) \to \{(z,u) \mid (z - z^*)/2i - \frac{1}{2}u^*u \gg 0 \}.$$

Indeed, for $w \in D(p,q)$,

$$\begin{pmatrix} -1_p & \\ & 1_q \end{pmatrix} \left\{ \begin{pmatrix} w \\ 1_q \end{pmatrix} \right\} > 0 \iff c \begin{pmatrix} -1_p & \\ & 1_q \end{pmatrix} c^{-1} \left\{ c \begin{pmatrix} w \\ 1_q \end{pmatrix} \right\} > 0$$
$$\iff (-H) \left\{ \begin{pmatrix} c(w) \\ 1_q \end{pmatrix} \right\} > 0.$$

Thus

$$\begin{aligned} c(D(p,q)) &= \left\{ (z,u) \,\middle|\, H\left\{ \begin{pmatrix} z \\ u \\ 1_q \end{pmatrix} \right\} < 0 \right\} \\ &= \{(z,u) \mid (z-z^*)/2i - \frac{1}{2}u^*u \gg 0\}. \end{aligned}$$

Also, $cU(p,q)c^{-1} = U_{p,q}$ and the Cayley map is equivariant with respect to $U(p,q)$ and $U_{p,q}$.

Remark 2.6 (a) $c(D(p,q))$ is a Siegel domain of second kind. Let Ω be a nondegenerate open convex cone in a vector space U over $\mathbb{R}$ of positive dimension, and let V be a vector space over $\mathbb{C}$. Assume that a Hermitian map $H: V \times V \to U_{\mathbb{C}}$ ($\mathbb{C}$–linear in the 2^{nd} component and $\mathbb{C}$-antilinear in the 1^{st}) is given, which is Ω-positive *i.e.*, $H(v,v) \in \bar{\Omega}$ for all $v \in V$. Then for such U, V, Ω, H, the Siegel domain of second kind $\mathcal{S} = \mathcal{S}(U,V,\Omega,H)$ is given by

$$\mathcal{S} = \{(u,v) \in U_{\mathbb{C}} \times V \mid \mathrm{Im}(u) - H(v,v) \in \Omega \}.$$

(b) If $V = \{0\}$, then we obtain the tube domain $\mathcal{S}(\Omega)$. Also, any Siegel domain $\mathcal{S}(U,V,\Omega,H)$ contains a tube domain as the zero section $\{v{=}0\}$.

(c) Let $U = \mathbb{R}$, $V = \mathbb{C}^n$, and let H be the standard Hermitian form

$$H(v,v) = \sum_{j=1}^{n} |v_j|^2 \quad (v = (v_j) \in \mathbb{C}^n).$$

Then the associated Siegel domain

$$\mathcal{S} = \{(u,v) \in \mathbb{C}^{n+1} \mid \mathrm{Im}(u) - \sum_{j=1}^{n} |v_j|^2 > 0 \}$$

is holomorphically equivalent to the ball

$$B^{n+1} =: \{(z_1, \ldots, z_{n+1}) \in \mathbb{C}^{n+1} \mid |z_1|^2 + \cdots + |z_{n+1}|^2 < 1 \}.$$

Indeed, by changing variables $z_1 = \dfrac{u-i}{u+i}$, $z_k = \dfrac{2v_{k-1}}{u+i}$ $(k = 2, \ldots, n+1)$, $(u,v) \in \mathcal{S} \iff 1 - \sum\limits_{k=1}^{n+1} |z_k|^2 = \dfrac{4}{|u+i|^2}(\mathrm{Im}(u) - \sum\limits_{j=1}^{n} |v_j|^2) > 0.$

(d) For $U = \mathrm{Herm}(q, \mathbb{C})$ (so that $U_{\mathbb{C}} = M_q(\mathbb{C})), V = M_{p-q,q}(\mathbb{C})$, $\Omega = \{u \in U \mid u \gg 0\}$, $H(u,v) = \frac{1}{2}u^*v$, we see that

$$\mathcal{S}(U, V, \Omega, H) = c(D(p,q))$$

for $p \geq q$.

2.3 Examples of Holomorphic Automorphic Forms.

Define a discrete subgroup

$$\Gamma = \mathrm{Sp}(n, \mathbb{Z}) = \left\{ g \in \mathrm{GL}_{2n}(\mathbb{Z}) \,\middle|\, g^t \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} g = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} \right\},$$

called the Siegel modular group, of $\mathrm{Sp}(n, \mathbb{R})$. Then $\mathrm{Sp}(n, \mathbb{Z})$ acts discontinuously on $\mathfrak{H}_n$. For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(n, \mathbb{R})$, $z \in \mathfrak{H}_n$, $k \in \mathbb{Z}$, define

$$\mu(g, z) = \det(cz + d)^{2k}.$$

A holomorphic Siegel modular form of weight $2k$ is defined to be a holomorphic function f on $\mathfrak{H}_n$ with the property : for all $\gamma \in \Gamma$ and $z \in \mathfrak{H}_n$,

$$f(\gamma(z)) = \mu(\gamma, z) f(z)$$

(plus a growth condition if $n = 1$).

Let $\mathrm{Symm}(n, \mathbb{R}) \cong \mathbb{R}^{\frac{n(n+1)}{2}}$ be the real vector space of all $n \times n$ symmetric matrices. Then consider the pairing

$$\mathrm{Symm}(n, \mathbb{R}) \times \mathrm{Symm}(n, \mathbb{R}) \to \mathbb{R} \text{ given by } (A, B) \mapsto \mathrm{Tr}(AB).$$

Theorem 2.1 The dual lattice Λ^* to the lattice Λ of all $n \times n$ integral symmetric matrices is

$$\begin{aligned} \Lambda^* &= \left\{ \xi \,\middle|\, \begin{array}{c} \xi \text{ is symmetric } n \times n, \text{ diagonal entries of } \xi \text{ are in } \mathbb{Z} \\ \text{and the off-diagonal entries are in } \frac{1}{2}\mathbb{Z} \end{array} \right\} \\ &= \{\xi \mid \xi \text{ is semi-integral}\}. \end{aligned}$$

Proof. Let ε_i be the matrix with 1 at (i,i) and 0 elsewhere, for $i = 1, 2, \ldots, n$. Let ε_{ij} be the matrix with 1 at (i,j) and (j,i) and with 0 elsewhere, for each $i < j$. Then ε_i $(i = 1, 2, \ldots, n)$ and ε_{ij} $(i<j)$ form a basis of Λ. $A = (a_{ij}) \in \mathrm{Symm}(n, \mathbb{R})$ belongs to Λ^* if and only if $\mathrm{Tr}(A\varepsilon_i) \in \mathbb{Z}$ for $i = 1, 2, \ldots, n$, and $\mathrm{Tr}(A\varepsilon_{ij}) \in \mathbb{Z}$ for $i < j$. But $\mathrm{Tr}(A\varepsilon_i) = a_{ii}$ and $\mathrm{Tr}(A\varepsilon_{ij}) = a_{ij} + a_{ji} = 2a_{ij}$. ∎

Since Γ contains the subgroup

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| u = u^t \text{ is } n \times n \text{ integral} \right\},$$

$f(x+u+iy) = f(x+iy)$ for all $z = x+iy \in \mathfrak{H}_n$ and $n \times n$ integral symmetric u, and hence

$$f(x+iy) = \sum_{\xi \in \Lambda^*} c_\xi(y) \exp(2\pi i \mathrm{Tr}(\xi x)).$$

Note that $\mathrm{Tr}(\xi x) = \sum_{i=1}^{n} \sum_{j=1}^{n} \xi_{ij} x_{ij} = 2 \sum_{i<j} \xi_{ij} x_{ij} + \sum_i \xi_{ii} x_{ii}$ for $\xi = (\xi_{ij})$, $x = (x_{ij})$. Thus the holomorphy of f implies

$$\begin{cases} 4\pi i \xi_{ij} c_\xi(y) = -i \dfrac{\partial c_\xi(y)}{\partial y_{ij}} & \text{for } i < j \\ 2\pi i \xi_{ii} c_\xi(y) = -i \dfrac{\partial c_\xi(y)}{\partial y_{ii}} & \text{for } i = 1, 2, \ldots, n, \end{cases}$$

and hence $c_\xi(y) = c_\xi \exp(-2\pi \mathrm{Tr}(\xi y))$. Thus we have

$$f(z) = \sum_{\xi \in \Lambda^*} c_\xi \exp(2\pi i \mathrm{Tr}(\xi z)).$$

Define discrete subgroups of $G(\mathbb{R}) = \{g \in \mathrm{GL}_{2n}(\mathbb{C}) \mid g^* H g = H\}$ as follows, where $H = \begin{pmatrix} 0 & -i1_n \\ i1_n & 0 \end{pmatrix}$. Let K be a imaginary quadratic field with the ring of integers $\mathcal{O}$. Then Hermitian modular group (depending on $\mathcal{O}$) is

$$\Gamma = \{g \in \mathrm{GL}_{2n}(\mathcal{O}) \mid g^* H g = H\} = \mathrm{GL}_{2n}(\mathcal{O}) \cap \mathrm{G}(\mathbb{R}),$$

which is again a discrete subgroup of $\mathrm{G}(\mathbb{R})$ and hence acts discontinuously on $\mathcal{J}_n$. Write the elements z of $\mathcal{J}_n = \{z \in \mathrm{M}_n(\mathbb{C}) \mid (z - z^*)/2i \gg 0\}$ as

$$z = x + iy = \left(\frac{z+z^*}{2}\right) + i\left(\frac{z-z^*}{2}\right),$$

so that x, y are hermitian and $y \gg 0$. For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G}(\mathbb{R})$, $z \in \mathcal{J}_n$, $k \in \mathbb{Z}$, $\mu(g,z) = \det(cz+d)^{2k}$.
Then a holomorphic hermitian modular form of weight $2k$ is defined to be a holomorphic function f on $\mathcal{J}_n$ with the property : for all $z \in \mathcal{J}_n$ and $\gamma \in \Gamma$,

$$f(\gamma(z)) = \mu(\gamma, z) f(z)$$

(plus a growth condition if $n = 1$). Consider the pairing

$$\mathrm{Herm}(n,\mathbb{C}) \times \mathrm{Herm}(n,\mathbb{C}) \to \mathbb{R} \quad \text{given by} \quad (A,B) \mapsto \mathrm{Tr}(AB),$$

where $\mathrm{Herm}(n,\mathbb{C}) \cong \mathbb{R}^{n^2}$ is the real vector space of $n \times n$ hermitian matrices.

(**Note** : $\overline{\mathrm{Tr}(AB)} = \mathrm{Tr}(AB)^* = \mathrm{Tr}(B^*A^*) = \mathrm{Tr}(A^*B^*) = \mathrm{Tr}(AB)$.)

Put $\Lambda = \{n \times n \text{ hermitian matrices with entries in } \mathcal{O}\}$. Then we see that

$$\Lambda^* = \left\{ \xi \;\middle|\; \begin{array}{c} \xi \text{ is } n \times n \text{ hermitian, diagonal entries in } \mathcal{O}^* \\ \text{and off-diagonal entries in } \frac{1}{2}\mathcal{O}^* \end{array} \right\},$$

where $\mathcal{O}^* = \{\alpha \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}) \subset \mathbb{Z}\}$ and the dual lattice Λ^* is with respect to the above pairing. Since Γ contains the subgroup

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{array}{c} u = u^* \text{ is an } n \times n \text{ matrix} \\ \text{with entries in } \mathcal{O} \end{array} \right\},$$

we have

$$f(x+iy) = \sum_{\xi \in \Lambda^*} c_\xi(y) \exp(2\pi i \mathrm{Tr}(\xi x)).$$

For f to be holomorphic, it must be that the Fourier coefficients (as functions of the imaginary part y of $z \in \mathcal{J}_n$) are of the form

$$c_\xi(y) = c_\xi \exp(-2\pi \mathrm{Tr}(\xi y)).$$

So the Fourier expansion of a holomorphic hermitian modular form has the form

$$f(z) = \sum_{\xi} c_\xi \exp(2\pi i \mathrm{Tr}(\xi z)).$$

2.4 Koecher's Principle for Siegel Modular Forms.

Let f be a holomorphic Siegel modular form on $\mathfrak{H}_n$ (with respect to $\Gamma = \mathrm{Sp}(n,\mathbb{Z})$). Let $f(z) = \sum_{\xi} c_\xi \exp(2\pi i \mathrm{Tr}(\xi z))$, where ξ runs over semi-integral symmetric matrices.

Theorem 2.2 (Koecher's Principle) Suppose that $n > 1$. Then the Fourier coefficient c_ξ of a Siegel modular form of weight $2k$ is zero unless ξ is positive semi-definite (semi-integral).

Proof. Note that Γ contains the subgroup

$$L = \left\{ \begin{pmatrix} A & 0 \\ 0 & A^{-t} \end{pmatrix} \middle| A \in \mathrm{GL}_n(\mathbb{Z}) \right\}.$$

Since $\det(0z + A^{-t})^{2k} = 1$, $f(AzA^t) = f(z)$ for all $z \in \mathfrak{H}_n$, $A \in \mathrm{GL}_n(\mathbb{Z})$ *i.e.*,

$$\begin{aligned} \sum_{\xi} c_\xi \exp(2\pi i \mathrm{Tr}(\xi z)) &= \sum_{\xi} c_\xi \exp(2\pi i \mathrm{Tr}(\xi A z A^t)) \\ &= \sum_{\xi} c_\xi \exp(2\pi i \mathrm{Tr}(A^t \xi A z)) \end{aligned}$$

and this implies $c(A^t \xi A) = c(\xi)$ for all $A \in \mathrm{GL}_n(\mathbb{Z})$.
Consider the subseries of $f(\lambda i 1_n)$ with $\lambda \in \mathbb{R}_{>0}$:

$$\begin{aligned} S &= \sum_{A \in GL_n(\mathbb{Z})} c(A^t \xi A) \exp(-2\pi\lambda \mathrm{Tr}(A^t \xi A)) \\ &= c(\xi) \sum_{A \in GL_n(\mathbb{Z})} \exp(-2\pi\lambda \mathrm{Tr}(A^t \xi A)). \end{aligned}$$

If $c(\xi) \neq 0$ and ξ is not positive semi-definite, then $N = \{ v \in \mathbb{R}^n \mid v^t \xi v < 0 \}$ is open and closed under multiplication by numbers in $\mathbb{R}^\times$. Thus one can find infinitely many $A \in \mathrm{GL}_n(\mathbb{Z})$ so that the columns of A lie in N. For such an $A = (A^1\, A^2 \cdots A^n)$,

$$\mathrm{Tr}(A^t \xi A) = (A^1)^t \xi A^1 + \cdots + (A^n)^t \xi A^n < 0.$$

Thus we have $\exp(-2\pi\lambda \mathrm{Tr}(A^t \xi A)) > 1$ and this implies S is divergent. ∎

3 Adelic Viewpoint.

3.1 Analysis on Adeles.

Let k be a number field, M_k the set of all places of k.
Given $v \in M_k$, let $\| \ \|_v : k_v \to \mathbb{R}_{\geq 0}$ be the unique absolute value inducing :

If $v < \infty$, then it is the v-adic topology such that $\|\pi\|_v = \frac{1}{q_v}$ (π a uniformizer of k_v, $q_v =$ cardinality of the residue field of k_v).

If $v = \infty$ *i.e.*, $k_v \cong \mathbb{R}$ or $\mathbb{C}$, then $\|x\|_v = \begin{cases} |x| & , \text{ if } k_v \cong \mathbb{R} \\ |x|^2 & , \text{ if } k_v \cong \mathbb{C} \end{cases}$.

1^0. Then we have the product formula : $\prod_{v \in M_k} \|x\|_v = 1, \quad \text{for } 0 \neq x \in k.$

2^0. Let μ be an (additive) Haar measure on k_v.
For $a \in k_v^\times$, let $\mu_a(U) = \mu(aU)$. Then $\mu_a = \|a\|_v \mu$.
Proof. Check this directly for $k_v = \mathbb{R}$, $\mathbb{C}$. For v finite,

$$\mu_\pi(\pi^{-1}\mathcal{O}_{k_v}) = \sum_{x \in \mathcal{O}_{k_v}/(\pi)} \mu\Big(\frac{x}{\pi} + \mathcal{O}_{k_v}\Big) = q_v \mu(\mathcal{O}_{k_v}). \qquad \blacksquare$$

The ring of adeles $k_{\mathbb{A}}$ of k is defined as follows : As a set,

$$k_{\mathbb{A}} = \Big\{ x = (x_v) \in \prod_{v \in M_k} k_v \mid \|x_v\|_v \leq 1 \text{ for all but finitely many } v \Big\}.$$

$k_{\mathbb{A}}$ is a ring under componentwise multiplication and addition. We may regard k as a subring of $k_{\mathbb{A}}$ under the "diagonal embedding"

$$x \mapsto (\cdots, x, x, x, \cdots) : k \to k_{\mathbb{A}}.$$

Topology for $k_{\mathbb{A}}$:
Let S be any finite subset of M_k containing all infinite places. Then

$$k_{\mathbb{A},S} = : \prod_{v \in S} k_v \times \prod_{v \notin S} \mathcal{O}_{k_v}, \quad k_{\mathbb{A}} = \bigcup_S k_{\mathbb{A},S} \subseteq \prod_{v \in M_k} k_v.$$

Since $k_{\mathbb{A},S}$ is the product of finitely many locally compact groups and infinitely many compact groups, $k_{\mathbb{A},S}$ is locally compact in the product topology, and

the addition and multiplication are continuous.
Topology on $k_{\mathbb{A}}$ is defined by declaring all subgroups $k_{\mathbb{A},S}$ to be open. So $k_{\mathbb{A}}$ is again locally compact, and addition and multiplication are continuous. A neighborhood base at 0 for the topology of $k_{\mathbb{A}}$is the collection of sets $U = \prod_{v \in M_k} U_v$, where $0 \in U_v \underset{open}{\subseteq} k_v$ and $U_v = \mathcal{O}_{k_v}$ for almost all v.

Facts 1 (a) $k \subseteq k_{\mathbb{A}}$ is discrete in $k_{\mathbb{A}}$.

(b) $k_{\mathbb{A}}/k$ is compact.

The group of ideles $\mathbb{J}_k$ of k is defined as follows : As a set,

$$\mathbb{J}_k = \left\{ x = (x_v) \in \prod_{v \in M_k} k_v^{\times} \mid \|x_v\|_v = 1 \text{ for all but finitely many } v \right\}.$$

Let S be a finite subset of M_k containing all infinite places. Then

$$\mathbb{J}_{k,S} =: \prod_{v \in S} k_v^{\times} \times \prod_{v \notin S} \mathcal{O}_{k_v}^{\times}, \quad \mathbb{J}_k = \bigcup_S \mathbb{J}_{k,S}.$$

$\mathbb{J}_{k,S}$ is locally compact and multiplication is continuous when it is equipped with the product topology.
$\mathbb{J}_k$ is equipped with topology by declaring each subgroup $\mathbb{J}_{k,S}$ to be open, so that it is also locally compact and multiplication is continuous. A neighborhood base of 1 for the topology of $\mathbb{J}_k$ is the collection of sets $U = \prod_{v \in M_k} U_v$, where $1 \in U_v \underset{open}{\subseteq} k_v^{\times}$ and $U_v = \mathcal{O}_{k_v}^{\times}$ for almost all v.

$$k^{\times} \subseteq \mathbb{J}_k \text{ via } x \mapsto (\cdots, x, x, x, \cdots).$$

$\| \ \| : \mathbb{J}_k \to \mathbb{R}_{>0}$ $(x \mapsto \|x\| = \prod_{v \in M_k} \|x_v\|_v)$, called norm, is a continuous homomorphism. Put $\mathbb{J}_k^0 =: \ker(\| \ \| : \mathbb{J}_k \to \mathbb{R}_{>0})$.
For $a \in \mathbb{J}_k$, and $b \in k_{\mathbb{A}}$, $ab \in k_{\mathbb{A}}$ $((ab)_v = a_v b_v)$ and hence we have :

$$\mathbb{J}_k \times k_{\mathbb{A}} \to k_{\mathbb{A}} \ ((a, b) \mapsto ab) \text{ is continuous.}$$

Note that for each $a \in \mathbb{J}_k$, $b \mapsto ab : k_{\mathbb{A}} \to k_{\mathbb{A}}$ is a continuous automorphism. Let μ be an additive Haar measure on $k_{\mathbb{A}}$. For $a \in \mathbb{J}_k$, define $\mu_a(U) = \mu(aU)$. One can check that $\mu_a = \|a\|\mu$.

Facts 2 (a) $k^\times$ is discrete in $\mathbb{J}_k$.

(b) $\mathbb{J}_k^0/k^\times$ is compact.

(c) The compactness of $\mathbb{J}_k^0/k^\times$ implies the finiteness of class number and the S-unit theorem. In particular, the Dirichlet unit theorem follows from the compactness of $\mathbb{J}_k^0/k^\times$. Recall the S-unit theorem :
Let k be a number field, S a finite set of places of k containing all infinite places, $s = \#S$, $k_S^\times = \{x \in k \mid \|x\|_v = 1 \text{ for all } v \notin S\}$. Then $k_S^\times / \left\{ \begin{smallmatrix} \text{roots of} \\ \text{unity} \end{smallmatrix} \right\}$ is free of rank $s-1$.

For the rest of this section, one can refer to :

Chapter XV of [C], Chapter III of [GGP] or Chapter VII of [W].

1^0 Normalization of additive Haar measures for local fields :

$$\begin{aligned} d\alpha &= \text{the usual Lebesgue measure for } k_v = \mathbb{R}, \\ d\alpha &= \text{twice the usual Lebesgue measure for } k_v = \mathbb{C}, \\ d\alpha &= \text{that measure for which } \mathcal{O}_v \text{ gets } (N\delta_v)^{-\frac{1}{2}} \text{ for } v < \infty. \end{aligned}$$

(Here $\mathcal{O}_v = \mathcal{O}_{k_v}$ for simplicity, and δ_v is the absolute local different of k_v.)

Note If $v < \infty$ and π is a uniformizer of k_v, then

$$\text{measure}(\pi^n \mathcal{O}_v) = q_v^{-n} N\delta_v^{-\frac{1}{2}}$$

and

$$\text{measure}(\mathcal{O}_v) \times \text{measure}(\delta_v^{-1}) = 1.$$

2^0 Normalization of multiplicative Haar measure for local fields :
For $v = \infty$, $d^\times\alpha = d\alpha / \| \ \|_v$.
For $v < \infty$, $d^\times\alpha =$ that measure for which $\mathcal{O}_v^\times$ gets 1.

Put $k_{\mathbb{A}}$ and $\mathbb{J}_k$ " product" measures.

3^0 Additive characters of $k_{\mathbb{A}}$:
For $v = \infty$, $\tau_v(x) = \exp(2\pi i \text{Tr}_{k_v/\mathbb{R}}(x))$.
For $v < \infty$, $\tau_v(x) = \exp(-2\pi i(\text{the fractional part of } \text{Tr}_{k_v/\mathbb{Q}_p}(x)))$,
where v lies over p.

For $x \in k_{\mathbb{A}}$, we put $\tau(x) = \prod_{v \in M_k} \tau_v(x_v)$.

Facts 3 (a) Then the set of all the additive characters (a continous map $\chi: k_{\mathbb{A}} \to \mathbb{C}^{\times}$, $|\chi| \equiv 1$, $\chi(a+b) = \chi(a)\chi(b)$) of $k_{\mathbb{A}}$ is given by

$$\{\tau_a \mid a \in k_{\mathbb{A}},\ \tau_a(x) =: \tau(ax) \text{ for all } x \in k_{\mathbb{A}}\}.$$

This just says that $k_{\mathbb{A}}$ is self-dual *i.e.*, $k_{\mathbb{A}}^{\wedge} = k_{\mathbb{A}}$.
Proof. Theorem 3.2.1 in [T]. ∎

(b) $(k_{\mathbb{A}}/k)^{\wedge} = k$

Proof. Define $\lambda_p: \mathbb{Q}_p \to \mathbb{R}/\mathbb{Z}$ as follows, for each prime p of $\mathbb{Q}$including ∞. If $p = \infty$, then $\lambda_\infty: \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ is the canonical map.

If $p < \infty$, then

$$\lambda_p: \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z} \xrightarrow{(-1)\times} \mathbb{R}/\mathbb{Z},$$

where the middle map is defined by taking the fractional part of each element of $\mathbb{Q}_p$. Put, for $x = (x_v) \in k_{\mathbb{A}}$,

$$\Lambda(x) = \sum_{p \le \infty} \lambda_p\Big(\sum_{v|p} \mathrm{Tr}_{k_v/\mathbb{Q}_p}(x_v)\Big).$$

Then $\tau(x) = \exp(2\pi i \Lambda(x))$ for $x \in k_{\mathbb{A}}$. Now, for $\alpha \in k$,

$$\Lambda(\alpha) = \sum_{p \le \infty} \lambda_p\Big(\sum_{v|p} \mathrm{Tr}_{k_v/\mathbb{Q}_p}(\alpha)\Big) = \sum_{p \le \infty} \lambda_p\big(\mathrm{Tr}_{k/\mathbb{Q}}(\alpha)\big).$$

Thus $\Big(\text{for } \xi \in \mathbb{Q},\ \sum_{p \le \infty} \lambda_p(\xi) \equiv 0 \pmod 1\Big) \implies \Lambda(\alpha) \equiv 0 \pmod 1$ for $\alpha \in k$. But for each fixed prime q, $\sum_p \lambda_p(\xi) = \sum_{p \ne q, \infty} \lambda_p(\xi) + (\lambda_q(\xi) + \xi)$ is a q-adic integer. Thus $(k_{\mathbb{A}}/k)^{\wedge} \supseteq k$, and $(k_{\mathbb{A}}/k)^{\wedge}$ is a vector space over k. Since $k_{\mathbb{A}}/k$ is compact, $(k_{\mathbb{A}}/k)^{\wedge}$ is discrete and hence $\big[(k_{\mathbb{A}}/k)^{\wedge} : k\big] < \infty \implies (k_{\mathbb{A}}/k)^{\wedge} = k$.∎

For an integrable $\mathbb{C}$-valued function f on k_v, define Fourier transform (and its inverse transform) by

$$f^{\wedge}(\xi) = \int_{k_v} f(x)\bar{\tau}_v(x\xi)dx, \quad f^{\vee}(\xi) = \int_{k_v} f(x)\tau_v(x\xi)dx.$$

For integrable functions f on $k_{\mathbb{A}}$,

$$f^{\wedge}(\xi) = \int_{k_{\mathbb{A}}} f(x)\bar{\tau}(\xi x)dx, \quad f^{\vee}(\xi) = \int_{k_{\mathbb{A}}} f(x)\tau(\xi x)dx.$$

Also, for integrable functions f on $k_{\mathbb{A}}/k$, define

$$f^{\wedge}(\xi) = \int_{k_{\mathbb{A}}/k} f(x)\bar{\tau}(x\xi)dx, \quad f^{\vee}(\xi) = \int_{k_{\mathbb{A}}/k} f(x)\tau(x\xi)dx.$$

Definition 3.1 On $k_{\mathbb{A}}$, consider functions φ that are representable as the product $\varphi = \prod_{v \in M_k} \varphi_v$, where the factors φ_v satisfy the following conditions :

(a) For $v = \infty$, φ_v is of C^{∞} and all partial derivatives of φ_v decrease faster than any power of $1 + \|x\|_v$ as $\|x\|_v \to \infty$.

(b) For $v < \infty$, φ_v is compactly supported and locally constant.

(c) For almost all finite places v, φ_v is the characteristic function of $\mathcal{O}_v$.

Such functions will be called elementary functions. Schwartz-Bruhat functions are those ones that are representable as finite linear combinations of elementary functions. $S(k_{\mathbb{A}})$ will be used to denote the set of all Schwartz-Bruhat functions on $k_{\mathbb{A}}$. One can show that for every $\varphi \in S(k_{\mathbb{A}})$,

$$\int_{k_{\mathbb{A}}} |\varphi(a)|da < \infty.$$

Theorem 3.1 (Fourier Inversion Formula) For Schwartz-Bruhat function f on $k_{\mathbb{A}}$ or k_v,

$$f^{\wedge\vee} = f = f^{\vee\wedge}$$

Proof. We just prove the first equality for functions f on $k_{\mathbb{A}}$. Since Fourier inversion Formula holds up to constants, we only need to check this for one non-trivial function, say

$$f = \prod_{v \in M_k} \varphi_v, \quad \text{where} \quad \begin{cases} \varphi_v(\xi) = e^{-\pi\xi^2} \text{ for } v \text{ real}, \\ \varphi_v(\xi) = e^{-2\pi|\xi|^2} \text{ for } v \text{ complex}, \\ \varphi_v = \text{ the characteristic function of } \mathcal{O}_v \text{ for } v < \infty. \end{cases}$$

Now, $(\prod_v \varphi_v)^\wedge = \prod_v \varphi_v^\wedge$ and hence this problem is local.
For v real,

$$\varphi_v^\wedge(\xi) = \int_{-\infty}^{\infty} e^{-\pi x^2 - 2\pi i \xi x} dx = e^{-\pi \xi^2}.$$

For v complex,

$$\begin{aligned}
\varphi_v^\wedge(u+iv) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-2\pi(x^2+y^2)} e^{-4\pi i(xu-yv)} 2dxdy \\
&= 2\left(\int_{-\infty}^{\infty} e^{-2\pi x^2 - 4\pi i u x} dx\right)\left(\int_{-\infty}^{\infty} e^{-2\pi y^2 + 4\pi i v y} dy\right) \\
&= \left(\int_{-\infty}^{\infty} e^{-\pi x^2 - 2\pi i(\sqrt{2}u)x} dx\right)\left(\int_{-\infty}^{\infty} e^{-\pi y^2 + 2\pi i(\sqrt{2}v)y} dy\right) \\
&= e^{-2\pi(u^2+v^2)}.
\end{aligned}$$

For $v < \infty$,

$$\varphi_v^\wedge(\xi) = \int_{\mathcal{O}_v} \bar{\tau}_v(x\xi)dx.$$

Now, if $\xi \in \mathcal{O}_v^*$, then

$$\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\xi x) \in \mathbb{Z}_p \text{ for all } x \in \mathcal{O}_v \implies \varphi_v^\wedge(\xi) = \mathrm{measure}(\mathcal{O}_v).$$

If $\xi \notin \mathcal{O}_v^*$, then there exists $x_0 \in \mathcal{O}_v$ such that $\mathrm{Tr}_{k_v/\mathbb{Q}_p}(\xi x_0) \notin \mathbb{Z}_p$ *i.e.*,

$$c = e^{-2\pi i \lambda_p(Tr_{k_v/\mathbb{Q}_p}(\xi x_0))} \neq 1 \implies \varphi_v^\wedge(\xi) = c\varphi_v^\wedge(\xi).$$

by replacing x by $x + x_0 \quad \implies \quad \varphi_v^\wedge(\xi) = 0$.
Thus $\varphi_v^\wedge$ = the characteristic function of $\mathcal{O}_v^* \times \mathrm{measure}(\mathcal{O}_v)$.
It only remains to compute $\varphi_v^{\wedge\vee}(\xi)$. But we see that

$$\begin{aligned}
\varphi_v^{\wedge\vee}(\xi) &= \int_{\mathcal{O}_v^*} \tau_v(x\xi)dx \\
&= (\text{the characteristic function of } \mathcal{O}_v) \\
&\qquad \times \mathrm{measure}(\mathcal{O}_v^*) \times \mathrm{measure}(\mathcal{O}_v).
\end{aligned}$$

Since $\mathrm{measure}(\mathcal{O}_v) \times \mathrm{measure}(\mathcal{O}_v^*) = 1$, $\varphi_v^{\wedge\vee} = \varphi_v$. ∎

Theorem 3.2 (Poisson Summation Formula) For a Schwartz-Bruhat function f on $k_{\mathbb{A}}$,

$$\sum_{\xi \in k} f(\xi) = \sum_{\xi \in k} f^\wedge(\xi).$$

Proof. Consider the function $\varphi(x) = \sum_{v \in k} f(x+v)$. Then this is a function on $k_{\mathbb{A}}/k$ which can be expanded as a Fourier series :

$$\varphi(x) = \sum_{v \in k} \tau(xv) \int_{k_{\mathbb{A}}/k} \varphi(u)\bar{\tau}(uv)du.$$

Thus for $x = 0$,

$$\sum_{v \in k} f(v) = \varphi(0) = \sum_{v \in k} \int_{k_{\mathbb{A}}/k} \varphi(u)\bar{\tau}(uv)du.$$

Now,

$$\begin{aligned} \int_{k_{\mathbb{A}}/k} \varphi(u)\bar{\tau}(uv)du &= \int_{k_{\mathbb{A}}/k} \sum_{\xi \in k} f(u+\xi)\bar{\tau}(uv)du \\ &= \int_{k_{\mathbb{A}}} f(u)\bar{\tau}(uv)du = f^{\wedge}(v). \end{aligned}$$

And $\sum_{v \in k} f(v) = \sum_{v \in k} f^{\wedge}(v)$. ∎

Corollary 3.1 For a Schwartz-Bruhat function f on $k_{\mathbb{A}}$, and for $\lambda \in \mathbb{J}_k$,

$$\sum_{v \in k} f(\lambda v) = \frac{1}{\|\lambda\|} \sum_{v \in k} f^{\wedge}(\lambda^{-1}v).$$

Proof. For g on $k_{\mathbb{A}}$ defined by $g(x) = f(\lambda x)$, we only need to see

$$g^{\wedge}(x) = \frac{1}{\|\lambda\|} f^{\wedge}(\lambda^{-1}x).$$

Indeed,

$$\begin{aligned} g^{\wedge}(\xi) &= \int_{k_{\mathbb{A}}} g(x)\bar{\tau}(\xi x)dx = \int_{k_{\mathbb{A}}} f(\lambda x)\bar{\tau}(\xi x)dx \\ &= \|\lambda\|^{-1} \int_{k_{\mathbb{A}}} f(x)\bar{\tau}(\xi\lambda^{-1}x)dx = \|\lambda\|^{-1} f^{\wedge}(\lambda^{-1}\xi). \end{aligned}$$

∎

Example 3.1 ***[The Mellin Transform of Schwartz-Bruhat Functions] The Tate Formula*** : Let π be a quasi-character of $\mathbb{J}_k$ *i.e.*, a continuous multiplicative mapping of $\mathbb{J}_k$ into $\mathbb{C}^{\times}$. Then $\pi = \prod_{v \in M_k} \pi_v$, where π_v is a quasi-character of $k_v^{\times}$ and unramified *i.e.*, π_v is trivial on $\mathcal{O}_v^{\times}$, for almost all finite v. Conversely, if π_v is a quasi-character of $k_v^{\times}$ which is unramified for almost all finite v, then $\prod_{v \in M_k} \pi_v$ is a quasi-character of $\mathbb{J}_k$.

One can show that if π is a quasi-character of $\mathbb{J}_k$ which is trivial on $k^\times$, then $\pi(\lambda) = \theta(\lambda)\|\lambda\|^s$ for some $s \in \mathbb{C}$ and a Grössencharacter (also called Hecke character) θ *i.e.*, $\theta = \prod_{v \in M_k} \theta_v$, where θ_v is a character of $k_v^\times$ such that

(1) θ_v is unramified for almost all v,

(2) $\theta(\lambda) = \prod_{v \in M_k} \theta_v(\lambda) = 1$, for $\lambda \in k^\times$.

i.e., a continuous homomorphism θ of $\mathbb{J}_k$ into $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ such that

(1) $\theta(\lambda) = 1$ for $\lambda \in k^\times$,

(2) There is a finite set S of places of k contaning infnite places such that $\theta(\lambda) = 1$ if $\lambda_v = 1$ for $v \in S$ and $|\lambda_v|_v = 1$ for $v \notin S$.

Fix a Schwartz-Bruhat function φ on $k_{\mathbb{A}}$.
For a quasi-character π on $\mathbb{J}_k/k^\times$, define the "Mellin Transform" of φ by

$$\Phi(\pi) = \int_{\mathbb{J}_k} \varphi(\lambda)\pi(\lambda)d^\times\lambda,$$

where $d^\times\lambda$ is the product measure of the previously normalized measures on $k_v^\times$. If $\pi = \theta\| \ \|^s$ for a Grössencharacter θ and $s \in \mathbb{C}$, then we also write

$$\Phi(\pi) = \Phi(\theta, s) = \int_{\mathbb{J}_k} \varphi(\lambda)\theta(\lambda)\|\lambda\|^s d^\times\lambda.$$

We will confine ourselves to elementary functions φ. Then

$$\Phi(\theta, s) = \prod_{v \in M_k} \int_{k_v^\times} \varphi_v(\lambda_v)\theta_v(\lambda_v)|\lambda_v|_v^s d^\times\lambda_v.$$

Clearly, each factor of this product converges for $\mathrm{Re}(s) > 0$. For almost all finite places v, $\theta_v(\lambda_v) = |\lambda_v|_v^{it_v}$ for some $t_v \in \mathbb{R}$ and φ_v is the characteristic function of $\mathcal{O}_v$. For such a place v,

$$\int_{k_v^\times} \varphi_v(\lambda_v)\theta_v(\lambda_v)|\lambda_v|_v^s d^\times\lambda_v = \sum_{n=0}^{\infty} \left(q_v^{-(s+it_v)}\right)^n = \frac{1}{1 - q_v^{-(s+it_v)}}.$$

Since $\prod_{v<\infty}\left(1-q_v^{-(s+it_v)}\right)^{-1}$ is absolutely convergent for $\mathrm{Re}(s)>1$, $\Phi(\theta,s)$ defines an analytic function of s in the domain $\mathrm{Re}(s)>1$ for fixed φ and θ. Split $\Phi(\theta,s)$ into the sum of two integrals :

$$\Phi(\theta,s)=\Phi^{+}(\theta,s)+\Phi^{-}(\theta,s),$$

where

$$\Phi^{+}(\theta,s)=\int_{\|\lambda\|\geq 1}\varphi(\lambda)\theta(\lambda)\|\lambda\|^{s}d^{\times}\lambda,$$

$$\Phi^{-}(\theta,s)=\int_{\|\lambda\|\leq 1}\varphi(\lambda)\theta(\lambda)\|\lambda\|^{s}d^{\times}\lambda.$$

Observe that $\Phi^{+}(\theta,s)$ is an entire function of s. Let E be a fundamental domain of $\{\lambda\in\mathbb{J}_k \mid \|\lambda\|\leq 1\}$ relative to $k^{\times}$. Then

$$\Phi^{-}(\theta,s)=\int_{E}\sum_{\alpha\in k^{\times}}\varphi(\lambda\alpha)\theta(\lambda)\|\lambda\|^{s}d^{\times}\lambda.$$

By the Poisson summation formula,

$$\sum_{\alpha\in k}\varphi(\lambda\alpha)=\frac{1}{\|\lambda\|}\sum_{\alpha\in k}\varphi^{\wedge}(\lambda^{-1}\alpha)$$

i.e.,
$$\sum_{\alpha\in k^{\times}}\varphi(\lambda\alpha)=\frac{1}{\|\lambda\|}\varphi^{\wedge}(0)-\varphi(0)+\frac{1}{\|\lambda\|}\sum_{\alpha\in k^{\times}}\varphi^{\wedge}(\lambda^{-1}\alpha)$$

and hence

$$\begin{aligned}\Phi^{-}(\theta,s) &= \int_{E}\sum_{\alpha\in k^{\times}}\varphi^{\wedge}(\lambda^{-1}\alpha)\theta(\lambda)\|\lambda\|^{s-1}d^{\times}\lambda\\ &\quad+\varphi^{\wedge}(0)\int_{E}\theta(\lambda)\|\lambda\|^{s-1}d^{\times}\lambda-\varphi(0)\int_{E}\theta(\lambda)\|\lambda\|^{s}d^{\times}\lambda,\end{aligned}$$

where the first term is

$$\int_{\|\lambda\|\geq 1}\varphi^{\wedge}(\lambda)\theta(\lambda)^{-1}\|\lambda\|^{1-s}d^{\times}\lambda=\Phi^{\wedge+}(\theta^{-1},1-s)$$

and $\Phi^{\wedge}$ is the Mellin transform of $\varphi^{\wedge}$. Now, if θ is not trivial on $\mathbb{J}_k^0$, then

$$\int_{E}\theta(\lambda)\|\lambda\|^{s-1}d^{\times}\lambda=0=\int_{E}\theta(\lambda)\|\lambda\|^{s}d^{\times}\lambda.$$

Otherwise, we may assume that $\theta = 1$ and

$$\int_E \|\lambda\|^s d^\times\lambda = \mathrm{vol}(\mathbb{J}_k^0/k^\times)\int_0^1 t^s dt/t = \mathrm{vol}(\mathbb{J}_k^0/k^\times)\frac{1}{s},$$

where $\mathrm{vol}(\mathbb{J}_k^0/k^\times) = 2^{r_1}(2\pi)^{r_2}hR/w$ and

$$\begin{cases} r_1 & : \text{the number of real embeddings,} \\ r_2 & : \text{the number of complex embeddings,} \\ h & : \text{the class number of } k, \\ R & : \text{the regulator of } k, \\ d & : \text{the absolute discriminant of } k, \\ w & : \text{the number of roots of unity in } k. \end{cases}$$

Thus

$$\Phi^-(\theta, s) = \Phi^{\wedge +}(\theta^{-1}, 1-s) + \varepsilon_\theta\left(\frac{\varphi^\wedge(0)}{s-1} - \frac{\varphi(0)}{s}\right),$$

where $$\varepsilon_\theta = \begin{cases} 0 & \text{if } \theta \text{ is not trivial on } \mathbb{J}_k^0, \\ 2^{r_1}(2\pi)^{r_2}hR/w. \end{cases}$$

Thus $\Phi(\theta, s)$ (defined for $\mathrm{Re}(s) > 1$) admits an analytic continuation to an entire function of s, unless θ is trivial, in which case it has singularities at $s = 0, 1$ with their respective residues $-\varepsilon_\theta\varphi(0)$, $\varepsilon_\theta\varphi^\wedge(0)$. Moreover,

$$\Phi(\theta, s) = \Phi^+(\theta, s) + \Phi^{\wedge +}(\theta^{-1}, 1-s) + \varepsilon_\theta\left(\frac{\varphi^\wedge(0)}{s-1} - \frac{\varphi(0)}{s}\right)$$

yields the functional equation (Tate's formula) :

$$\Phi(\theta, s) = \Phi^\wedge(\theta^{-1}, 1-s).$$

As an illustration, choose $\varphi = \prod_{v \in M_k} \varphi_v$, where

$$\begin{cases} \varphi_v(x) = e^{-\pi x^2} \text{ for } v \text{ real}, \\ \varphi_v(x) = \frac{1}{2\pi}e^{-2\pi|x|^2} \text{ for } v \text{ complex}, \\ \varphi_v = \text{ the characteristic function of } \mathcal{O}_v \text{ for } v < \infty. \end{cases}$$

Then for $\theta_0 \equiv 1$,

$$\begin{aligned} \Phi(\theta_0, s) &= \left(\int_{\mathbb{R}^\times} e^{-\pi x^2}|x|^{s-1}dx\right)^{r_1}\left(\frac{1}{\pi}\int_{\mathbb{C}^\times} e^{-2\pi|z|^2}|z|^{2(s-1)}dz\right)^{r_2} \\ &\quad \times \prod_{v<\infty}\left(\int_{|\lambda_v|\le 1}|\lambda_v|^s d^\times\lambda_v\right) \\ &= \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{r_1}\left((2\pi)^{-s}\Gamma(s)\right)^{r_2}\zeta_k(s), \end{aligned}$$

where $\zeta_k(s)$ is the Dedekind zeta function of k.
By the computation in the proof of the Fourier inversion formula,

$$\varphi^{\wedge} = \prod_{v \in M_k} \varphi_v^{\wedge},$$

where $\begin{cases} \varphi_v^{\wedge} = \varphi_v \text{ for } v \text{ real and complex,} \\ \varphi_v^{\wedge} = \text{measure}(\mathcal{O}_v) \times \text{the characteristic function of } \mathcal{O}_v^*. \end{cases}$

Thus we see that

$$\Phi^{\wedge}(\theta_0, s) = \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left((2\pi)^{-s}\Gamma(s)\right)^{r_2} |d|^{s-\frac{1}{2}}\zeta_k(s).$$

Thus $|d|^{\frac{s}{2}} \left(\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left((2\pi)^{-s}\Gamma(s)\right)^{r_2} \zeta_k(s)$ is invariant under $s \longleftrightarrow 1-s$ and admits an analytic continuation to $\mathbb{C}$, with simple poles at $s = 0, 1$ (respective residues are $-2^{r_1}hR/w$, $2^{r_1}hR/w$) as their only singularities.

3.2 Comparison of Classical and Adelic View Points.

Proposition 3.1 Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})^m$, $\kappa \in \mathbb{Z}^m$. Then there is a one to one correspondence between

$$\{ f \in \mathfrak{H}^m \mid f|_{\kappa}\gamma = f, \ \forall \gamma \in \Gamma \}$$

and $$\left\{ \varphi \in \mathrm{SL}_2(\mathbb{R})^m : \begin{array}{c} \varphi(\gamma g k(\theta)) = \varphi(g)e^{i\kappa\theta} \text{ for } \gamma \in \Gamma, \\ g \in \mathrm{SL}_2(\mathbb{R})^m, \ k(\theta) \in \mathrm{SO}(2)^m \end{array} \right\},$$

where for $\theta = (\theta_1, \ldots, \theta_m) \in \mathbb{R}^m$, $k(\theta)$ denotes

$$\left(\begin{pmatrix} \cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & \cos\theta_1 \end{pmatrix}, \ldots, \begin{pmatrix} \cos\theta_m & \sin\theta_m \\ -\sin\theta_m & \cos\theta_m \end{pmatrix} \right) \in \mathrm{SO}(2)^m.$$

Proof. For such a function f on $\mathfrak{H}^m$, define the function $f^{\natural}$ on $\mathrm{SL}_2(\mathbb{R})^m$ by

$$f^{\natural}(g) = f(g(i))\mu(g, i)^{-\kappa} \qquad \text{for } g \in \mathrm{SL}_2(\mathbb{R})^m.$$

Then

$$\begin{aligned} f^\natural(\gamma g k(\theta)) &= f(\gamma g(i))\mu(\gamma g k(\theta), i)^{-\kappa} \\ &= (f|_\kappa \gamma)(g(i))\mu(\gamma, g(i))^\kappa \mu(\gamma g k(\theta), i)^{-\kappa} \\ &= f(g(i))\mu(g, i)^{-\kappa} e^{i\kappa\theta} \\ &= f^\natural(g) e^{i\kappa\theta}. \end{aligned}$$

Conversely, for such a function φ on $\mathrm{SL}_2(\mathbb{R})^m$, define $\varphi^\natural$ on $\mathfrak{H}^m$ by

$$\varphi^\natural(x+iy) = y^{-\frac{\kappa}{2}} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & 0 \\ 0 & y^{-\frac{1}{2}} \end{pmatrix}\right),$$

for $x \in \mathbb{R}^m$, $y \in (0,\infty)^m$. Let $z = x + iy$, $\gamma(z) = x_1 + iy_1$, for a fixed $\gamma \in \Gamma$. Then

$$\gamma\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}} \end{pmatrix}(i) = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}} \end{pmatrix}(i),$$

and hence

$$\gamma\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}} \end{pmatrix} k(\theta) = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}} \end{pmatrix}$$

for some $\theta \in \mathbb{R}^m$. Then

$$\begin{aligned} \left(\varphi^\natural|_\kappa \gamma\right)(z) &= \varphi^\natural(\gamma(z))\mu(\gamma, z)^{-\kappa} \\ &= y_1^{-\frac{\kappa}{2}} \varphi\left(\gamma\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}} \end{pmatrix} k(\theta)\right)\mu(\gamma, z)^{-\kappa} \\ &= y_1^{-\frac{\kappa}{2}} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}} \end{pmatrix}\right) e^{i\kappa\theta}\mu(\gamma, z)^{-\kappa} \\ &= \varphi^\natural(z) y_1^{-\frac{\kappa}{2}} y^{\frac{\kappa}{2}} e^{i\kappa\theta}\mu(\gamma, z)^{-\kappa}. \end{aligned}$$

But

$$\begin{aligned} \mu(\gamma, z) &= \mu\Big(\gamma, \gamma^{-1}\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}} \end{pmatrix} i\Big) \\ &= \mu\Big(\gamma^{-1}\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}} \end{pmatrix} k(-\theta), i\Big)^{-1} \\ &\quad \times \mu\Big(\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}} \end{pmatrix} k(-\theta), i\Big) \end{aligned}$$

$$
\begin{aligned}
&= \mu\Big(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y^{\frac{1}{2}} & \\ & y^{-\frac{1}{2}}\end{pmatrix}, i\Big)^{-1} \\
&\quad \times \mu\Big(\begin{pmatrix}1 & x_1\\ 0 & 1\end{pmatrix}\begin{pmatrix}y_1^{\frac{1}{2}} & \\ & y_1^{-\frac{1}{2}}\end{pmatrix}, i\Big)\mu(k(-\theta), i) \\
&= y^{\frac{1}{2}} y_1^{-\frac{1}{2}} e^{i\theta}.
\end{aligned}
$$

Thus $\varphi^{\natural}|_{\kappa}\gamma = \varphi$, for all $\gamma \in \Gamma$.
Now, it is easy to see that $(f^{\sharp})^{\natural} = f$, $(\varphi^{\natural})^{\sharp} = \varphi$. ∎

Remark 3.1 (a) It is useful to observe that every element $g \in \mathrm{SL}_2(\mathbb{R})^m$ can be written, in a multi-index notation, as

$$
g = \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y^{\frac{1}{2}} & 0\\ 0 & y^{-\frac{1}{2}}\end{pmatrix} k(\theta),
$$

for unique $x \in \mathbb{R}^m$, $y \in (0,\infty)^m$, $k(\theta) \in \mathrm{SO}(2)^m$.

(b) Let F be any number field, with ring of integers $\mathcal{O}$, adeles $\mathbb{A}$, ideles $\mathbb{J}$. For any commutative $\mathcal{O}$-algebra R, put

$$
\begin{aligned}
\mathrm{GL}_2(R) &= \{\, g \in M_2(R) \mid \det g \in R^{\times} \,\}, \\
P(R) &= \{\, g \in \mathrm{GL}_2(R) \mid g \text{ is upper triagular} \,\}, \\
U(R) &= \left\{ u(x) = \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \middle| \, x \in R \right\}, \\
T(R) &= \left\{ \ell(y) = \begin{pmatrix}y & 0\\ 0 & 1\end{pmatrix} \middle| \, y \in R^{\times} \right\}, \\
Z(R) &= \left\{ \begin{pmatrix}t & 0\\ 0 & t\end{pmatrix} \middle| \, t \in R^{\times} \right\}.
\end{aligned}
$$

Note that

$$
\begin{aligned}
&\mathrm{GL}_2(\mathbb{A}) = \{\, g \in M_2(\mathbb{A}) : \det g \in \mathbb{J} \,\} \\
&= \Big\{ g{=}(g_v) \in \prod_{v \le \infty} \mathrm{GL}_2(F_v) : g_v \in K_v \text{ for almost all finite places } v \Big\},
\end{aligned}
$$

where we put $K_v = \begin{cases} \mathrm{GL}_2(\mathcal{O}_v) & , \text{ for } v < \infty \\ \mathrm{SO}(2) & , \text{ for } v \text{ real} \\ \mathrm{SU}(2) & , \text{ for } v \text{ complex.} \end{cases}$

Take subsets of the form

$$\left\{ U = \prod_{v \leq \infty} U_v \,\middle|\, \begin{array}{c} U_v \subset \mathrm{GL}_2(F_v) \text{ is open and } U_v = K_v \\ \text{for almost all finite places } v \end{array} \right\}$$

as a neighborhood base of 1 for the topology of $\mathrm{GL}_2(\mathbb{A})$.

Remark 3.2 (a) For any place v, we have the Iwasawa decomposition

$$\mathrm{GL}_2(F_v) = P(F_v)K_v = U(F_v)(\mathrm{Z}(F_v)\mathrm{T}(F_v))K_v$$

and the Cartan decomposition

$$\mathrm{GL}_2(F_v) = K_v(\mathrm{Z}(F_v)\mathrm{T}(F_v))K_v.$$

(b) Similarly, one can define $\mathrm{SL}_2(\mathbb{A})$ and more generally the adele group $G(\mathbb{A})$ can be defined for any linear algebraic group G defined over F.

(c) For a general discussion about strong approximation, the reader is referred to [KN]. For a number field F, G a linear algebraic group defined over F, $G(\mathbb{A})$ the adele group, $G(F)(\subset G(\mathbb{A}))$ the F-rational points of G, the S-component $G_S(\subset G(\mathbb{A})) = \prod_{v \in S} G(F_v)$ for S a finite set of places of F. The problem of strong approximation is as follows :

Under what conditions on G and S is $\mathrm{G}_S\mathrm{G}(F)$ dense in $G(\mathbb{A})$?
As a special case of the strong approximation theorem for SL_n, we have :

$$\mathrm{SL}_n(F)\mathrm{SL}_n(F_\infty) \text{ is dense in } \mathrm{SL}_n(\mathbb{A}),$$

where $F_\infty = \prod_{v=\infty} F_v$. [1] Note that the above assertion is not true for SL_n replaced by GL_n. Indeed, recall the fundamental exact sequence from the global class field theory :

$$1 \longrightarrow \overline{F^\times F_{\infty+}^\times} \longrightarrow \mathbb{J}_F \longrightarrow \mathrm{Gal}(F_{ab}/F) \longrightarrow 1,$$

where $F_{\infty+}^\times$ denotes the connected component of the identity element of $F_\infty^\times$ and F_{ab} is the maximal abelian extension of F.

[1] *cf. Appendix A.3 of [G1].*

(d) Let F be a totally real number field. If Γ is a congruence subgroup of $\mathrm{SL}_2(F)$, then there is a compact open subgroup $\boldsymbol{K}$ of $\mathrm{SL}_2(\mathbb{A}_0)$ such that $\Gamma = \mathrm{SL}_2(F) \bigcap \mathrm{SL}_2(F_\infty)K$, where $\mathbb{A}_0$ is the finite adeles of F.
Conversely, if $\boldsymbol{K}$ is such, then $\Gamma = \mathrm{SL}_2(F) \bigcap \mathrm{SL}_2(F_\infty)K$ is a congruence subgroup of $\mathrm{SL}_2(F)$.

Proposition 3.2 For any Γ and $\boldsymbol{K}$ just as above,

$$\Gamma\backslash \mathrm{SL}_2(F_\infty) \approx \mathrm{SL}_2(F)\backslash \mathrm{SL}_2(\mathbb{A})/K$$

is a homeomorphism under $\Gamma g \mapsto \mathrm{SL}_2(F)gK$.

Proof. This is well-defined, since

$$\begin{aligned} & \Gamma g = \Gamma g' \\ \Longrightarrow \quad & g = \gamma g' \text{ for some } \gamma \in \mathrm{SL}_2(F_\infty) \text{ and } \gamma k \in \mathrm{SL}_2(F) \text{ for some } k \in K \\ \Longrightarrow \quad & g = \gamma k g' k^{-1} \implies \mathrm{SL}_2(F)gK = \mathrm{SL}_2(F)g'K. \end{aligned}$$

Suppose that $\gamma gk = g'$ for $\gamma \in \mathrm{SL}_2(F)$, $g, g' \in \mathrm{SL}_2(F_\infty)$, $k \in K$. Then for each finite place v, the v-component of γk is 1_2 *i.e.*,

$$\gamma \in \mathrm{SL}_2(F) \bigcap \mathrm{SL}_2(F_\infty)K = \Gamma.$$

This implies that $\gamma g = g'$ inside $\mathrm{SL}_2(F_\infty)$ and hence that the map is injective. Since $\mathrm{SL}_2(F_\infty)K$ is open in $\mathrm{SL}_2(\mathbb{A})$, by the strong approximation theorem

$$\mathrm{SL}_2(\mathbb{A}) = \mathrm{SL}_2(F)\mathrm{SL}_2(F_\infty)(\mathrm{SL}_2(F_\infty)K) = \mathrm{SL}_2(F)\mathrm{SL}_2(F_\infty)K.$$

This implies that the map is surjective. ∎

Corollary 3.2 There is a one to one correspondence between

$$\left\{ \varphi \,\middle|\, \begin{array}{c} \varphi \text{ is a function on } \mathrm{SL}_2(\mathbb{R})^m \text{ and } \varphi(\gamma g k(\theta)) = \varphi(g)e^{i\kappa\theta}, \\ \text{for } \gamma \in \Gamma,\ g \in \mathrm{SL}_2(\mathbb{R})^m,\ k(\theta) \in \mathrm{SO}(2)^m \end{array} \right\}$$

and

$$\left\{ \psi \,\middle|\, \begin{array}{l} \psi \text{ is a function on } \mathrm{SL}_2(\mathbb{A}) \text{ such that it is left } \mathrm{SL}_2(F)\text{-invariant,} \\ \text{right } \boldsymbol{K}\text{-invariant, and right } \mathrm{SO}(2)^m\text{-equivariant by } k(\theta) \mapsto e^{i\kappa\theta} \end{array} \right\}.$$

Proof. For such a φ, define the function $\varphi^\sharp$ on $\mathrm{SL}_2(\mathbb{A})$ by $\varphi^\sharp(\gamma g k) = \varphi(g)$, for $\gamma \in \mathrm{SL}_2(F)$, $g \in \mathrm{SL}_2(F_\infty)$, $k \in K$. Then it is well-defined (in view of the above homeomorphism) and satisfies the required invariance and equivariance properties. Conversely, if ψ is such a function, then define the function $\psi^\natural$ on $\mathrm{SL}_2(\mathbb{R})^m$ as the restriction $\psi^\natural = \psi|_{SL_2(F_\infty)}$. ∎

For a nonzero ideal $\mathfrak{n}$ of $\mathcal{O}$, define

$$\begin{aligned}
K(\mathfrak{n}) &= \{\gamma \in \mathrm{SL}_2(\hat{\mathcal{O}}) \mid \gamma \equiv 1_2 \text{ modulo } \mathfrak{n}\},\\
K_{00}(\mathfrak{n}) &= \left\{\gamma \in \mathrm{SL}_2(\hat{\mathcal{O}}) \middle| \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } b \equiv c \equiv 0 \bmod \mathfrak{n}\right\},\\
\widetilde{K}(\mathfrak{n}) &= \{\gamma \in \mathrm{GL}_2(\hat{\mathcal{O}}) \mid \gamma \equiv 1_2 \text{ modulo } \mathfrak{n}\},\\
\widetilde{K}_{00}(\mathfrak{n}) &= \left\{\gamma \in \mathrm{GL}_2(\hat{\mathcal{O}}) \middle| \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } b \equiv c \equiv 0 \bmod \mathfrak{n}\right\}.
\end{aligned}$$

Proposition 3.3 There is a homeomorphism :

$$\mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/\widetilde{K}_{00}(\mathfrak{n}) \approx \coprod_\xi \mathrm{Z}(F_\infty)\Gamma_\xi \backslash \mathrm{GL}_2^+(F_\infty),$$

where ξ runs over a finite set X of elements of $\mathrm{GL}_2(\mathbb{A})$ so that $\{\det\xi : \xi \in X\}$ forms a set of representatives for the narrow ideal class group $\mathbb{J}/F_{\infty+}^\times F^\times \hat{\mathcal{O}}^\times$ and Γ_ξ is the discrete subgroup of $\mathrm{GL}_2^+(F_\infty)$ given by

$$\Gamma_\xi = \mathrm{GL}_2^+(F) \bigcap \mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n})\xi^{-1}.$$

Proof. Define the map

$$\imath : \coprod_\xi \mathrm{Z}(F_\infty)\Gamma_\xi\backslash \mathrm{GL}_2^+(f_\infty) \to \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/\widetilde{K}_{00}(\mathfrak{n})$$

by $$\imath(\mathrm{Z}(F_\infty)\Gamma_\xi g) = \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)g\xi\widetilde{K}_{00}(\mathfrak{n}).$$

This is well–defined, since $\mathrm{Z}(F_\infty)\Gamma_\xi g = \mathrm{Z}(F_\infty)\Gamma_\xi g'$ implies that $g = z\gamma g'$ for some $z \in \mathrm{Z}(F_\infty)$, $\gamma \in \mathrm{GL}_2^+(F_\infty)$ and $\gamma\xi k\xi^{-1} \in \mathrm{GL}_2^+(F)$ for some $k \in \widetilde{K}_{00}(\mathfrak{n})$. Then

$$g\xi = z\gamma\xi k\xi^{-1}g'\xi k^{-1} \Longrightarrow \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)g\xi\widetilde{K}_{00}(\mathfrak{n}) = \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)g'\xi\widetilde{K}_{00}(\mathfrak{n}).$$

Moreover, $\bigcup_\xi \imath\Big(\mathrm{Z}(F_\infty)\Gamma_\xi\backslash \mathrm{GL}_2^+(F_\infty)\Big) = \bigcup_\xi \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n})$.

By the strong approximation theorem,

$$\mathrm{SL}_2(\mathbb{A}) = \mathrm{SL}_2(F)\mathrm{SL}_2(F_\infty)\xi K_{00}(\mathfrak{n})\xi^{-1}$$

and hence

$$\mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{SL}_2(\mathbb{A})\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n}) = \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n}).$$

Also, we see that $\bigcup_\xi \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{SL}_2(\mathbb{A})\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n}) = \mathrm{GL}_2(\mathbb{A})$, by taking determinants. Thus $\imath$ is surjective.
Since $\bigcup_\xi \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n})$ is a disjoint union, it is enough to show that

$$\begin{array}{rcl} \mathrm{Z}(F_\infty)\Gamma_\xi\backslash\mathrm{GL}_2^+(F_\infty) & \longrightarrow & \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n}) \\ \Big(\ \mathrm{Z}(F_\infty)\Gamma_\xi g & \mapsto & \mathrm{Z}(F_\infty)\mathrm{GL}_2(F)g\xi\widetilde{K}_{00}(\mathfrak{n})\Big) \end{array}$$

is injective. Suppose that $g'\xi = z\gamma g\xi k$, for $g, g' \in \mathrm{GL}_2^+(F_\infty)$, $z \in \mathrm{Z}(F_\infty)$, $\gamma \in \mathrm{GL}_2(F)$, $k \in \widetilde{K}_{00}(\mathfrak{n})$. Then

$$\gamma \in \mathrm{GL}_2(F)\bigcap\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n})\xi^{-1} = \Gamma_\xi,$$

since $\gamma = z^{-1}g'(\xi k^{-1}\xi^{-1})g^{-1} = z^{-1}g'g^{-1}(\xi k^{-1}\xi^{-1})$.
Thus inside $\mathrm{GL}_2^+(F_\infty)$, $g' = z\gamma g$. ∎

Corollary 3.3 $\mathrm{Z}(F_\infty)\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\widetilde{K}_{00}(\mathfrak{n})\mathrm{SO}(2)^m$ is a finite disjoint union of quotients of $\mathfrak{H}^m$ by congruence subgroups. ∎

Fix $\mathfrak{n}$ and $\{\xi\}$ as in the above. Note that

$$\widetilde{K}_{00}(\mathfrak{n}) \to (\mathcal{O}/\mathfrak{n})^\times \bigoplus (\mathcal{O}/\mathfrak{n})^\times \qquad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a \bmod \mathfrak{n},\ d \bmod \mathfrak{n})\right)$$

is an epimorphism with kernel $\widetilde{K}(\mathfrak{n})$. Thus $\widetilde{K}_{00}(\mathfrak{n}) \triangleright \widetilde{K}(\mathfrak{n})$, and $\widetilde{K}_{00}(\mathfrak{n})/\widetilde{K}(\mathfrak{n})$ is finite abelian. Also, if we put

$$\Gamma_{1\xi} =: \mathrm{GL}_2^+(F)\bigcap\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}(\mathfrak{n})\xi^{-1},$$

then

$$\begin{array}{rcl} \Gamma_\xi = \mathrm{GL}_2^+(F)\bigcap\mathrm{GL}_2^+(F_\infty)\xi\widetilde{K}_{00}(\mathfrak{n})\xi^{-1} & \to & \widetilde{K}_{00}(\mathfrak{n})/\widetilde{K}(\mathfrak{n}) \\ \Big(\Gamma_\xi \ni \gamma\xi k\xi^{-1}(\gamma \in \mathrm{GL}_2^+(F_\infty),\ k \in \widetilde{K}_{00}(\mathfrak{n})) & \mapsto & k \bmod \widetilde{K}(\mathfrak{n})\Big) \end{array}$$

is an epimorphism with kernel $\Gamma_{1\xi}$. Thus

$$M(\Gamma_{1\xi}, \kappa) = \bigoplus_{\chi} M(\Gamma_\xi, \kappa, \chi),$$

where

$$M(\Gamma_{1\xi}, \kappa) = \left\{ \begin{array}{c} \text{functions on } \mathrm{GL}_2^+(F_\infty) \text{ which is left} \\ \Gamma_{1\xi} - \text{invariant and of weight } \kappa \end{array} \right\},$$

$$M(\Gamma_\xi, \kappa, \chi) = \left\{ f \in M(\Gamma_{1\xi}, \kappa) \,\middle|\, \begin{array}{c} f(\gamma^{-1}g) = \chi(\gamma) f(g), \\ \text{for } \gamma \in \Gamma_\xi,\ g \in \mathrm{GL}_2^+(F_\infty) \end{array} \right\},$$

and χ runs over the characters of $\Gamma_\xi/\Gamma_{1\xi}$ (viewed as characters on Γ_ξ which are trivial on $\Gamma_{1\xi}$). For a character χ of $\widetilde{K}_{00}(\mathfrak{n})/\widetilde{K}(\mathfrak{n})$, put

$$\widetilde{M}(\mathfrak{n}, \kappa, \chi) = \left\{ \begin{array}{c} \text{functions on} \\ \mathrm{GL}_2(\mathbb{A}) \end{array} \,\middle|\, \begin{array}{c} f \text{ is left } \mathrm{Z}^+\mathrm{GL}_2(F) - \text{invariant, of weight } \kappa, \\ f(gk) = \chi(k) f(g) \text{ for } k \in \widetilde{K}_{00}(\mathfrak{n}) \end{array} \right\},$$

where Z^+ is the connected component of the identity in $\mathrm{Z}(F_\infty)$. Let χ be a character of $\widetilde{K}_{00}(\mathfrak{n})/\widetilde{K}(\mathfrak{n})$ which is trivial on elements of the form

$$\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \in \widetilde{K}_{00}(\mathfrak{n}).$$

Corollary 3.4 Then there is a bijection

$$\imath : \widetilde{M}(\mathfrak{n}, \kappa, \chi) \to \bigoplus_{\xi} M(\Gamma_\xi, \kappa, \chi_\xi) \text{ given by } \imath(f)_\xi(g) = f(g\xi),$$

for $g \in \mathrm{GL}_2^+(F_\infty)$, where $\chi_\xi(\gamma) = \chi(\text{ finite part of } \xi^{-1}\gamma\xi)$.

Proof. For $g \in \mathrm{GL}_2(\mathbb{A})$, g_0, g_∞ denote respectively its finite and infinite part so that $g = g_0 g_\infty = g_\infty g_0$. For $\gamma \in \Gamma_\xi$,

$$\begin{aligned} & \imath(f)_\xi(\gamma^{-1}g) = f(\gamma_\infty^{-1} g\xi) = f(\gamma^{-1} g \gamma_0 \xi) \\ = \ & f(g\gamma_0\xi) = f(g\xi\xi^{-1}\gamma_0\xi) = f(g\xi(\xi^{-1}\gamma\xi)_0) \\ = \ & f(g\xi)\chi((\xi\gamma\xi)_0) = f(g\xi)\chi_\xi(\gamma) = \imath(f)_\xi(g)\chi_\xi(\gamma). \end{aligned}$$

∎

Let $\widetilde{M}(\mathfrak{n}, \kappa, \chi, \omega) = \left\{ f \in \widetilde{M}(\mathfrak{n}, \kappa, \chi) : f\left(\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} g\right) = \omega(t) f(g) \right\}.$

Since $\omega \equiv 1$ on $F_{\infty+}^\times F^\times \{ \alpha \in \hat{\mathcal{O}}^\times : \alpha \equiv 1 (\mathrm{mod}\, \mathfrak{n}) \}$, we can decompose :

Corollary 3.5 $\widetilde{M}(\mathfrak{n},\kappa,\chi)=\bigoplus_{\omega}\widetilde{M}(\mathfrak{n},\kappa,\chi,\omega)$, where ω runs over the characters of the " ray class group $\bmod \mathfrak{n}$" *i.e.*,

$$\mathbb{J}/F_{\infty+}^{\times}F^{\times}\{\alpha\in\hat{\mathcal{O}}^{\times}\mid \alpha\equiv 1(\mathrm{mod}\mathfrak{n})\}. \qquad \blacksquare$$

Remark 3.3 (a) Since χ is trivial on $\begin{pmatrix} t & 0\\ 0 & 1\end{pmatrix}\in\widetilde{K}_{00}(\mathfrak{n})$ and on $\widetilde{K}(\mathfrak{n})$, χ is determined by its values on $Z(\hat{\mathcal{O}}^{\times})$ and hence by ω.

(b) The finite part of the conductor of ω divides $\mathfrak{n}$, since ω is trivial on $\{\alpha\in\hat{\mathcal{O}}^{\times}\mid \alpha\equiv 1(\mathrm{mod}\mathfrak{n})\}$.

Let F be a totally real number field. For a finite place v of F and a Hecke character ω, unramified at v,

$$H=H_{v,\omega}=\left\{\varphi:\mathrm{GL}_2(F_v)\to\mathbb{C}\;\middle|\;\begin{array}{c}\varphi \text{ is continuous, left and right}\\ \mathrm{GL}_2(\mathcal{O}_v)\text{ -invariant, }(Z_v,\omega)\text{-equivariant,}\\ \text{compactly supported mod}Z_v\end{array}\right\}$$

with multiplication given by the (right) convolution

$$(\varphi*\psi)(g)=\int_{Z_v\backslash GL_2(F_v)}\varphi(gh^{-1})\psi(h)dh,$$

where Z_v is the center of $\mathrm{GL}_2(F_v)$ and dh is the Haar measure on $\mathrm{GL}_2(F_v)$ giving $\mathrm{GL}_2(\mathcal{O}_v)$ measure 1.

For $\varphi\in H=H_{v,\omega}$, a right $\mathrm{GL}_2(\mathcal{O}_v)$-invariant, (Z_v,ω)-equivariant, measurable function f on $\mathrm{GL}_2(F_v)$, define

$$(*)\qquad (T_\varphi f)(g)=\int_{Z_v\backslash GL_2(F_v)}f(gh^{-1})\varphi(h)dh.$$

Put

$$V(v,\omega)=\left\{f:\mathrm{GL}_2(\mathbb{A})\to\mathbb{C}\;\middle|\;\begin{array}{c}f \text{ is continuous, left } \mathrm{GL}_2(F)\text{-invariant,}\\ \text{right } \mathrm{GL}_2(\mathcal{O}_v)\text{-invariant, } f(\zeta g)=\omega(\zeta)f(g)\\ \text{for } \zeta\in Z(\mathbb{A}),\text{ and } <f,f><\infty\end{array}\right\},$$

where $V(v,\omega)$ has the inner product given by

$$<f_1,f_2>=\int_{Z(\mathbb{A})GL_2(F)\backslash GL_2(\mathbb{A})}f_1(g)\overline{f_2(g)}\,dg.$$

Then $H=H_{v,\omega}$ acts on $V(v,\omega)$ by the same formula as in $(*)$.

Theorem 3.3 (i) $H = H_{v,\omega}$ is closed under convolution, and the algebra H, with convolution, is commutative.

(ii) The operators T_φ form a commutative ring of bounded operators on $V(v,\omega)$, which is closed under adjoint with respect to $<,>$. In fact, the adjoint of T_φ is T_{φ^*}, with $\varphi^*(g) = \overline{\varphi(g^{-1})}$.

Corollary 3.6 If V is a finite dimensional subspace of $V(v,\omega)$ invariant under the action of $H = H_{v,\omega}$, then V has an orthogonal basis consisting of simultaneous eigenvectors for H.

Proof of Theorem 3.3. Write, for brevity, $G = \mathrm{GL}_2(F_v)$, $Z = Z(F_v)$, $K = \mathrm{GL}_2(\mathcal{O}_v)$ and $A = \{$ diagonal elements of $G\}$.
(i) It is left to the reader to check that H is closed under convolution. We claim that for $f \in H$, $g \in G$ and with $g \mapsto g^\sigma$ the transpose on G, $f(g^\sigma) = f(g)$. With $t \in A$, $k_1, k_2 \in K$, $g = k_1 t k_2$,

$$f(g) = f(k_1 t k_2) = f(t) = f(t^\sigma) = f(k_2^\sigma t^\sigma k_1^\sigma) = f(g^\sigma).$$

By the above claim, for φ, $\psi \in H$,

$$\begin{aligned}
(\varphi * \psi)(g) &= (\varphi * \psi)(g^\sigma) \\
&= \int_{Z\backslash G} \varphi(g^\sigma h^{-1})\psi(h)dh \\
&= \int_{Z\backslash G} \varphi(g^\sigma h)\psi(h^{-1})dh \qquad \text{(replacing } h \text{ by } h^{-1}\text{)} \\
&= \int_{Z\backslash G} \varphi(h)\psi(h^{-1}g^\sigma)dh \qquad \text{(replacing } h \text{ by } g^{\sigma^{-1}}h\text{)} \\
&= \int_{Z\backslash G} \varphi(h^\sigma)\psi(h^{\sigma^{-1}}g^\sigma)dh \qquad \text{(replacing } h \text{ by } h^\sigma\text{)} \\
&= \int_{Z\backslash G} \varphi(h)\psi(gh^{-1})dh \qquad \text{(by the above claim)} \\
&= (\psi * \varphi)(g).
\end{aligned}$$

(ii) Check that T_φ is a bounded operator of $V(v,\omega)$. It is formal to see that for φ, $\psi \in H$, $T_\varphi T_\psi = T_{\varphi * \psi}$ and hence that $T_\varphi T_\psi = T_\psi T_\varphi$ by (i). For a, b in $V(v,\omega)$,

$$< T_\varphi a, b > \;=\; \int T_\varphi(a)(g)\bar{b}(g)dg$$

$$
\begin{aligned}
&= \iint a(gh^{-1})\varphi(h)\bar{b}(g)dhdg \\
&= \iint a(gh^{-1})\varphi(h)\bar{b}(g)dgdh \\
&= \iint a(g)\varphi(h)\bar{b}(gh)dgdh \\
&= \iint a(g)\varphi(h)\bar{b}(gh)dhdg \\
&= \iint a(g)\varphi(h^{-1})\bar{b}(gh^{-1})dhdg \quad \text{(by replacing } h \text{ by } h^{-1}\text{)} \\
&= \int a(g)\overline{\left(\int \overline{\varphi}(h^{-1})b(gh^{-1})dh\right)}dg \\
&= <a, T_{\varphi^*}b>,
\end{aligned}
$$

where g and h are respectively over $Z(\mathbb{A})\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})$ and $Z\backslash G$. ∎

Remark 3.4 Let v, w be distinct finite places of F. If $f \in V(v,\omega)\bigcap V(w,\omega)$, then $T_\psi T_\varphi(f) = T_\varphi T_\psi(f)$, for all $\varphi \in H_{v,\omega}$, $\psi \in H_{w,\omega}$.

Definition 3.2 Let f be a left $\mathrm{GL}_2(F)$-invariant continuous function on $\mathrm{GL}_2(\mathbb{A})$. For $\xi \in F$, the ξ-th Fourier coefficient of f is the function W_ξ on $\mathrm{GL}_2(\mathbb{A})$ given by

$$W_\xi(g) = \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi x)f(u(x)g)dx.$$

Moreover, such an f is called a weak cuspform if $W_0(g) = 0$ for almost every g.

Proposition 3.4 (i) For $u(x) \in U(\mathbb{A})$, $W_\xi(u(x)g) = \tau(\xi x)W_\xi(g)$.

(ii) $f(g) = \sum_{\xi\in F} W_\xi(g)$.

(iii) For $p = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(F)$, $W_\xi(g) = W_{a^{-1}d\xi}(pg)$. In particular, $W_\xi(g) = W_1(\ell(\xi)g)$ for all $0 \neq \xi \in F$.

Proof. (i)

$$\begin{aligned} W_\xi(u(x)g) &= \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi\alpha) f(u(\alpha+x)g)d\alpha \\ &= \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi(\alpha-x)) f(u(\alpha)g)d\alpha \\ &= \tau(\xi x) W_\xi(g). \end{aligned}$$

(ii) For each fixed $g \in \mathrm{GL}_2(\mathbb{A})$, $\varphi(x) = f(u(x)g)$ is a continuous function on $\mathbb{A}$ which is F-invariant. Thus

$$\varphi(x) = \sum_{\xi\in F} \tau(\xi x) \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi\alpha)\varphi(\alpha)d\alpha \qquad i.e.,$$

$$f(u(x)g) = \sum_{\xi\in F} \tau(\xi x) W_\xi(g) = \sum_{\xi\in F} W_\xi(u(x)g)$$

by (i). Thus we have $f(g) = \sum_{\xi\in F} W_\xi(g)$.

$$\begin{aligned} \text{(iii)} \qquad W_{a^{-1}d\xi}(pg) &= \int_{F\backslash\mathbb{A}} \overline{\tau}(a^{-1}d\xi x) f(u(x)pg)dx \\ &= \int_{F\backslash\mathbb{A}} \overline{\tau}(a^{-1}d\xi x) f(u(a^{-1}dx)g)dx \\ &= \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi x) f(u(x)g)dx \quad \text{(by replacing } x \text{ by } ad^{-1}x\text{)} \\ &= W_\xi(g). \end{aligned}$$

■

Remark 3.5 (a) Writing $W = W_1$, we see that

$$f(g) = W_0(g) + \sum_{\xi\in F^\times} W(\ell(\xi)g).$$

(b) Let f be a holomorphic Hilbert modular cuspform of weight κ with respect to $\mathrm{GL}_2^+(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a totally real number field F of narrow class number 1. If $f(z) = \sum_{\substack{\xi\in\mathcal{O}^* \\ \xi\gg 0}} c(\xi)e^{2\pi i Tr(\xi z)}$, then it corresponds to the function φ_0 on $\mathrm{GL}_2^+(F_\infty)$ given by

$$\varphi_0\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}\right) = y^{\frac{\kappa}{2}} \sum_{\substack{\xi\in\mathcal{O}^* \\ \xi\gg 0}} c(\xi)e^{2\pi i Tr(\xi z)} (x \in \mathbb{R}^m,\ y \in (0,\infty)^m)$$

and further to the function φ on $\mathrm{GL}_2(\mathbb{A})$ given by $\varphi(\zeta\gamma gk) = \varphi_0(g)$, for $\zeta \in Z(F_\infty)$, $\gamma \in \mathrm{GL}_2(F)$, $g \in \mathrm{GL}_2^+(F_\infty), k \in \mathrm{GL}_2(\hat{\mathcal{O}})$. Now, for $y \in (0,\infty)^m$, $\xi \in \mathcal{O}^*$ with $\xi \gg 0$,

$$\begin{aligned} W_\xi\left(\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right) &= \int_{F\backslash\mathbb{A}} \overline{\tau}(\xi x)\varphi\left(u(x)\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right) dx \\ &= \int_{\mathcal{O}\backslash\mathbb{R}^m} \overline{\tau}_\infty(\xi x)\varphi_0\left(u(x)\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right) dx \end{aligned}$$

(Recall here that $F\backslash\mathbb{A} = (\mathcal{O}\backslash\mathbb{R}^m) \times \prod_{v<\infty} \mathcal{O}_v$.)

$$\begin{aligned} &= y^{\frac{\kappa}{2}} \sum_{\substack{\xi' \in \mathcal{O}^* \\ \xi' \gg 0}} c(\xi') e^{-2\pi Tr(\xi' y)} \int_{\mathcal{O}\backslash\mathbb{R}^m} e^{2\pi i Tr(\xi' - \xi)x} dx \\ &= c(\xi) y^{\frac{\kappa}{2}} e^{-2\pi Tr(\xi y)} \end{aligned}$$

(where we normalized the Haar measure dx on $\mathbb{A}$ so that $\mathbb{A}/F$ gets total measure 1).

Theorem 3.4 Let $f \in V(v,\omega)$ (for a Hecke character ω, unramified at $v < \infty$) be such that $W_0(g) = 0$ for almost all g, and such that it is an eigenfunction for $H_{v,\omega}$. Let $f(g) = \sum_{\xi \in F^\times} W(\ell(\xi)g)$, and let $\eta \in H_{v,\omega}$ be given by :

$$\eta\left(\mathrm{GL}_2(\mathcal{O}_v)\begin{pmatrix} \alpha & \\ & \alpha \end{pmatrix}\begin{pmatrix} t & \\ & 1 \end{pmatrix}\mathrm{GL}_2(\mathcal{O}_v)\right) = \begin{cases} \omega(\alpha), & \text{for } \mathrm{ord}_v t = -1, \\ 0, & \text{else} \end{cases}.$$

Assume that $T_\eta f = \lambda f$. Then $W(g) = W'(g')W''(g'')$, where g' is the non-v part of $g \in \mathrm{GL}_2(\mathbb{A})$, $g'' \in \mathrm{GL}_2(F_v)$, $g = g'g''$. Moreover, for any $\varepsilon \in \mathcal{O}_v^\times$,

$$W''(\ell(\varepsilon\pi^m\delta)) = \begin{cases} W''(\ell(\delta)) \times (\alpha^m + \alpha^{m-1}\beta + \cdots + \alpha\beta^{m-1} + \beta^m) & , m \geq 0 \\ 0 & , m < 0 \end{cases}$$

where π is a local uniformizer at v, δ a generator for the local inverse different at v, and α, β are the roots of $x^2 - N_v^{-1}\lambda\omega(\pi)x + \omega(\pi)N_v^{-1} = 0$ ($N_v = [\mathcal{O}_v : \pi\mathcal{O}_v]$).

Proof. Since we have the Iwasawa decomposition

$$\mathrm{GL}_2(F_v) = U(F_v)Z(F_v)T(F_v)K_v,$$

and W is left $(U(F_v),\tau)$-equivariant, right K_v-invariant, $(Z(F_v),\omega)$-equivariant, W is completely determined by its values on the elements of the form $g'\ell(y)$. We will show that $W(g'\ell(\delta))$ together with the eigenvalue λ determines W completely. Observe that $T_\eta f = \lambda f$ implies $T_\eta W = \lambda W$.
For $u(x) \in \mathrm{GL}_2(\mathcal{O}_v)$,

$$\begin{aligned} W(g'\ell(y)) &= W(g'\ell(y)u(x)) = W(g'\ell(yx)\ell(y)) \\ &= W(\ell(yx)g'\ell(y)) = \tau_v(yx)W(g'\ell(y)). \end{aligned}$$

This implies that $W(g'\ell(y)) = 0$ if $y \notin \delta\mathcal{O}_v = \mathcal{O}_v^*$. Now,

$$\begin{aligned} \lambda W(g'\ell(y)) &= \int_{Z_v\backslash GL_2(F_v)} W(g'\ell(y)h^{-1})\eta(h)dh \\ &= \int_{Z_v\backslash Z_vK_v\sigma K_v} W(g'\ell(y)h^{-1})\eta(h)dh \\ &= W\left(g'\ell(y)\begin{pmatrix}\pi^{-1} & \\ & 1\end{pmatrix}\right) \\ &\qquad + \sum_{b\in\mathcal{O}_v/\pi\mathcal{O}_v} W\left(g'\ell(y)\begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \\ & \pi^{-1}\end{pmatrix}\right) \\ &= W(g'\ell(y/\pi)) + \sum_{b\in\mathcal{O}_v/\pi\mathcal{O}_v} \omega(\pi^{-1})\tau_v(-by)W(g'\ell(y\pi)) \end{aligned}$$

where $\sigma = \begin{pmatrix}1 & \\ & \pi\end{pmatrix}$ in the second integral. (Note here that $W(g'\ell(y)h^{-1})\eta(h)$ is left K_v-invariant in h and

$$K_v\begin{pmatrix}1 & \\ & \pi\end{pmatrix}K_v = K_v\begin{pmatrix}1 & \\ & \pi\end{pmatrix}\bigcup\left(\bigcup_{b\in\mathcal{O}_v/\pi\mathcal{O}_v} K_v\begin{pmatrix}1 & b\\ 0 & \pi\end{pmatrix}\right) \quad \text{(disjoint).}\ )$$

Thus

$$\lambda W(g'\ell(\pi^m\delta)) = W(g'\ell(\pi^{m-1}\delta)) + \omega(\pi)^{-1}N_vW(g'\ell(\pi^{m+1}\delta)),\ \text{for } m \geq 0.$$

Put $a_m = W(g'\ell(\pi^m\delta))$ for $m \geq -1$ (Note that $a_{-1} = 0$),
$A = \begin{pmatrix}\lambda\omega(\pi)/N_v & -\omega(\pi)/N_v\\ 1 & 0\end{pmatrix}$. Then

$$\begin{pmatrix}a_{m+1}\\ a_m\end{pmatrix} = A\begin{pmatrix}a_m\\ a_{m-1}\end{pmatrix} \Longrightarrow \begin{pmatrix}a_{m+1}\\ a_m\end{pmatrix} = A^{m+1}\begin{pmatrix}a_0\\ a_{-1}\end{pmatrix}$$

and α, β are the eigenvalues of A with respective eigenvectors $\begin{pmatrix}\alpha\\1\end{pmatrix}$, $\begin{pmatrix}\beta\\1\end{pmatrix}$ *i.e.*,

$$\begin{aligned} & A\begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix}\begin{pmatrix}\alpha & \\ & \beta\end{pmatrix} \\ \Longrightarrow \quad & A^{m+1}\begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix}\begin{pmatrix}\alpha^{m+1} & \\ & \beta^{m+1}\end{pmatrix} \\ \Longrightarrow \quad & A^{m+1} = \begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix}\begin{pmatrix}\alpha^{m+1} & \\ & \beta^{m+1}\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ 1 & 1\end{pmatrix}^{-1} \end{aligned}$$

Therefore, $a_m = (\alpha^m + \alpha^{m-1}\beta + \cdots + \alpha\beta^{m-1} + \beta^m)W(g'\ell(\delta))$. ∎

Remark 3.6 Under the assumption that F has narrow class number 1, we will demonstrate the equivalence of the classical and adelic versions of Hecke operators. Recall that under this restriction on F we have

$$\begin{aligned} \mathrm{SL}_2(\mathcal{O})\backslash\mathrm{SL}_2(F_\infty) &\cong \mathrm{SL}_2(F)\backslash\mathrm{SL}_2(\mathbb{A})/\mathrm{SL}_2(\hat{\mathcal{O}}) \\ &\cong Z^+\mathrm{GL}_2^+(\mathcal{O})\backslash\mathrm{GL}_2^+(F_\infty) \\ &\cong Z(F_\infty)\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\mathrm{GL}_2(\hat{\mathcal{O}}). \end{aligned}$$

For a left $Z^+\mathrm{GL}_2^+(\mathcal{O})$-invariant function f on $\mathrm{GL}_2^+(F_\infty)$, we define a function $f^\#$ on $\mathrm{GL}_2(\mathbb{A})$ by $f^\#(\zeta\gamma gk)=f(g)$, where $\zeta\in Z(F_\infty)$, $\gamma\in\mathrm{GL}_2(F)$, $g\in\mathrm{GL}_2^+(F_\infty)$, $k\in\mathrm{GL}_2(\hat{\mathcal{O}})$. Then $f^\#$ is well-defined, left $Z(F_\infty)\mathrm{GL}_2(F)$-invariant, and right $\mathrm{GL}_2(\hat{\mathcal{O}})$- invariant. Let $\mathfrak{n}$ be an ideal of $\mathcal{O}$ such that $\mathfrak{n} = \wp^m$ for a prime ideal $\wp$. Put

$$\Delta(\mathfrak{n}) = :\{g \in M_2(\mathcal{O}) \mid \det g \gg 0,\ (\det g) = \mathfrak{n}\}.$$

For a left $\mathrm{GL}_2^+(\mathcal{O})$-invariant function f on $\mathrm{GL}_2^+(F_\infty)$, the action of the "classical" Hecke operator T_n on f is defined by

$$(T_n f)(g) = \sum_{\delta\in GL_2^+(\mathcal{O})\backslash\Delta(n)} f(\delta g).$$

Also, put $$\Delta'(\mathfrak{n}) = :\{g \in M_2(\mathcal{O}_v) \mid (\det g) = \mathfrak{n}\mathcal{O}_v\},$$

where the finite place v corresponds to $\wp$. If φ is the characteristic function of $Z_v\Delta'(\mathfrak{n})$, and if A is left $Z(\mathbb{A})\mathrm{GL}_2(F)$-invariant and right $\mathrm{GL}_2(\mathcal{O}_v)$- invariant, then $T_n'A$ is defined by

$$(T_n'A)(g) = \int_{Z_v\backslash GL_2(F_v)} A(gh^{-1})\varphi(h)dh.$$

Then we claim that for a left $Z^+\mathrm{GL}_2^+(\mathcal{O})$-invariant function f on $\mathrm{GL}_2^+(F_\infty)$,

$$(T_n f)^\# = T_n'(f^\#).$$

Proof. It is enough to show that $(T_n f)^\#(g) = (T_n'(f^\#))(g)$, for $g \in \mathrm{GL}_2^+(F_\infty)$. Let π be a totally positive generator of $\wp \subseteq \mathcal{O}$ so that $\mathfrak{n} = \pi^m\mathcal{O}$, and let π_v be the image of π in F_v. As representatives for $\mathrm{GL}_2(\mathcal{O}_v)\backslash\Delta'(\mathfrak{n})$, we may choose :

$$X = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; \begin{array}{l} a,\ d \text{ are nonnegative powers} \\ \text{of } \pi_v,\ ad = \pi_v^m,\ b \in \mathcal{O}_v/d\mathcal{O}_v \end{array} \right\}.$$

Thus
$$T_n'(f^\#)(g) = \sum_{\delta \in X} f^\#(g\delta^{-1}).$$

By the strong approximation theorem, there exists an upper triangular matrix $p \in \Delta(\mathfrak{n}) \subseteq \mathrm{GL}_2^+(F)$ such that $p\delta^{-1} \in \mathrm{GL}_2(\mathcal{O}_v)$ (when projected to $\mathrm{GL}_2(F_v)$), $p \in \mathrm{GL}_2(\mathcal{O}_w)$ (when projected to $\mathrm{GL}_2(F_w)$ for finite places $w \neq v$). Note that

$$f^\#(g\delta^{-1}) = f^\#(pg\delta^{-1}) = f^\#(p_\infty g p_0 \delta^{-1}) = f^\#(p_\infty g) = f(p_\infty g).$$

Since a map $X \to \mathrm{GL}_2^+(\mathcal{O})\backslash\Delta(\mathfrak{n})$ given by $\delta \mapsto p$ is a bijection,

$$T_n'(f^\#)(g) = \sum_{\delta \in X} f^\#(g\delta^{-1}) = \sum_{\delta \in X} f(p_\infty g) = (T_n f)(g) = (T_n f)^\#(g). \qquad \blacksquare$$

Now, suppose that f is a twice differentiable function on $\mathfrak{H}^m$ such that $f|_\kappa\gamma = f$, for some $\kappa \in \mathbb{Z}^m$ and all $\gamma \in \Gamma$ in some discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{R})^m$. Now, $f^\#$ is the lifting of f to a function on $\mathrm{SL}_2(\mathbb{R})^m$ *i.e.*, $f^\#(g) = f(g(i))\mu(g,i)^{-\kappa}$.

Proposition 3.5 Let L_j be the Maass lowering operator

$$L_j = e^{-2i\theta}\left(y_j\frac{\partial}{\partial x_j} + iy_j\frac{\partial}{\partial y_j} - \frac{1}{2}\frac{\partial}{\partial\theta_j}\right)$$

on the j-th factor of $\mathrm{SL}_2(\mathbb{R})^m$. Then f is holomorphic in z_j if and only if $L_j f^\# = 0$.

(Here we use the Iwasawa coordinates for $SL_2(\mathbb{R})^m$ *i.e.*,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{\frac{1}{2}} & 0 \\ 0 & y^{-\frac{1}{2}} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$
$$= \left(\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1^{\frac{1}{2}} & 0 \\ 0 & y_1^{-\frac{1}{2}} \end{pmatrix} k(\theta_1), \ldots, \begin{pmatrix} 1 & x_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_m^{\frac{1}{2}} & 0 \\ 0 & y_m^{-\frac{1}{2}} \end{pmatrix} k(\theta_m) \right) .)$$

Proof. Note that

$$f^{\#}\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{\frac{1}{2}} & 0 \\ 0 & y^{-\frac{1}{2}} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \right) = f(x+iy) y^{\frac{\kappa}{2}} e^{i\kappa\theta}.$$

Put $\delta = (0, \ldots, 0, 1, 0, \ldots, 0)$, with 1 at j-th entry. Then

$$\begin{aligned} L_j f^{\#} &= e^{-2i\theta}\Big(y_j y^{\frac{\kappa}{2}} e^{i\kappa\theta} \frac{\partial f}{\partial x_j} + i y_j e^{i\kappa\theta} \frac{\partial (f y^{\frac{\kappa}{2}})}{\partial y_j} - \frac{1}{2} f y^{\frac{\kappa}{2}} \frac{\partial (e^{i\kappa\theta})}{\partial \theta_j} \Big) \\ &= e^{-2i\theta}\Big(y_j y^{\frac{\kappa}{2}} e^{i\kappa\theta} \frac{\partial f}{\partial x_j} + i y_j e^{i\kappa\theta} y^{\frac{\kappa}{2}} \frac{\partial f}{\partial y_j} \\ &\qquad + i y_j e^{i\kappa\theta} f\Big(\frac{1}{2}\kappa_j\Big) y^{\frac{\kappa}{2}-\delta} - \frac{1}{2} f y^{\frac{\kappa}{2}} (i\kappa_j) e^{i\kappa\theta} \Big) \\ &= e^{-2i\theta} y_j y^{\frac{\kappa}{2}} e^{i\kappa\theta}\Big(\frac{\partial f}{\partial x_j} + i \frac{\partial f}{\partial y_j} \Big) \\ &= 2 e^{-2i\theta} y_j y^{\frac{\kappa}{2}} e^{i\kappa\theta} \frac{\partial f}{\partial \bar{z}_j}. \end{aligned}$$

■

Proposition 3.6 Let Y_j be the Casimir operator

$$Y_j = y_j^2 \left(\frac{\partial^2}{\partial x_j^2} + \frac{\partial^2}{\partial y_j^2} \right) - y_j \frac{\partial^2}{\partial x_j \partial \theta_j}$$

on the j-th factor of $SL_2(\mathbb{R})^m$. If f is holomorphic in z_j, then

$$Y_j f^{\#} = \frac{1}{2}\kappa_j \left(\frac{1}{2}\kappa_j - 1 \right) f^{\#}.$$

Proof.
$$Y_j f^{\#}\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{\frac{1}{2}} & 0 \\ 0 & y^{-\frac{1}{2}} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \right)$$
$$= y_j^2 \left(y^{\frac{\kappa}{2}} e^{i\kappa\theta} \frac{\partial^2 f}{\partial x_j^2} + e^{i\kappa\theta} \frac{\partial^2 (f y^{\frac{\kappa}{2}})}{\partial y_j^2} \right) - y_j y^{\frac{\kappa}{2}} (i\kappa_j) \frac{\partial f}{\partial x_j} e^{i\kappa\theta}$$

$$
\begin{aligned}
&= y_j^2\left(y^{\frac{\kappa}{2}}e^{i\kappa\theta}\frac{\partial^2 f}{\partial x_j^2} + e^{i\kappa\theta}y^{\frac{\kappa}{2}}\frac{\partial^2 f}{\partial y_j^2} + \kappa_j e^{i\kappa\theta}\frac{\partial f}{\partial y_j}y^{\frac{\kappa}{2}-\delta}\right.\\
&\quad \left.+\frac{\kappa_j}{2}\Big(\frac{\kappa_j}{2}-1\Big)e^{i\kappa\theta}fy^{\frac{\kappa}{2}-2\delta}\right) - i\kappa_j y_j y^{\frac{\kappa}{2}}\frac{\partial f}{\partial x_j}e^{i\kappa\theta}\\
&= y_j^2 y^{\frac{\kappa}{2}}e^{i\kappa\theta}\left(\frac{\partial^2 f}{\partial x_j^2}+\frac{\partial^2 f}{\partial y_j^2}\right)\\
&\quad +\frac{1}{2}\kappa_j\Big(\frac{1}{2}\kappa_j-1\Big)f^{\#}\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y^{\frac{1}{2}} & 0\\ 0 & y^{-\frac{1}{2}}\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\right)\\
&= \frac{1}{2}\kappa_j\Big(\frac{1}{2}\kappa_j-1\Big)f^{\#}\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y^{\frac{1}{2}} & 0\\ 0 & y^{-\frac{1}{2}}\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\right),
\end{aligned}
$$

since f is holomorphic in z_j, and hence

$$\frac{\partial f}{\partial x_j} = -i\frac{\partial f}{\partial y_j} \quad \text{and} \quad \frac{\partial^2 f}{\partial x_j^2}+\frac{\partial^2 f}{\partial y_j^2} = 0. \qquad \blacksquare$$

Remark 3.7 Let $\mathcal{G}$ be the Lie algebra of $G = \mathrm{GL}_2(\mathbb{R})$ *i.e.*,

$$\mathcal{G} = \{g \in M_2(\mathbb{R}) | \mathrm{Tr}(g) = 0\}.$$

For $\gamma \in \mathcal{G}$, we have the differential operator X_γ on $C^\infty(G)$ defined by :

$$(X_\gamma f)(g) = \frac{d}{dt}\Big|_{t=0} f(ge^{t\gamma}), \quad f \in C^\infty(G).$$

Note that every such an operator X_γ is left G-invariant *i.e.*, if we define $\ell(g)f(h) = f(g^{-1}h)$, then $\ell(g)X_\gamma f = X_\gamma \ell(g)f$. Then by using Iwasawa coordinates

$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y^{\frac{1}{2}} & 0\\ 0 & y^{-\frac{1}{2}}\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix} \qquad (x \in \mathbb{R},\ y \in \mathbb{R}_{>0},\ \theta \in \mathbb{R}/2\pi\mathbb{Z})$$

for $\mathrm{SL}_2(\mathbb{R})$, the Maass (raising and lowering) operators are defined by

$$
\begin{aligned}
R &= e^{2i\theta}\left(y\frac{\partial}{\partial x} - iy\frac{\partial}{\partial y} - \frac{1}{2}\frac{\partial}{\partial\theta}\right),\\
L &= e^{-2i\theta}\left(y\frac{\partial}{\partial x} + iy\frac{\partial}{\partial y} - \frac{1}{2}\frac{\partial}{\partial\theta}\right).
\end{aligned}
$$

Also, define the Casimir operator by

$$Z = y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) - y\frac{\partial^2}{\partial x \partial \theta}.$$

Then one can show that :

(a) Z is left and right $\mathrm{SL}_2(\mathbb{R})$-invariant, commutes with R and L, and satisfies

$$2Z = RoL + LoR - \frac{1}{2}\frac{\partial^2}{\partial \theta^2}.$$

(b) R and L are left $\mathrm{SL}_2(\mathbb{R})$-invariant.

(c) If f is of weight κ ($\kappa \in \mathbb{Z}$) *i.e.*, $f(gk(\theta)) = f(g)e^{i\kappa\theta}$, then Rf and Lf have respectively weights $\kappa + 2$ and $\kappa - 2$.

A general definition of adelic automorphic forms on $\mathrm{GL}_2(\mathbb{A})$ (F is here totally real) can be given as follows :

(i) f is a $\mathbb{C}$-valued, left $\mathrm{GL}_2(F)$-invariant function on $\mathrm{GL}_2(\mathbb{A})$.

(ii) f has a central character ω *i.e.*, $f(\zeta g) = \omega(\zeta)f(g)$ for all $\zeta \in Z(\mathbb{A})$, $g \in \mathrm{GL}_2(\mathbb{A})$, with some Hecke character ω.

(iii) f is right K-finite *i.e.*, the span over $\mathbb{C}$ of $\{g \mapsto f(gk) \mid k \in \prod_{v \leq \infty} K_v\}$ is finite dimensional.

(iv) Viewed as a function of G_∞ alone, f is smooth and Z-finite, where Z denotes the center of universal enveloping algebra of G_∞.

(v) f is slowly increasing *i.e.*, for every $c > 0$, compact subset X of $\mathrm{GL}_2(\mathbb{A})$ there exist $C, N > 0$ such that $f(\ell(y)g) \leq C\|y\|^N$, for all $g \in X$, $y \in \mathbb{J}$ with $\|y\| \geq c$.

f is a cuspform if further it satisfies :

(vi) $\int_{F\backslash\mathbb{A}} f(u(x)g)dx = 0$ for almost all $g \in \mathrm{GL}_2(\mathbb{A})$.

Remark 3.8 (a) (iii) is equivalent to saying that the span over $\mathbb{C}$ of

$$\{g \mapsto f(gk) \mid k \in \prod_{v<\infty} K_v = \mathrm{GL}_2(\hat{\mathcal{O}})\}$$

and that of

$$\{g \mapsto f(gk) \mid k \in \prod_{v=\infty} K_v = \mathrm{SO}(2)^m\}$$

are finite dimensional, respective of which are referred to as right K_0-finiteness and right K_∞-finiteness. Note that right K_0-finiteness $\Longleftrightarrow$ right $\boldsymbol{K}$-invariance, where $\boldsymbol{K}$ is a compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_0)$ and that right K_∞-finiteness $\Longleftrightarrow$ $f = \sum f_\kappa$ is a finite sum of functions of weight κ. Here a function h on $\mathrm{GL}_2(\mathbb{A})$ is of weight $\kappa \in \mathbb{Z}^m$ if $h(gk(\theta)) = h(g)e^{i\kappa\theta}$ for $g \in \mathrm{GL}_2(\mathbb{A})$, $k(\theta) \in \mathrm{SO}(2)^m$.

(b) If f is of weight $\kappa = (\kappa_1, \ldots, \kappa_m)$, then we see that the central character ω must satisfy $\omega(-1_i) = (-1)^{\kappa_i}$ $(i = 1, 2, \ldots, m)$, where -1_i denotes the idele which is 1 at all places except the i-th infinite place, where it is -1.

(c) (iv) is equivalent to saying that $f = \sum f_\lambda$ is a finite sum of functions of eigenvalues λ. Here h has eigenvalue λ if there exists an algebra homomorphism $\lambda: Z \to \mathbb{C}$ such that $Yh = \lambda(Y)h$, for all $Y \in Z$. Recall that the center of the universal enveloping algebra of $\mathrm{SL}_2(\mathbb{R})$ (*i.e.*, the left and right invariant differential operators on $\mathrm{SL}_2(\mathbb{R})$) is $\mathbb{C}[Z]$, where Z is the Casimir operator.

(d) As remarked in (a), f is right $\mathrm{GL}_2(\mathcal{O}_v)$-invariant, for almost all finite places X of F. Primes of X are often called good primes or unramified primes, or primes not dividing the level. If f is an eigenfunction for all Hecke operators T_φ $(\varphi \in H_{v,\omega})$ for all $v \in X$, then we say that f is a Hecke eigenfunction at good primes.

(e) If $\int_{Z(\mathbb{A})GL_2(F)\backslash GL_2(\mathbb{A})} |f(g)|^2 dg < \infty$ with respect to any right $\mathrm{GL}_2(\mathbb{A})$-invariant measure on $Z(\mathbb{A})\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})$, then we say that f is square integrable.

Assume now that f is a cuspform on $\mathrm{GL}_2(\mathbb{A})$ with central character ω, right $\mathrm{GL}_2(\mathcal{O}_v)$-invariant for $v \notin S$ (S is a finite set of places of F including all

infinite places), a Hecke eigenfunction at $v \notin S$. Let χ be a (not necessarily unitary *i.e.*, $\chi = \chi_0 \| \|^s$ for some unitary Hecke character χ_0, and $s \in \mathbb{C}$) Hecke character, unramified at $v \notin S$. Then the standard L-function associated with (f, χ) is given by :

$$\begin{aligned} L(f,\chi) &= \int_{F^\times \backslash \mathbb{J}} \chi(y) f(\ell(y)) d^\times y \\ &= \int_{F^\times \backslash \mathbb{J}} \chi(y) \sum_{\xi \in F^\times} W(\ell(\xi y)) d^\times y \\ &= \int_{\mathbb{J}} \chi(y) W(\ell(y)) d^\times y. \end{aligned}$$

Let $t = (t_v)$ be an idele so that $t_v = 1$ for $v \in S$, t_v is a generator for local inverse different for $v \notin S$. Then we further have :

$$\begin{aligned} L(f,\chi) &= \int_{\prod_{v \in S} F_v^\times} \chi(y) W(\ell(yt)) d^\times y \\ &\qquad \times \prod_{v \notin S} \chi(t_v)(1 - \alpha_v \chi(\pi_v))^{-1}(1 - \beta_v \chi(\pi_v))^{-1} \\ &= \int_{\prod_{v \in S} F_v^\times} \chi(y) W(\ell(yt)) d^\times y \times \prod_{v \notin S} \chi(t_v) \times L_S(f,\chi), \end{aligned}$$

where

$$\begin{aligned} L_S(f,\chi) &= \prod_{v \notin S} [(1 - \alpha_v \chi(\pi_v))(1 - \beta_v \chi(\pi_v))]^{-1} \\ &= \prod_{v \notin S} (1 - (\alpha_v + \beta_v)\chi(\pi_v) + \omega(\pi) N_v^{-1} \chi(\pi_v)^2)^{-1} \end{aligned}$$

is called the L-function associated with (f, χ) at good primes. Note that

$$L_S(f,\chi) = \prod_{v \notin S} \det(1_2 - \chi(\pi_v)\Phi_v)^{-1},$$

where $\Phi_v = \begin{pmatrix} \alpha_v & 0 \\ 0 & \beta_v \end{pmatrix}$, for $v \notin S$.

Also, if ρ is a finite dimensional representation of $\mathrm{GL}_2(\mathbb{C})$, then the higher L-function associated with (f, ρ, χ) is given by :

$$L_S(f,\rho,\chi) = \prod_{v \notin S} \det(1 - \chi(\pi_v)\rho(\Phi_v))^{-1}.$$

Remark 3.9 (a) Note that $L_S(f,\rho,\chi) = L_S(f,\rho_1,\chi)L_S(f,\rho_2,\chi)$ if $\rho = \rho_1 \oplus \rho_2$ and that $L_S(f,\rho,\chi) = L_S(\omega\chi\|\ \|)$ if $\rho(g) = \det(g)$, where the latter is the abelian L-function associated with the Hecke character $\omega\chi\|\ \|$.

(b) Let $f_i\,(i = 1,2,\ldots,n)$ be a cuspform as above, which is a Hecke eigenfunction at $v \notin S$ with associated matrix $\Phi_{v,i}$. Then the tensor product L-function is defined by

$$(*) \qquad L(f_1 \otimes \cdots \otimes f_n, \chi) = \prod_{v \notin S} \det(1 - \chi(\pi_v)\Phi_{v,1} \otimes \cdots \otimes \Phi_{v,n})^{-1}.$$

Under the additional hypothesis that these cuspforms are eigenfunctions for invariant differential operators, it is conjectured that all such L-functions have analytic continuation to meromorphic functions in $\mathbb{C}$ with finitely many poles and have functional equations.
In 1938, Rankin found the analytic continuation of $(*)$ to a meromorphic function in $\mathbb{C}$ for $n = 2$ and in 1986, Garrett did that of $(*)$ to a meromorphic function in $\mathbb{C}$ for $n = 3$. See [G2].

(c) It is known that all holomorphic representations of $\mathrm{GL}_2(\mathbb{C})$ are of the form

$$g \longmapsto \det(g)^m \times \mathrm{Sym}^n(g),$$

where Sym^n is the representation of $\mathrm{GL}_2(\mathbb{C})$ given by

$$(gP)(x,y) = P((x,y)g)$$

with P a homogeneous polynomial of degree n in two variables. Under the assumption that f is an eigenfunction for invariant differential operators, $L_S(f,\mathrm{Sym}^n,\chi)$ has meromorphic continuation to $\mathbb{C}$ for $n \leq 5$ (F.Shahidi).

References

[B] W.L.Baily,Jr. and A.Borel, 'Compactification of arithmetic quotients of bounded symmetric domains', *Ann.of Math.* **84** (1966),442–528.

[C] J.W.S.Cassels and A.Fröhlich, *Algebraic Number Theory*, Academic Press, London and New York, 1967.

[F] E.Freitag, *Hilbert Modular Forms*, Springer-Verlag, Berlin, 1990.

[G1] P.B.Garrett, *Holomorphic Hilbert Modular Forms*, Wadsworth & Brooks / Cole Ad Books & software, Pacific Grove, 1990.

[G2] P.B.Garrett, 'Decomposition of Eisenstein Series : Rankin Triple Products', *Ann. Math*, **125** (1987), 209–235.

[GGP] I.M. Gel'fand, M.I.Graev and I.I.Pyatetskii-Shapiro, *Representation Theory and Automorphic Functions*, Academic Press, Boston, 1990.

[KL] H.Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge Univ. Press, Cambridge, 1990.

[KN] M.Kneser, 'Strong Approximation', *Proc. Sym. Pure Math.* **9**, AMS(1966), 187–196.

[S1] G.Shimula, *Introduction to the Arithmetic Theory of Automorphic Forms*, Iwanami Shoten and Princeton Univ. Press, 1971.

[S2] G.Shimula, 'Confluent Hypergeometric Functions on Tube Domain, *Math. Ann.* **260** (1982), 269–302.

[S3] G.Shimula, 'On the Holomorphy of Certain Dirichlet Series', *Proc. London Math. Soc.* **31**(3) (1975), 79–98.

[T] J.T.Tate, *Fourier Analysis in Number Fields and Hecke's Zeta Functions*, Thesis, Princeton, 1950.

[W] A.Weil, *Basic Number Theory*, Springer-Verlag, New York, 1968.