

Theory of Automorphic Forms of Weight 1

Toyokazu Hiramatsu

Dedicated to Professor Setsuya Seki on his 60th birthday

In this paper a brief exposition is given of some recent developments in the theory of automorphic forms of weight 1 of a complex variable and their applications to number theory. The main contents of this paper are based on my lectures given at Kobe University in 1982–86, at Nagoya University in 1983, and at Tokyo Metropolitan University in 1984.

Table of Contents

- Chapter 1. Higher reciprocity laws
 - § 1.1. Some examples of non-abelian case
 - § 1.2. The Langlands conjecture and $\text{Spl}\{f\}$
- Chapter 2. Hilbert class fields over imaginary quadratic fields
 - § 2.1. The classical theory of complex multiplication
 - § 2.2. Proof of Theorem 2.1.
 - § 2.3. Schläfli's modular function
 - § 2.4. The case of $q=47$
- Chapter 3. Indefinite modular forms
 - § 3.1. Hecke's indefinite modular forms of weight 1
 - § 3.2. Ray class fields over real quadratic fields
 - § 3.3. Positive definite and indefinite modular forms of weight 1
 - § 3.4. Numerical examples
 - § 3.5. Higher reciprocity laws for some real quadratic fields
 - § 3.6. Cusp forms of weight 1 related to quartic residuacity
 - § 3.7. Fundamental lemmas
 - § 3.8. Three expressions of $\theta(\tau; K)$
- Chapter 4. 2-dimensional Galois representations and the Stark conjecture
 - § 4.1. Results of Deligne-Serre
 - § 4.2. The Stark conjecture in the case of weight 1

Received January 7, 1987.

Chapter 5. Dimension formulas and $\text{tr}(T(\Gamma\alpha\Gamma))$ in the case of weight 1

- § 5.1. The Selberg eigenspaces
- § 5.2. The compact case
- § 5.3. The Arf invariant and $d_1 \pmod{2}$
- § 5.4. The finite case
- § 5.5. The traces of Hecke operators on the space of cusp forms of weight 1

Chapter 1. Higher Reciprocity Laws

Let $f(x)$ be a monic irreducible polynomial with integer coefficients and let p be a prime number. Reducing the coefficients of $f(x)$ modulo p , we obtain a polynomial $f_p(x)$ with coefficients in the p -element field F_p . We define $\text{Spl}\{f(x)\}$ to be the set of all primes such that the polynomial $f_p(x)$ factors into a product of distinct linear polynomials over the field F_p . What is a rule to determine the primes belonging to $\text{Spl}\{f(x)\}$? We may call its answer a higher reciprocity law for the polynomial $f(x)$. For example, the usual law of quadratic reciprocity in the elementary number theory gives a 'reciprocity law' in the above sense: Let q be an odd prime. Then the set $\text{Spl}\{x^2 - q\}$ can be described by congruence conditions modulo q if $q \equiv 1 \pmod{4}$ and modulo $4q$ if $q \equiv 3 \pmod{4}$. The polynomial $f(x)$ is called an abelian polynomial if its Galois group is abelian. Then, the next theorem, a natural consequence from class field theory over the rational number field \mathbf{Q} , is known:

Theorem. *The set $\text{Spl}\{f(x)\}$ can be described by congruence relations for a modulus depending only on $f(x)$ if and only if $f(x)$ is abelian.*

If $f(x)$ is a polynomial with non-abelian Galois group, then very little can be said about the set $\text{Spl}\{f(x)\}$. We may call any rule to determine the set $\text{Spl}\{f(x)\}$ a higher reciprocity law for non-abelian polynomial $f(x)$. The main purpose of this chapter is to give some examples of higher reciprocity law for non-abelian polynomials arising from the dihedral cusp forms of weight 1.

§ 1.1. Some examples of non-abelian case

Example 1. $f(x) = x^3 - d$

E1.1. $\text{Spl}\{x^3 - 2\}$

Let $\omega = (-1 + \sqrt{-3})/2$ and consider the ring $\mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\}$.

Let π be a prime in $\mathbf{Z}[\omega]$. If $N(\pi) \neq 3$, the cubic residue of α modulo π is given by

- (i) $(\alpha/\pi)_3 = 0$ if $\pi \mid \alpha$,
- (ii) $\alpha^{(N(\pi)-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$, with $(\alpha/\pi)_3$ equal to 1, ω or ω^2 .

A prime π is called primary if $\pi \equiv 2 \pmod{3}$. Then we can state

Theorem (Cubic Reciprocity Law). *Let π_1 and π_2 be primary, $N(\pi_1), N(\pi_2) \neq 3$, and $N(\pi_1) \neq N(\pi_2)$. Then*

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

Now we have the following by the above cubic reciprocity law:

Theorem 1.1. $\text{Spl}\{x^3 - 2\}$

$$\begin{aligned} &= \{p \mid p \equiv 1 \pmod{3}, p = x^2 + 27y^2, x, y \in \mathbf{Z}\} \\ &= \left\{p \mid p \equiv 1 \pmod{3}, \left(\frac{2}{p}\right)_3 = 1 \text{ for } p = \pi\bar{\pi}\right\} \\ &= \{p \mid p \equiv 1 \pmod{3}, a(p) = 2\}, \end{aligned}$$

where $a(p)$ denotes the p th coefficient of the expansion

$$\eta(6\tau)\eta(18\tau) = \sum_{n=1}^{\infty} a(n)q^n, \quad q = e^{2\pi i\tau}$$

with the Dedekind eta function $\eta(\tau)$.

Proof. The first half. Let p be a rational prime such that $p \equiv 1 \pmod{3}$. Then $p = \pi\bar{\pi}$ in $\mathbf{Z}[\omega]$. Suppose that π is primary. Then, by the law of cubic reciprocity, we have the following two facts:

- (1) $x^3 \equiv 2 \pmod{\pi}$ is solvable if and only if $\pi \equiv 1 \pmod{2}$;
- (2) If $p \equiv 1 \pmod{3}$, then $x^3 \equiv 2 \pmod{p}$ is solvable if and only if there are integers x and y such that $p = x^2 + 27y^2$.

By (1) and (2), we have the first half of Theorem 1.1.

The latter half. By the Euler pentagonal number theorem, we have

$$\eta(6\tau)\eta(18\tau) = \sum_{m,n \in \mathbf{Z}} (-1)^{m+n} q^{\{(6m+1)^2 + 3(6n+1)^2\}/4}.$$

Let denote by $A(p)$ the number of solutions (m, n) of

$$(6m+1)^2 + 3(6n+1)^2 = 4p.$$

Then we have easily the following assertions:

- (i) $A(p)=2$ and $m+n$ is even if $p=x^2+27y^2$;
- (ii) $A(p)=1$ and $m+n$ is odd if $p \neq x^2+27y^2$.

Therefore we have the latter half of Theorem 1.1.

E1.2. Cubic residuacity

Let d be a non-cubic integer and put $K=k(\sqrt[3]{d})$ for $k=\mathbf{Q}(\sqrt{-3})$. Then K is a splitting field of $f(x)=x^3-d$ over \mathbf{Q} with the Galois group $\text{Gal}(K/\mathbf{Q}) \cong S_3$, the symmetric group of order 3, and K/k is a cyclic extension of degree 3. Hence K is the class field over k with conductor $\mathfrak{f}=(3d)$. We denote by $T_{\mathfrak{f}}$ the ideal group corresponding to K .

For any odd prime p except the divisors of \mathfrak{f} , we know that $f \pmod p$ can factor over the p -element field F_p in one of three ways:

- (i) (Linear) (Quadratic) if $p \equiv 2 \pmod 3$,
- (ii) Three linear factors if $p \equiv 1 \pmod 3$ and $\left(\frac{d}{p}\right)_3 = 1$,
- (iii) Irreducible otherwise.

If $p \equiv 1 \pmod 3$, then p splits in k as $p = \mathfrak{p}_p \bar{\mathfrak{p}}_p$, and we obtain

$$\begin{aligned}
 \mathfrak{p}_p \in T_{\mathfrak{f}} &\longleftrightarrow \mathfrak{p}_p \text{ splits completely in } K \\
 &\longleftrightarrow f(x) \text{ has exactly 3 linear factors mod } p \\
 &\longleftrightarrow f(x) \equiv 0 \pmod p \text{ has an integral solution} \\
 &\longleftrightarrow \left(\frac{d}{p}\right)_3 = 1.
 \end{aligned}$$

Now put

$$\begin{aligned}
 I_{\mathfrak{f}} &= \{(\alpha) \mid (\alpha, \mathfrak{f}) = 1\}, \\
 J_{\mathfrak{f}} &= \{(\alpha) \in I_{\mathfrak{f}} \mid \alpha \equiv a \pmod{\mathfrak{f}} \text{ for some } a \in \mathbf{Z}\}, \\
 P_{\mathfrak{f}} &= \{(\alpha) \in I_{\mathfrak{f}} \mid \alpha \equiv 1 \pmod{\mathfrak{f}}\}.
 \end{aligned}$$

Then we have the following table:

field	corresponding ideal group	index
maximal ray class field	$P_{\mathfrak{f}}$	$d + \left(\frac{d}{3}\right)$
ring class field	$J_{\mathfrak{f}}$	$\frac{1}{3} \left(d - \left(\frac{d}{3}\right)\right)$
K	$T_{\mathfrak{f}}$	
k	$I_{\mathfrak{f}}$	3

Hence we observe the group T_f as the union of $\frac{1}{3}\left(d - \left(\frac{d}{3}\right)\right)$ cosets of J_f .

And if d is prime then it follows that I_f/P_f is the direct product of two cyclic groups or a cyclic group according as $d \equiv 1 \pmod{3}$ or not.

Let χ be an ideal character of I_f/T_f , and put

$$L(s, \chi) = \sum_{\alpha} \chi(\alpha) N_{k/Q}(\alpha)^{-s} = \sum_{n=1}^{\infty} a_n n^{-s},$$

where α runs all integral ideals in I_f . Since $L(s, \chi)$ has an Euler product expansion

$$L(s, \chi) = \prod_{p \equiv 2(3)} (1 - p^{-2s})^{-1} \prod_{\left(\frac{d}{p}\right)_3 = 1} (1 - p^{-s})^{-2} \prod_{\substack{p \equiv 1(3) \\ \left(\frac{d}{p}\right)_3 \neq 1}} (1 + p^{-s} + p^{-2s})^{-1} \quad (p \nmid f),$$

we have

$$\begin{aligned} a_p &= 0 && \text{if } p \equiv 2 \pmod{3}, \\ a_p &= 2 && \text{if } p \equiv 1 \pmod{3} \quad \text{and} \quad \left(\frac{d}{p}\right)_3 = 1, \\ a_p &\equiv -1 && \text{if } p \equiv 1 \pmod{3} \quad \text{and} \quad \left(\frac{d}{p}\right)_3 \neq 1. \end{aligned}$$

Therefore,

$$\#\{\alpha \in \mathbf{F}_p \mid f(\alpha) = 0\} = a_p + 1.$$

Put $q = e^{2\pi i \tau}$ for $\text{Im}(\tau) > 0$. Then the corresponding form

$$\theta(\tau) = \sum_{\alpha} \chi(\alpha) q^{N(\alpha)} = \sum_{n=1}^{\infty} a_n q^n$$

of $L(s, \chi)$ is a cusp form of weight 1 and character $\left(\frac{-3}{*}\right)$ for the congruence subgroup $\Gamma_0(3^3 d^2)$. Hence we can obtain that the cubic residuacity of d is determined by the reduction modulo 2 of the Fourier coefficients of the above θ . Then we set

Problem. Express $\theta(\tau)$ explicitly by using the known functions and consider the cubic residuacity more concretely.

Example 1₂. $d = 2$.

In this case it follows that $T_f = J_f = P_f$, and we have

$$I_f/P_f = \langle \mathfrak{p}_7 P_f \rangle,$$

where $\mathfrak{p}_7 = (2 + \sqrt{-3})$. By a simple calculation, we see that

$$a + b\omega \in \mathfrak{P}_7 \iff a \equiv 0 \pmod{6} \quad \text{and} \quad b \equiv 1 \pmod{6}$$

and

$$a + b\omega \in \mathfrak{p}_7 \mathfrak{P}_7 \iff a \equiv 3 \pmod{6} \quad \text{and} \quad b \equiv 1 \pmod{6},$$

where $\omega = (1 + \sqrt{-3})/2$. Thus we can exchange a and b for $3a$ and $6b + 1$ respectively. And since

$$N(3a + (6b + 1)\omega) = \{(6(a + b) + 1)^2 + 3(6b + 1)^2\}/4,$$

we obtain that

$$\begin{aligned} \theta(\tau) &= \sum_{a \in \mathfrak{P}_7} q^{N(a)} - \sum_{a \in \mathfrak{p}_7 \mathfrak{P}_7} q^{N(a)} \\ &= \sum_{a, b \in \mathbb{Z}} (-1)^a q^{N(3a + (6b + 1)\omega)} \\ &= \sum_{a, b \in \mathbb{Z}} (-1)^{a+b} q^{((6a+1)^2 + 3(6b+1)^2)/4} \\ &= \eta(6\tau)\eta(18\tau). \end{aligned}$$

Example 1₃. $d = 3$.

In this case $T_i = J_i$, and we have

$$I_i/J_i = \langle \mathfrak{p}_7 J_i \rangle.$$

For an integral ideal α belonging to I_i , we set

$$\alpha = (x) \quad \text{and} \quad \alpha = (x + 3y\sqrt{-3})/2,$$

where $x \equiv 2 \pmod{3}$ and $x \equiv y \pmod{2}$.

Then, by the easy calculation we see that

$$(\alpha) \in J_i \iff y \equiv 0 \pmod{3},$$

$$(\alpha) \in \mathfrak{p}_7 J_i \iff y \equiv 1 \pmod{3},$$

$$(\alpha) \in \mathfrak{p}_7^2 J_i \iff y \equiv 2 \pmod{3}.$$

Hence we obtain

$$\chi(\alpha) = \zeta^y$$

for $\zeta = e^{2\pi i/3}$, and hence

$$\begin{aligned} \theta(\tau) &= \sum_{\substack{x \equiv 2(3) \\ x \equiv y(2)}} \zeta^y q^{(x^2 + 27y^2)/4} \\ &= \frac{1}{2} \left\{ \sum_{\substack{x \equiv 2(3) \\ y}} \zeta^y q^{(x^2 + 27y^2)/4} + \sum_{\substack{x \equiv 2(3) \\ y}} (-1)^{x+y} \zeta^y q^{(x^2 + 27y^2)/4} \right\} \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{2} \left\{ \sum_{x \equiv 2(3)} q^{x^2/4} \cdot \sum_y \zeta^y q^{27y^2/4} + \sum_{x \equiv 2(3)} (-1)^x q^{x^2/4} \cdot \sum_y (-1)^y \zeta^y q^{27y^2/4} \right\} \\
 &= \frac{1}{8} \{ (\theta_3(\tau/2) - \theta_3(9\tau/2))(3\theta_3(243\tau/2) - \theta_3(27\tau/2)) \\
 &\quad + (\theta_6(\tau/2) - \theta_6(9\tau/2))(3\theta_6(243\tau/2) - \theta_6(27\tau/2)) \} \\
 &= \frac{1}{4} \{ (\theta_3(2\tau) - \theta_3(18\tau))(3\theta_3(486\tau) - \theta_3(54\tau)) \\
 &\quad + (\theta_2(2\tau) - \theta_2(18\tau))(3\theta_2(486\tau) - \theta_2(54\tau)) \},
 \end{aligned}$$

where

$$\begin{aligned}
 \theta_0(\tau) &= \sum_{m \in \mathbf{Z}} (-1)^m q^{m^2/2}, \quad \theta_3(\tau) = \sum_{m \in \mathbf{Z}} q^{m^2/2} \quad \text{and} \\
 \theta_2(\tau) &= \sum_{m \in \mathbf{Z}} q^{(m+1/2)^2/2}.
 \end{aligned}$$

Moreover we can obtain other expression as below:

$$\begin{aligned}
 \theta(\tau) &= \frac{\eta(6\tau)^2 \eta(9\tau) \eta(36\tau) \eta(27\tau) \eta(108\tau) \eta(162\tau)^2}{\eta(3\tau) \eta(12\tau) \eta(18\tau) \eta(54\tau) \eta(81\tau) \eta(324\tau)} \\
 &\quad - \frac{\eta(12\tau) \eta(18\tau)^2 \eta(54\tau)^2 \eta(324\tau)}{\eta(6\tau) \eta(36\tau) \eta(108\tau) \eta(162\tau)}
 \end{aligned}$$

and

$$\begin{aligned}
 \theta(\tau) &= \theta^{(3)} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix} (6\tau|0) \cdot \theta^{(1)} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \left(54\tau \middle| \frac{1}{3} \right) + \theta^{(6)} \begin{bmatrix} 1 \\ 6 \\ 0 \end{bmatrix} (3\tau|0) \cdot \theta^{(2)} \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} \left(27\tau \middle| \frac{1}{3} \right) \\
 &= \frac{1}{2} \left\{ \theta^{(3)} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix} \left(\frac{3}{2}\tau|0 \right) \cdot \theta^{(1)} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \left(\frac{27}{2}\tau \middle| \frac{1}{3} \right) \right. \\
 &\quad \left. + \theta^{(3)} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix} \left(\frac{3}{2}\tau \middle| \frac{1}{2} \right) \cdot \theta^{(1)} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \left(\frac{27}{2}\tau \middle| \frac{1}{6} \right) \right\},
 \end{aligned}$$

where

$$\theta^{(n)} \begin{bmatrix} a \\ n \\ 0 \end{bmatrix} (\tau|z) = \sum_{m \in \mathbf{Z}} e^{\pi i n \{ (m+a/n)^2 \tau + 2(m+a/n)z \}}.$$

Example 2. $f(x) = 4x^3 - 4x^2 + 1$.

E2.1. We put

$$\eta(\tau)^2 \eta(11\tau)^2 = \sum_{n=1}^{\infty} b(n) q^n, \quad q = e^{2\pi i \tau}.$$

By the Euler pentagonal number theorem, we have

$$\sum_{n=1}^{\infty} b(n) q^n \equiv \sum_{u, v \in \mathbf{Z}} q^{((6n+1)^2 + 11(6v+1)^2)/12} \pmod{2}.$$

Let $B(n)$ be the number of solutions (u, v) of

$$(6u+1)^2 + 11(6v+1)^2 = 12n.$$

when n is a prime $p \equiv 2, 6, 7, 8, 10 \pmod{11}$, we see that $B(p) = 0$. For the remaining cases, we have the following

Lemma. *Let p be a prime such that $p \equiv 1, 3, 5, 9 \pmod{11}$. Then either $p \equiv x^2 + 11y^2$ or $p \equiv 3u^2 + 2uv + 4v^2$, and two cases are mutually exclusive, namely, either p or $3p$ is of the form $x^2 + 11y^2$ for some integers x and y . Moreover, the following assertions hold:*

- (i) $B(p) = 2$ and $u + v$ is even if $p = x^2 + 11y^2$;
- (ii) $B(p) = 1$ and $u + v$ is odd if $3p = X^2 + 11Y^2$.

Proof. The first half. Since $(-11/p) = 1$, we have

$$p = a^2 + ab + 3b^2$$

for some integers a and b . If b is even, then

$$\begin{aligned} p &= \left(a + \frac{b}{2}\right)^2 + 11\left(\frac{b}{2}\right)^2 \\ &= x^2 + 11y^2 \quad (x, y \in \mathbf{Z}). \end{aligned}$$

For b odd,

$$3p = \left(3b + \frac{a}{2}\right)^2 + 11\left(\frac{a}{2}\right)^2 \quad (a: \text{even})$$

or

$$3p = \left(3b - \frac{a+b}{2}\right)^2 + 11\left(\frac{a+b}{2}\right)^2 \quad (a: \text{odd}),$$

and hence $3p = X^2 + 11Y^2$ for some integers X and Y . Since matrices

$\begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \\ 1 & 4 \end{pmatrix}$ are not equivalent, the two cases are mutually exclusive.

The latter half. Put

$$D(p) = \{(s, t) \mid s^2 + 11t^2 = 4p, s + t \equiv 2 \pmod{12}\}.$$

Then we see at once that $B(p) = \#D(p)$. If $p = x^2 + 11y^2$, then there are four solutions of the equation $s^2 + 11t^2 = 4p$. Moreover, $s + t \equiv 2 \pmod{4}$ and $s + t \not\equiv 0 \pmod{3}$. Therefore $\#D(p) = 2$. If $3p = X^2 + 11Y^2$, then $X \equiv Y \pmod{3}$, $X \not\equiv Y \pmod{2}$ and

$$4p = \left(\frac{x + 11y}{3}\right)^2 + 11\left(\frac{x - y}{3}\right)^2.$$

Hence there is the only solution of $s^2 + 11t^2 = 4p$ such that $s + t \equiv 2 \pmod{4}$ and $s + t \equiv 2 \pmod{3}$. Therefore $\#D(p) = 1$. Hence we have

$$B(p) = \begin{cases} 2, & \text{if } p = x^2 + 11y^2, \\ 1, & \text{if } 3p = X^2 + 11Y^2. \end{cases}$$

Next it is obvious that

$$\begin{aligned} p &= (3u^2 + u) + 11(3v^2 + v) + 1 \\ &= \left(\frac{u + 11v}{2} + 1\right)^2 + 11\left(\frac{v - u}{2}\right)^2. \end{aligned}$$

Therefore, if $u + v$ is even then

$$p = x^2 + 11y^2 \quad (x, y \in \mathbf{Z}).$$

On the other hand,

$$\begin{aligned} 3p &= 3(3u^2 + u) + 33(3v^2 + v) + 3 \\ &= \left(\frac{-5u + 11v + 11}{2}\right)^2 + 11\left(\frac{u + 5v + 1}{2}\right)^2. \end{aligned}$$

Therefore, if $u + v$ is odd then $3p = X^2 + 11Y^2$ ($X, Y \in \mathbf{Z}$).

Let E be the elliptic curve over \mathbf{Q} defined by

$$y^2 = f(x), \quad f(x) = 4(x^3 - x^2) + 1,$$

which is derived from Tate's form $y^2 + y = x^3 - x^2$. Let p be a good prime for E and \tilde{E}_p denote the reduction modulo p of E which is an elliptic curve over F_p . It is a special (proved) case of the Taniyama-Weil conjecture that the number N_p of F_p -rational points of \tilde{E}_p is given by

$$N_p = p - b(p).$$

Then it is clear that (1) N_p is even if $f(x)$ is irreducible (mod p), (2) N_p is

odd if $f(x)$ has exactly one or three linear factors (mod p). Therefore we have the following ([7])

Theorem 1.2. *Let p be any odd prime, except 11 and put $f_p(x) = f(x) \pmod p$. Then $f_p(x)$ can factor over F_p in one of three ways:*

- (i) *exactly one linear factor if $\left(\frac{-11}{p}\right) = -1$;*
- (ii) *exactly 3 linear factors if $\left(\frac{-11}{p}\right) = 1$ and $p = x^2 + 11y^2 (x, y \in \mathbf{Z})$;*
- (iii) *no linear factor if $\left(\frac{-11}{p}\right) = 1$ and $3p = X^2 + 11Y^2 (X, Y \in \mathbf{Z})$.*

Corollary. $\text{Spl} \{4x^3 - 4x^2 + 1\}$

$$\begin{aligned}
 &= \left\{ p \mid \left(\frac{-11}{p}\right) = 1, p = x^2 + 11y^2 \right\} \\
 &= \left\{ p \mid \left(\frac{-11}{p}\right) = 1, b(p) \equiv 0 \pmod{2} \right\}.
 \end{aligned}$$

E.2.2. We start with

$$\begin{aligned}
 \eta(2\tau)\eta(22\tau) &= q \prod_{n=1}^{\infty} (1 - q^{2n})(1 - q^{22n}) \\
 &= q \sum_{u, v \in \mathbf{Z}} (-1)^{u+v} q^{(3u^2+u) + 11(3v^2+v)} \\
 &= \sum_{u, v \in \mathbf{Z}} (-1)^{u+v} q^{\{(6u+1)^2 + 11(6v+1)^2\}/12}. \\
 &= \sum_{n=1}^{\infty} c(n)q^n,
 \end{aligned}$$

where $q = e^{2\pi i\tau}$. Then, by Lemma, it is immediate that

$$c(p) = \begin{cases} 0, & \text{if } \left(\frac{-11}{p}\right) = -1, \\ 2, & \text{if } \left(\frac{-11}{p}\right) = 1 \text{ and } p = x^2 + 11y^2 \ (x, y \in \mathbf{Z}), \\ -1, & \text{if } \left(\frac{-11}{p}\right) = 1 \text{ and } 3p = X^2 + 11Y^2 \ (X, Y \in \mathbf{Z}). \end{cases}$$

We can now state

Theorem 1.3 ([21]). *Let p be any odd prime, except 11. Then we have the following arithmetic congruence relation*

$$\#\{x \in \mathbf{F}_p \mid 4x^3 - 4x^2 + 1 = 0\} = c(p) - \left(\frac{-11}{p}\right) = c(p)^2 + 1.$$

Proof. In place of $f(x) = 4x^3 - 4x^2 + 1$, we shall consider

$$h(x) = 2f\left(\frac{1-x}{2}\right) = x^3 - x^2 - x - 1.$$

The polynomial $h(x)$ has discriminant -44 . Let $h_p(x)$ be a reduction modulo p of $h(x)$ and let K_h be a splitting field of $h_p(x)$ over the field \mathbf{F}_p . Then it can easily be seen that

$$\begin{aligned} \left(\frac{-11}{p}\right) = -1 &\longleftrightarrow [K_h : \mathbf{F}_p] = 2 \\ &\longleftrightarrow h_p(x) \text{ has exactly one linear factor over } \mathbf{F}_p. \end{aligned}$$

Next we consider the case of $\left(\frac{-11}{p}\right) = 1$. Let L_h be a splitting field of $h(x)$ over \mathbf{Q} . Put $k = \mathbf{Q}(\sqrt{-11})$, and observe that L_h is an abelian extension over k of degree 3. Considering L_h as a class field of k , we denote by H its corresponding class group and by f a conductor of H . Since 2 is only ramified in L_h , we thus obtain $f = (2)$. Hence

$$H = \{(\alpha) : \text{ideals in } k \mid \alpha \equiv 1 \pmod{2}\}.$$

By the assumption $\left(\frac{-11}{p}\right) = 1$, we also have

$$p = \mathfrak{p}\bar{\mathfrak{p}} \quad \text{in } k,$$

where \mathfrak{p} denotes a prime ideal in k and $\bar{\mathfrak{p}}$ a conjugate of \mathfrak{p} ; and moreover

$$\mathfrak{p} \in H \longleftrightarrow \mathfrak{p} \text{ splits completely in } L_h.$$

Now we put $\mathfrak{p} = (\pi)$ with $\pi = a + b\omega$, where $\omega = (-1 + \sqrt{-11})/2$, a and b are rational integers. Then we see from the above result that

$$\begin{aligned} \mathfrak{p} \in H &\longleftrightarrow \pi \equiv 1 \pmod{2} \\ &\longleftrightarrow b \equiv 0 \pmod{2} \\ &\longleftrightarrow p = N(\pi) = x^2 + 11y^2 \quad (x, y \in \mathbf{Z}) \\ &\longleftrightarrow \mathfrak{p} \text{ splits completely in } L_h \\ &\longleftrightarrow h(x) \text{ has exactly 3 linear factors (mod } \mathfrak{p}) \\ &\longleftrightarrow h_p(x) \text{ has exactly 3 linear factors over } \mathbf{F}_p. \end{aligned}$$

Finally, we suppose b is an odd integer in the expression $p = N(\pi) = a^2 + ab + 3b^2$. Then, $3p = X^2 + 11Y^2$ for some integers X and Y , and hence

$$3p = X^2 + 11Y^2 \longleftrightarrow h_p(x) \text{ has no linear factor over } F_p.$$

Corollary. $\text{Spl} \{4x^3 - 4x^2 + 1\} = \{p \mid c(p) = 2, p \neq 2, 11\}$.

Remark 1. Let

$$f(x) = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbf{Z})$$

be an irreducible polynomial whose splitting field K_f is a Galois extension over \mathbf{Q} with $\text{Gal}(K_f/\mathbf{Q}) \cong S_3$ and contains an imaginary quadratic field k . Let $L(s, \rho)$ be the Artin L -function associated with the representation

$$\rho: \text{Gal}(K_f/\mathbf{Q}) \longrightarrow GL_2(\mathbf{C})$$

with conductor N . Then there exists normalized new form $F(z)$ on $\Gamma_0(N)$ of weight 1 and character $\det \rho$. Now, bringing two objects E.2.1 and E.2.2 into unity, Koike obtained the following arithmetic congruence relation for $f(x)$ ([38]):

Theorem. Let M be the product of all primes which appear in a, b and c and let p be any prime such that $p \nmid MN$. Then we have

$$\#\{\alpha \in F_p \mid f(\alpha) = 0\} = a(p)^2 - \left(\frac{-D}{p}\right),$$

where $-D$ denotes the discriminant of k and $a(p)$ denotes the p th Fourier coefficient of $F(z)$:

$$F(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}.$$

Corollary. Let p be any prime such that $p \nmid MN$. then

$$\text{Spl} \{f(x)\} = \{p: \text{prime} \mid a(p) = 2\}$$

up to finite set of primes.

Example 3. $f(x) = x^4 - 2x^4 + 2$

First let us recall some known results which appeared in Smith's Number Theory Report.¹⁾

¹⁾ H. J. S. Smith: Report on the theory of numbers VI, Reports of the British Association for 1865, pp. 322-375, §128: Theorems of Jacobi on Simultaneous Quadratic Forms.

$$(i) \quad \begin{aligned} \eta(8\tau)\eta(16\tau) &= \sum_{a,b \in \mathbf{Z}} (-1)^b q^{(4a+1)^2 + 8b^2} \\ &= \sum_{\alpha, \beta \in \mathbf{Z}} (-1)^{\alpha+\beta} q^{(4\alpha+1)^2 + 16\beta^2}, \end{aligned}$$

where $q = e^{2\pi i\tau}$;

(ii) Let $d(n)$ be the n th Fourier coefficient of $\eta(8)\eta(16\tau)$ at ∞ . Then $d(n)$ is multiplicative and has the following properties:

- (1) $d(p) = 2\varepsilon(-1)^{(p-1)/8}$ if $p \equiv 1 \pmod{8}$, here $\varepsilon \equiv 2^{(p-1)/4} \pmod{p}$;
- (2) $d(p^{2\nu}) = (-1)^\nu$ if $p \equiv 3 \pmod{8}$;
- (3) $d(p^{2\nu}) = 1$ if $p \equiv 5, 7 \pmod{8}$.

The result (ii) is the first instance of an explicit computation of the Fourier coefficients of a cusp form of weight 1 which is of interest from the point of view of history. Let k be an imaginary quadratic field, say $k = \mathbf{Q}(\sqrt{-p})$ with a prime number $p \equiv 1 \pmod{8}$, and let h be the class number of k . We put

$$p = (4a+1)^2 + 8b^2 = (4\alpha+1)^2 + 16\beta^2.$$

Then it is easy to see that

$$\begin{aligned} b \equiv 0 \pmod{2} &\longleftrightarrow \alpha + \beta \equiv 0 \pmod{2} \\ &\longleftrightarrow \left(\frac{-4}{p}\right)_8 = 1 \\ &\longleftrightarrow h \equiv 0 \pmod{8}, \end{aligned}$$

where $\left(\frac{-}{p}\right)_8$ denotes the octic residue symbol modulo p . The identity (i) gives a generalization of the above equivalence.

We can now state

Theorem 1.4 ([41]). *Let p be any odd prime. Then we have the following arithmetic congruence relation*

$$\#\{x \in \mathbf{F}_p \mid x^4 - 2x^2 + 2 = 0\} = 1 + \left(\frac{-1}{p}\right) + d(p).$$

Corollary. $\text{Spl}\{x^4 - 2x^2 + 2\} = \{p \mid p \equiv 1 \pmod{8}, d(p) = 2\}$.

Remark 2. The function $\eta(6\tau)\eta(18\tau)$, $\eta(2\tau)\eta(22\tau)$ and $\eta(8\tau)\eta(16\tau)$ are cusp forms of weight 1 on $\Gamma_0(108)$, $\Gamma_0(44)$ and $\Gamma_0(128)$ respectively. Also Tunell ([55]) proved that $\eta(8\tau)\eta(16\tau)$ is the unique normalized newform of weight 1, level 128 and character χ_{-2} corresponding to $\mathbf{Q}(\sqrt{-2})$. A. Weil characterized the Dirichlet series corresponding to modular forms for $\Gamma_0(N)$ by functional equations for many associated Dirichlet series ([57]). Its Fourier coefficients are effective to describe the set $\text{Spl}\{f\}$.

Remark 3. Let \prod be the set of all prime numbers and $T \subset \prod$ be any subset. For any real $x \geq 1$, we put

$$\sigma(x, T) = \frac{\text{Card} \{p \in T \mid p < x\}}{\text{Card} \{p \in \prod \mid p < x\}}.$$

If T is a set of primes such that $\lim_{x \rightarrow \infty} \sigma(x, T) = \delta(T) < \infty$, then T has density $\delta(T)$. We have now the following theorem.

Tchebotarev Density Theorem. *Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ with Galois group G , and let C be a fixed conjugacy class of elements in G . Let S be the set of primes p whose Artin symbol C_p equals to C . Then S has a density, and*

$$\delta(S) = \frac{\text{Card}(C)}{\text{Card}(G)}.$$

In particular, if $C = \{1\}$, then $S = \text{Spl} \{f\}$ and $\delta(S) = 1/\text{Card}(G)$. If $f(x) = x^5 - x - 1$, then the Galois group of $f(x)$ is the symmetric group S_5 . Therefore $f(x)$ is one of non-solvable polynomials. What is a rule to determine the set $\text{Spl} \{x^5 - x - 1\}$? Wyman ([58]) discussed the relative size of $\text{Spl} \{x^5 - x - 1\}$.

§ 1.2. The Langlands conjecture and $\text{Spl} \{f\}$

Suppose F is a number field and K is a finite Galois extension of F with Galois group $G = \text{Gal}(K/F)$. Let

$$\sigma: G \longrightarrow GL(n, C)$$

be an n -dimensional representation of G . For each place v of F let σ_v denote the restriction of σ to the decomposition group of G at v . The Artin L -function attached to σ is given by the following

$$L(s, \sigma) = \prod_v L(s, \sigma_v)$$

extending over all the places of F . If v is unramified in K , and C_v denotes a Frobenius element over v , then

$$L(s, \sigma_v) = [\det(I - \sigma(C_v)N_v^{-s})]^{-1}.$$

For each place v of F let F_v denote the completion of F at v . Let A_F denote the adèle ring of F and G_A the adèle ring

$$GL(n, A) = \prod_v GL(n, F_v) \quad (\text{a restricted direct product}).$$

Let π be any irreducible unitary representation of G_A . If π can be realized by right translation operators in the space of automorphic (resp. cuspidal automorphic) forms on $GL(n)$, we call π an automorphic (resp. cuspidal) representation of $GL(n)$. Then, there is associated to π a family of local representations π_v which is uniquely determined by π and has the following properties:

- (1) π_v is irreducible for every v ;
- (2) π_v is unramified for almost every v ;
- (3) $\pi = \otimes_v \pi_v$.

Langlands' Reciprocity Conjecture. *For each Galois representation σ , there exists an automorphic representation $\pi(\sigma)$ of $GL(n, A_F)$ such that $L(s, \sigma) = L(s, \pi(\sigma))$. Moreover, if σ is irreducible and non-trivial, then $\pi(\sigma)$ is cuspidal.*

Example 1. $n=2$ and $F=\mathbb{Q}$. Suppose that $\pi_f = \otimes \pi_p$ is generated by the classical modular form

$$f(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi i n z}$$

of weight k . The decomposition $\pi_f = \otimes \pi_p$ corresponds to the fact that f is an eigenfunction for all Hecke operators T_p . The unramified representation π_p then corresponds to the conjugacy class

$$A_p = \begin{pmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{pmatrix}$$

such that $\det(A_p) = 1$ and $\text{tr}(A_p) = p^{-(k-1)/2} a_p$. In this case, Langlands' reciprocity conjecture can be shown to be equivalent to Artin's conjecture for $L(s, \sigma)$. Let $\bar{\mathbb{Q}}$ denote an algebraic closure of \mathbb{Q} and let σ be an irreducible 2-dimensional representation of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ taking complex conjugation to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then the hypothetical representation $\pi(\sigma)$ corresponds to a cusp form of weight 1. Deligne and Serre ([8]) proved that all forms of weight 1 are so obtained (cf. § 4.1).

Suppose that $F=\mathbb{Q}$ and we think of K as the splitting field of some monic polynomial $f(x)$ with integer coefficients. For almost all primes p , we let C_p denote the Frobenius automorphism in $G = \text{Gal}(K/\mathbb{Q})$. Recall that the prime p splits completely in K if and only if $C_p = \text{Id.}$, namely, $f_p(x)$ splits into linear factors. Let $\text{Spl}(K)$ denote the set of primes p which split completely in K . Given a Galois extension K of \mathbb{Q} as above, there exists a Galois representation

$$\sigma: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(n, \mathbb{C})$$

with the property that $\text{Gal}(\bar{\mathbf{Q}}/K)$ is the kernel of σ . Thus we obtain a faithful representation, still denoted

$$\sigma: \text{Gal}(K/\mathbf{Q}) \longrightarrow GL(n, \mathbf{C}),$$

to which we can associate the Artin L -function $L(s, \sigma)$. Then it is clear that

$$\text{Spl}(K) = \{p \mid \sigma(C_p) = I\}.$$

Therefore, under the Langlands reciprocity conjecture, there exists an automorphic representation $\pi = \otimes \pi_p$ of $GL(n)$ such that $A_p = \sigma(C_p)$ for almost all p . In particular,

$$\text{Spl}(K) = \{p \mid A_p(\pi(\sigma)) = I\}.$$

Consequently, Langlands' program reduces the problem of $\text{Spl}(K)$ to the study of automorphic representations of G_A .

Example 2. $n=2$. Langlands' program brings the following:

$$\text{Spl}\{f\} = \{p \mid p \nmid D_f, a(p) = 2\},$$

where D_f denotes the discriminant of f , $\pi(\sigma) = \pi f_\sigma$ and $a(p)$ the p th Fourier coefficient of a cusp form f_σ of weight 1:

$$f_\sigma(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}.$$

Chapter 2. Hilbert Class Fields over Imaginary Quadratic Fields

Let K be an imaginary quadratic field, say $K = \mathbf{Q}(\sqrt{-q})$ with a prime number $q \equiv -1 \pmod{8}$, and let h be the class number of K . By a classical theory of complex multiplication, the Hilbert class field of L of K can be generated by any one of the class invariants over K , which is necessarily an algebraic integer, and a defining equation of which is denoted by $\Phi(x) = 0$. The main purpose of this chapter is to establish the following theorem concerning the arithmetic congruence relation for $\Phi(x)$ ([24]):

Theorem 2.1. *Let p be any prime not dividing the discriminant D_Φ of $\Phi(x)$, and F_p the p -element field. Suppose that the ideal class group of K is cyclic. Then we have*

$$\#\{x \in F_p: \Phi(x) = 0\} = \frac{h}{6} a(p)^2 + \frac{h}{6} a(p) - \frac{1}{2} \left(\frac{-q}{p} \right) + \frac{1}{2},$$

where $\left(\frac{*}{p}\right)$ denotes the Legendre symbol and $a(p)$ denotes the p th Fourier coefficient of a cusp form which will be defined by (1) in Section 2.2 below. One notes that in case $p=2$, we have $\left(\frac{-q}{2}\right)=1$.

§ 2.1. The classical theory of complex multiplication ([10], [13], [61])

Let Λ be a lattice in the complex plane C , and define

$$G_k(\Lambda) = \sum_{\omega \neq 0} \omega^{-k},$$

$$g_2(\Lambda) = 60G_4(\Lambda), \quad g_3(\Lambda) = 140G_6(\Lambda),$$

where l denotes a positive integer and the sum is taken over all non-zero ω in Λ . The torus C/Λ is analytically isomorphic to the elliptic curve E defined by

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

via the Weierstrass parametrization

$$C/\Lambda \ni z \longrightarrow (p(z), p'(z)) \in E,$$

where

$$p(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}, \quad p'(z) = \sum_{\omega} \frac{-2}{(z-\omega)^3}.$$

Let Λ and M be two lattices in C . Then the two tori C/Λ and C/M are isomorphic if and only if there exists a complex number α such that $\Lambda = \alpha M$. If this condition is satisfied, then two lattices Λ and M are said to be linearly equivalent, and we write $\Lambda \sim M$. If so, we have a bijection between the set of lattices in C modulo \sim and the set of isomorphism classes of elliptic curves. Let us define an invariant j depending only on the isomorphism classes of elliptic curves:

$$j(\Lambda) = \frac{1728g_2^3(\Lambda)}{g_3^2(\Lambda) - 27g_2^3(\Lambda)}.$$

In fact, $j(\alpha\Lambda) = j(\Lambda)$ for all $\alpha \in C$. Take a basis $\{\omega_1, \omega_2\}$ of Λ over the ring of rational integers Z such that $\text{Im}(\omega_1/\omega_2) > 0$ and write $\Lambda = [\omega_1, \omega_2]$. Since $[\omega_1, \omega_2] \sim [\omega_1/\omega_2, 1]$, the invariant $j(\Lambda)$ is determined by $\tau = \omega_1/\omega_2$ which is called the moduli of E . Therefore we can write the following:

$j(\Lambda)=j(\tau)$. The lattice Λ has many different pairs of generators, the most general pair $\{\omega'_1, \omega'_2\}$ with τ' in the upper half-plane having the form

$$\begin{cases} \omega'_1 = a\omega_1 + b\omega_2 \\ \omega'_2 = c\omega_1 + d\omega_2 \end{cases}$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$, the special linear group of degree 2 with coefficients in \mathbf{Z} . Thus the function $j(\tau)$ is a modular function with respect to $SL(2, \mathbf{Z})$. It is well known that

$$j(\sqrt{-1})=1728, \quad j(e^{2\pi\sqrt{-1/3}})=0, \quad j(\infty)=\infty.$$

The modular function $j(\tau)$ can be characterized by the above properties.

Let there be given a lattice Λ and the elliptic curve E as described in the above. If for some $\alpha \in \mathbf{C} - \mathbf{Z}$, $\wp(\alpha z)$ is a function on \mathbf{C}/Λ , then we say that E admits multiplication by α ; and then α and ω_1/ω_2 are in the same quadratic field. If E admits multiplication by α_1 and α_2 , then E admits multiplication by $\alpha_1 \pm \alpha_2$ and $\alpha_1\alpha_2$. Thus the set of all such α is an order in an imaginary quadratic field K . Consider the case when E admits multiplication by the maximal order \mathfrak{o}_K in K . Then the invariant j defines a function on the ideal classes k_0, k_1, \dots, k_{h-1} of K (h being the class number of K) and the numbers $j(k_i)$ are called 'singular values' of j . Put

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad=n>0, 0 \leq b < d, (a, b, d)=1, a, b, d \in \mathbf{Z} \right\},$$

and consider the polynomial

$$F_n(t) = \prod_{\alpha \in A} (t - j(\alpha z)).$$

We may view $F_n(t)$ as a polynomial in two independent variables t and j over \mathbf{Z} , and write it as

$$F_n(t) = F_n(t, j) \in \mathbf{Z}[t, j].$$

Let us put $H_n(j) = F_n(j, j)$. Then $H_n(j)$ is a polynomial in j with coefficients in \mathbf{Z} , and if n is not a square, then the leading coefficient of $H_n(j)$ is ± 1 . This equation

$$H_n(j) = 0$$

is called the modular equation of order n . Now we can find an element w in \mathfrak{o}_K such that the norm of w is square-free:

$$w = \begin{cases} 1 + \sqrt{-1}, & \text{if } K = \mathcal{Q}(\sqrt{-1}), \\ \sqrt{-m}, & \text{if } K = \mathcal{Q}(\sqrt{-m}) \text{ with } m > 1 \text{ and square-free.} \end{cases}$$

Let, $\{\omega_1, \omega_2\}$ be a basis of an ideal in an ideal class k_i such that $\text{Im}(\omega_1/\omega_2) > 0$. Then

$$\begin{cases} w\omega_1 = a\omega_1 + b\omega_2 \\ w\omega_2 = c\omega_1 + d\omega_2 \end{cases}$$

with integers a, b, c, d and the norm of w is equal to $ad - bc$. Thus $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is primitive and $\alpha\tau = \tau$. Hence $j(\tau) = j(k_i)$ is a root of the modular equation $H_n(j) = 0$. Therefore we have the following

(i) $j(k_i)$ is an algebraic integer.

Furthermore we know

(ii) $K(j(k_i))$ is the Hilbert class field of K .

By the class field theory, there exists a canonical isomorphism between the ideal class group C_K of K and the Galois group G of $K(j(k_i))/K$, and we have the following formulas which describe how it operates on the generator $j(k_i)$:

(iii) Let σ_k be the element of G corresponding to an ideal class k by the canonical isomorphism. Then

$$\sigma_k(j(k')) = j(k^{-1}k')$$

for any $k' \in C_K$.

(iv) For each prime ideal \mathfrak{p} of K of degree 1, we have

$$j(\mathfrak{p}^{-1}k) \equiv j(k)^{N(\mathfrak{p})} \pmod{\mathfrak{p}}, \quad k \in C_K,$$

where $N(\mathfrak{p})$ denotes the norm of \mathfrak{p} .

(v) The invariants $j(k_i)$, $i = 0, 1, \dots, h-1$, of K form a complete set of conjugates over the field of rational numbers \mathcal{Q} .

§ 2.2. Proof of Theorem 2.1

Let q be a prime number such that $q \equiv -1 \pmod{8}$, $K = \mathcal{Q}(\sqrt{-q})$ and let h be the class number of K , which is necessarily odd. For $0 \leq i \leq h-1$, we denote by $Q_{k_i}(x, y)$ the binary quadratic form corresponding to the ideal class k_i (k_0 : principal class) in K and put

$$\theta_i(\tau) = \frac{1}{2} \sum_{n=0}^{\infty} A_{k_i}(n) e^{2\pi\sqrt{-1}n\tau} \quad (\text{Im}(\tau) > 0),$$

where $A_{k_i}(n)$ is the number of integral representations of n by the form Q_{k_i} . Then the following lemma is classical:

Lemma 1. 1) *If p is any odd prime, except q , then we have*

$$\frac{1}{2}A_{k_0}(p) + \sum_{i=1}^{h-1} A_{k_i}(p) = 1 + \left(\frac{-q}{p}\right).$$

2) *If we identify opposite ideal classes by each other, there remain only $A_{k_0}(p), A_{k_1}(p), \dots, A_{k_{(h-1)/2}}(p)$, among which there is at most one non-zero element.*

Moreover, for each ideal class k in K , we have

Lemma 2. 1) $A_k(n) = 2\#\{\alpha \in \mathfrak{o}_K : \alpha \in k^{-1}, N(\alpha) = n\}$,

2) $2A_k(mn) = \sum_{\substack{k_1 k_2 = k \\ k_1, k_2 \in C_K}} A_{k_1}(m)A_{k_2}(n)$ if $(m, n) = 1$.

Let χ be any character ($\neq 1$) on the group C_K of ideal classes and put

$$A(n) = \frac{1}{2} \sum_{k_i \in C_K} \chi(k_i)A_{k_i}(n).$$

Then we have the following multiplicative formulas.

Lemma 3. 1) $A(mn) = A(m)A(n)$ if $(m, n) = 1$,

2) $A(p)A(p^r) = A(p^{r+1}) + \left(\frac{-q}{p}\right)A(p^{r-1})$ for prime $p(\neq q)$ and $r \geq 1$,

3) $A(qn) = A(q)A(n)$.

We define here two functions f and F as follows:

(1) $f(\tau) = \theta_0(\tau) - \theta_1(\tau)$,

and

(2) $F(\tau) = \sum_{i=0}^{h-1} \chi(k_i)\theta_i(\tau) = \sum_{n=1}^{\infty} A(n)e^{2\pi\sqrt{-1}n\tau}$,

where $\theta_0(\tau)$ is the theta-function corresponding to the principal class k_0 . Then $f(\tau)$ is a normalized cusp form on the congruence subgroup $\Gamma_0(q)$ of weight 1 and character $\left(\frac{-q}{p}\right)$, and moreover, by Lemma 3, $F(\tau)$ is a

normalized new form on $\Gamma_0(q)$ of weight 1 and character $\left(\frac{-p}{q}\right)$ (cf. [17]).

From now on, we assume that the ideal class group C_K of K is cyclic. By Lemma 1, we shall calculate the Fourier coefficients of $f(\tau)$ and $F(\tau)$. Let

$$C_K = \langle k_1 \rangle \quad \text{and} \quad \chi(k_1) = e^{2\pi\sqrt{-1}/h}.$$

Then we can write the function $F(\tau)$ as

$$F(\tau) = \theta_0(\tau) + 2 \sum_{i=1}^{(k-1)/2} \cos \frac{2\pi i}{h} \theta_i(\tau),$$

where $k_i = k_1^i \left(1 \leq i \leq \frac{1}{2}(h-1) \right)$. If $\left(\frac{-q}{p} \right) = -1$, then $A_k(p) = 0$ for all $k \in C_K$. If $\left(\frac{-q}{p} \right) = 1$, then $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ ($\mathfrak{p} \neq \bar{\mathfrak{p}}$) in K , where \mathfrak{p} denotes a prime ideal in K and $\bar{\mathfrak{p}}$ a conjugate of \mathfrak{p} . We denote by $k_{\mathfrak{p}}$ the ideal class such that $\mathfrak{p} \in k_{\mathfrak{p}}$. If $k_{\mathfrak{p}}$ is ambiguous, then

$$A_k(p) = \begin{cases} 4, & \text{if } k = k_{\mathfrak{p}}^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

If k is not ambiguous, then

$$A_k(p) = \begin{cases} 2, & \text{if } k = k_{\mathfrak{p}} \text{ or } k = k_{\mathfrak{p}}^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

In the case $p = q$, put $(p) = \mathfrak{p}^2$ ($\mathfrak{p} = \bar{\mathfrak{p}}$) with $\mathfrak{p} \in k_{\mathfrak{p}}$. Then we have

$$A_k(p) = \begin{cases} 2, & \text{if } k = k_{\mathfrak{p}}, \\ 0, & \text{otherwise.} \end{cases}$$

Let $a(n)$ be the n th coefficient of the Fourier expansion for $f(\tau)$:

$$f(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi\sqrt{-1}n\tau}.$$

By the above results, we have the following formulas for $a(p)$ and $A(p)$.

Lemma 4. *Suppose that the ideal class group C_K of K is cyclic. Then, for each prime p , the Fourier coefficients $a(p)$ and $A(p)$ are given as follows:*

$$a(p) = \begin{cases} 0, & \text{if } \left(\frac{-q}{p} \right) = -1, \\ 2, & \text{if } \left(\frac{-q}{p} \right) = 1 \text{ and } p = x^2 + xy + \frac{1+q}{4}y^2 \quad (x, y \in \mathbf{Z}), \\ 0 \text{ or } 1, & \text{if } \left(\frac{-q}{p} \right) = 1 \text{ and } k_{\mathfrak{p}} \neq k_0 \text{ with } (p) = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \in k_{\mathfrak{p}}, \\ 1, & \text{if } p = q, \end{cases}$$

and

$$A(p) = \begin{cases} 0, & \text{if } \left(\frac{-q}{p}\right) = -1, \\ 2, & \text{if } \left(\frac{-q}{p}\right) = 1 \text{ and } p = x^2 + xy + \frac{1+q}{4}y^2 \quad (x, y \in \mathbf{Z}), \\ 2 \cos \frac{2\pi n}{h}, & \text{if } \left(\frac{-q}{p}\right) = 1 \text{ and } k_p = k_n^{\pm 1} (\neq k_0) \text{ with } (p) = \mathfrak{p}\bar{\mathfrak{p}}, \\ & \mathfrak{p} \in k_p \quad (1 \leq n \leq (h-1)/2). \end{cases}$$

Let

$$\Phi(x) = 0$$

be the defining equation of a generating element of the Hilbert class field L over the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-q})$. Then the polynomial $\Phi(x)$ is one of the irreducible factors of the modular polynomial $H_q(x)$. We say simply $\Phi(x)$ is a modular polynomial. Now, in order to prove Theorem 2.1, it is enough to show that if the ideal class group C_K is a cyclic group of order h , then

$$\#\{x \in \mathbf{F}_p \mid \Phi(x) = 0\} = \begin{cases} 1, & \text{if } \left(\frac{-q}{p}\right) = -1, \\ h, & \text{if } \left(\frac{-q}{p}\right) = 1 \text{ and } p = x^2 + xy + \frac{1+q}{4}y^2 \quad (x, y \in \mathbf{Z}), \\ 0, & \text{if } \left(\frac{-q}{p}\right) = 1 \text{ and } k_p \neq k_0 \text{ with } (p) = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \in k_p. \end{cases}$$

We denote by H the ideal group corresponding to the Hilbert class field L of K :

$$H = \{(\alpha) : \text{principal ideals in } K\}.$$

Case 1. $\left(\frac{-q}{p}\right) = 1$. Let $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in K . Then we have the following relation:

$$\begin{aligned} \mathfrak{p} \in H &\longleftrightarrow \mathfrak{p} = (\pi), \quad \pi = a + b\omega \quad (\omega = (1 + \sqrt{-q})/2, a, b \in \mathbf{Z}) \\ &\longleftrightarrow p = N(\mathfrak{p}) = a^2 + ab + \frac{1+q}{4}b^2 \quad (a, b \in \mathbf{Z}), \end{aligned}$$

and

\mathfrak{p} splits completely in $L \longleftrightarrow \Phi(x) \pmod p$ has exactly h factors.

Therefore

$$p = a^2 + ab + \frac{1+q}{4} b^2 \quad (a, b \in \mathbf{Z}) \longleftrightarrow \Phi(x) \pmod p \text{ has exactly } h \text{ factors.}$$

On the other hand, it is obvious that

$$\begin{aligned} \mathfrak{p} \notin H \longleftrightarrow \mathfrak{p} \text{ is a product of prime ideals of degree } > 1 \text{ in } L \\ \longleftrightarrow \Phi(x) \pmod p \text{ has no linear factors in } \mathbf{F}_p[x]. \end{aligned}$$

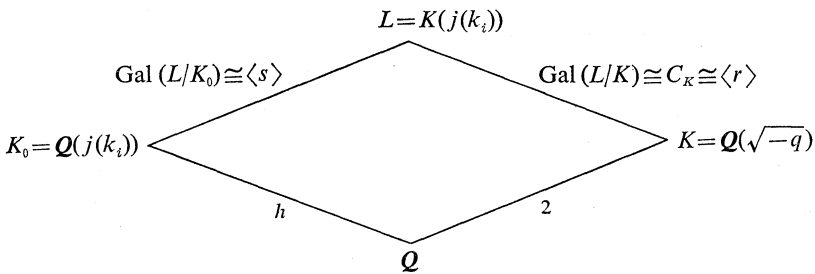
Case 2. $\left(\frac{-q}{p}\right) = -1$. The polynomial $\Phi(x)$ splits completely modulo p in $\mathfrak{o}_K/(p)$ and the field $\mathfrak{o}_K/(p)$ is a quadratic extension of \mathbf{F}_p . Therefore

$$\Phi(x) \pmod p = h_1(x) \cdots h_t(x)$$

and $\deg h_i \leq 2$ ($i = 1, 2, \dots, t$), where each $h_i(x)$ is irreducible in $\mathbf{F}_p[x]$. Since the class number h of K is odd, there exist odd numbers of i such that $\deg h_i = 1$. In the following, we shall show that there exists one and only one of each i . The dihedral group D_h has $2h$ elements and is generated by r, s with the defining relations

$$r^h = s^2 = 1, \quad srs = r^{-1}.$$

Let K_0 be the maximal real subfield of L . We have the following diagram:



Let \mathfrak{o}_{K_0} be the ring of algebraic integers in K_0 . Then the ideal $p\mathfrak{o}_{K_0}$ decomposes into a product of distinct prime ideals in K_0 :

$$p\mathfrak{o}_{K_0} = \mathfrak{p}_1 \cdots \mathfrak{p}_m \mathfrak{g}_1 \cdots \mathfrak{g}_n,$$

where

$$N_{K_0/Q}(\mathfrak{p}_l) = p \quad (1 \leq l \leq m) \quad \text{and} \quad N_{K_0/Q}(\mathfrak{g}_l) = p^2 \quad (1 \leq l \leq n).$$

Moreover, if \mathfrak{o}_L is the ring of algebraic integers in L , then

$$\mathfrak{p}_l \mathfrak{o}_L = \mathfrak{P}_l \quad (1 \leq l \leq m),$$

where each \mathfrak{P}_l is a prime ideal in \mathfrak{o}_L . On the other hand, the ideal $p\mathfrak{o}_L$ has the following decomposition via the field K :

$$p\mathfrak{o}_L = \mathfrak{P}_1 \mathfrak{P}_1^r \cdots \mathfrak{P}_1^{h-1}.$$

Since $\mathfrak{p}_1^s = \mathfrak{p}_1$, we have also $\mathfrak{P}_1^s = \mathfrak{P}_1$. Similarly, $\mathfrak{P}_i^s = \mathfrak{P}_i$ ($2 \leq i \leq m$). However, since h is odd and $srs = r^{-1}$, we deduce

$$\mathfrak{P}_1^{r^i s} = \mathfrak{P}_1^{-r^i} \neq \mathfrak{P}_1^{r^i}, \quad (1 \leq i \leq h-1).$$

Since $\mathfrak{P}_i = \mathfrak{P}_1^{r^i}$ for some i , we have $m=1$. This completes the proof of Theorem 2.1.

Corollary (Higher Reciprocity Law).

$$\text{Spl} \{ \Phi(x) \} = \left\{ p \mid p \nmid D_\Phi, \left(\frac{-q}{p} \right) = 1 \text{ and } a(p) = 2 \right\}.$$

§ 2.3. Schläfli's modular equation

The problem of determining the modular polynomial $F_n(t, j)$ explicitly for an arbitrary order n was treated by N. Yui ([59]). But, even for $n=2$, $F_2(t, j)$ has an astronomically long form. We shall use here the Schläfli modular function $h_0(\tau)$ in place of $j(\tau)$:

$$h_0(\tau) = e^{-\pi \sqrt{-1}/24} \frac{\eta((\tau+1)/2)}{\eta(\tau)} = e^{-\pi \sqrt{-1}\tau/24} \prod_{n=1}^{\infty} (1 + e^{(2n-1)\pi \sqrt{-1}\tau}),$$

where η is the Dedekind eta function. This function $h_0(\tau)$ is the modular function for the principal congruence subgroup of level 48 and has the following properties:

$$j(\tau) = \frac{\{h_0(\tau)^{24} - 16\}^3}{h_0(\tau)^{24}} \quad \text{and} \quad h_0\left(-\frac{1}{\tau}\right) = h_0(\tau).$$

Lemma 5 ([56]). *Let q be any prime number such that $q \equiv -1 \pmod{8}$. Then*

- 1) $\sqrt{2} h_0(\sqrt{-q}) \in \mathcal{Q}(j(\sqrt{-q}))$,
- 2) $\sqrt{1/2} h_0(\sqrt{-q})$ is a unit of an algebraic number field.

Put

$$x = \frac{1}{\sqrt{2}} h_0(\sqrt{-q}).$$

Then, by Lemma 5,1), we have

$$Q(x) = Q(j(\sqrt{-q})).$$

The defining equation of x is called the *Schläfli modular equation of order q* ([56], §§ 73–75 and § 131).

Example ([56]). $n=47$. Schläfli’s modular equation of order 47 is given by

$$x^5 - x^3 - 2x^2 - 2x - 1 = 0.$$

§ 2.4. The case of $q=47$

Let \mathfrak{o}_K be the principal order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-47})$ and put $\mathfrak{o}_K = [1, \omega]$ with $\omega = (1 + \sqrt{-47})/2$. The field K has class number 5. Let

$$\begin{aligned} Q_0(x, y) &= x^2 + xy + 12y^2, \\ Q_1(x, y) &= 7x^2 + 3xy + 2y^2, \\ Q_2(x, y) &= 3x^2 - xy + 4y^2, \end{aligned}$$

be the binary quadratic forms corresponding to the ideals $\mathfrak{o}_K, [7, 1 + \omega], [3, \omega]$, respectively, and let

$$\theta_i(\tau) = \frac{1}{2} \sum_{n=0}^{\infty} A_{Q_i}(n) e^{2\pi \sqrt{-1}n\tau} \quad (i=0, 1, 2)$$

be the theta-functions belonging to the above binary quadratic forms, respectively, where $A_{Q_i}(n)$ denotes the number of integral representations of n by the form Q_i . By Lemma 1, we have easily the following table:

		$A_{Q_0}(p)$	$A_{Q_1}(p)$	$A_{Q_2}(p)$
$\left(\frac{-47}{p}\right) = -1$		0	0	0
$\left(\frac{-47}{p}\right) = 1$	$p = x^2 + 47y^2$	4	0	0
	$7p = x^2 + 46y^2$	0	2	0
	$3p = x^2 + 47y^2$	0	0	2

For $p=2, 47$, we have

$$\begin{aligned} A_{Q_0}(2) &= A_{Q_2}(2) = 0, & A_{Q_1}(2) &= 2; \\ A_{Q_0}(47) &= 2, & A_{Q_1}(47) &= A_{Q_2}(47) = 0. \end{aligned}$$

Now we define two functions as follows:

$$\begin{aligned} F_1(\tau) &= \theta_0(\tau) - \theta_1(\tau) = \sum_{n=1}^{\infty} a(n)e^{2\pi\sqrt{-1}n\tau}, \\ F_2(\tau) &= \theta_0(\tau) - \theta_2(\tau). \end{aligned}$$

Then $F_1(\tau)$ and $F_2(\tau)$ are normalized cusp forms on the group $\Gamma_0(47)$ of weight 1 and character $\left(\frac{-47}{p}\right)$. Put $\varepsilon_0 = \frac{1}{2}(1 + \sqrt{5})$ and define

$$\begin{aligned} F_3(\tau) &= \varepsilon_0 F_1(\tau) + \varepsilon_0 F_2(\tau) = F_1(\tau) + \varepsilon_0 \eta(\tau) \eta(47\tau) \\ &= \sum_{n=1}^{\infty} A(n)e^{2\pi\sqrt{-1}n\tau}. \end{aligned}$$

Then the function $F_3(\tau)$ is also a normalized cusp form of weight 1 and character $\left(\frac{-47}{p}\right)$ on the group $\Gamma_0(47)$, and the Fourier coefficient $A(n)$

is multiplicative. The Fourier coefficients of $F_1(\tau)$ and $F_3(\tau)$ are obtained by the above table as follow, respectively. For each prime $p(\neq 2, 47)$, we have

$$(3) \quad a(p) = \begin{cases} 0 & \text{if } \left(\frac{-47}{p}\right) = -1, \\ 2 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}), \\ 0 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 3p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}), \\ -1 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 7p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}), \end{cases}$$

and

$$(4) \quad A(p) = \begin{cases} 0 & \text{if } \left(\frac{-47}{p}\right) = -1, \\ 2 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}), \\ -\varepsilon_0 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 3p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}), \\ -\varepsilon_0 & \text{if } \left(\frac{-47}{p}\right) = 1 \quad \text{and} \quad 7p = x^2 + 47y^2 \quad (x, y \in \mathbf{Z}). \end{cases}$$

Furthermore we have $a(2) = -1$, $a(47) = A(47) = 1$ and $A(2) = -\varepsilon_0$.

Put $h_0(-47) = \sqrt{2}x$. Then the class invariant x satisfies the following Schläfli's modular equation of order 47 (cf. § 2.3):

$$(5) \quad f_W(x) = x^5 - x^3 - 2x^2 - 2x - 1 = 0 \quad (D_{f_W} = 47^2).$$

Let L be the Hilbert class field over K . Then the field L is a splitting field for the polynomial

$$(6) \quad f_H(x) = x^5 - 2x^4 + 2x^3 - 3x^2 - 3x + 6x - 5 \quad (D_{f_H} = 11^2 \cdot 47^2),$$

and the Galois group $G(L/\mathbf{Q})$ is equal to the dihedral group D_5 ([14]), [15]).

Put

$$\eta_0 = \frac{1}{2} \left(\frac{47 - 5\sqrt{5}}{2} + \frac{-5 + \sqrt{5}}{2} \sqrt{47\sqrt{5}\varepsilon_0} \right)$$

and

$$\omega_0 = \frac{9353 + 422\sqrt{5}}{7} - \frac{715 + 325\sqrt{5}}{4} \sqrt{47\sqrt{5}\varepsilon_0},$$

then from Hasse's result ([14]) we deduce that

$$\theta_H = \frac{1}{5} \left(\sqrt[5]{\omega_0} - \frac{1}{\sqrt[5]{\omega_0}} - \frac{\sqrt[5]{\omega_0}}{\eta_0} + \frac{\eta_0}{\sqrt[5]{\omega_0}} + 2 \right)$$

generates L/K . Consider the following equation ([11], p. 492):

$$(7) \quad f_F(x) = x^5 - x^4 + x^3 + x^2 - 2x + 1 = 0.$$

It is known that there are two relations

$$(8) \quad \begin{cases} \theta_H = 5\theta_W^2 - 5\theta_W - 2, \\ \theta_W = -\theta_F^4 - 2\theta_F + 1 \end{cases}$$

for the real roots θ_W , θ_H and θ_F of (5), (6) and (7), respectively ([60]). Put

$$f_M(x) = x^5 - 2x^4 + 3x^3 + x^2 - x - 1.$$

The discriminant of our polynomial $f_M(x)$ is $5^2 \cdot 47^2$. By a simple calculation, we can verify the following remarkable relation:

$$(9) \quad x^2 - ax + b \mid f_F(x) \iff f_H(a)f_M(a) = 0,$$

where a and b denote any constants. If θ is the real root of the equation $f_M(x) = 0$, then we obtain the following relations by making use of Newton's method:

$$(10) \quad \left\{ \begin{array}{l} \theta_H = 2\theta_F^4 + \theta_F^3 + \theta_F^2 + 2\theta_F - 2, \text{ (by (8))} \\ \theta = -2\theta_F^4 + \theta_F^3 - \theta_F^2 - 3\theta_F + 3, \\ \theta_F = \frac{-1}{11}(\theta_H^4 + \theta_H^3 + 5\theta_H^2 + \theta_H - 2), \\ \theta = \frac{1}{11}(\theta_H^4 + \theta_H^3 + 5\theta_H^2 - \theta_H + 9), \\ \theta_F = \frac{1}{5}(\theta^4 - 5\theta^3 + 8\theta^2 - 8\theta - 2), \\ \theta_H = \frac{1}{5}(-\theta^4 + 5\theta^3 - 8\theta^2 + 3\theta + 7). \end{array} \right.$$

Now we consider $f_F(x) \pmod p$ for any odd prime number $p (\neq 47)$. Because of (9) and (10), the reduced polynomial $f_F \pmod p$ ($p \neq 5, 11$) can factor over the p -element field F_p in one of three ways:

- 1) Five linear factors,
- 2) (linear) (Quadratic) (Quadratic).
- 3) Quintic.

The reduced polynomials $f_F \pmod 5$ and $f_F \pmod 11$ have the above type 2). When we combine these with (3), we are led to the another proof of the arithmetic congruence relation in the case of $q=47$.

Theorem 2.2. *Let p be any prime, except 47, and F_p the field of p elements. Let $a(n)$ be the n th coefficient of the expansion*

$$F_1(\tau) = \sum_{n=1}^{\infty} a(n) e^{2\pi\sqrt{-1}n\tau}.$$

Then the following congruence relation for $f_F(x)$ holds:

$$\#\{x \in F_p \mid f_F(x) = 0\} = \frac{5}{6}a(p)^2 + \frac{5}{6}a(p) - \frac{1}{2}\left(\frac{-47}{p}\right) + \frac{1}{2},$$

where for $p=2$, we understand $\left(\frac{-47}{2}\right) = 1$.

Proof. In order to prove this, it is enough to show the following fact. Let L_p be a splitting field of $f_F(x) \pmod p$ over the field F_p . Then it can easily be seen that

$$\left(\frac{-47}{p}\right) = -1 \iff [L_p : F_p] = 2$$

$\iff f_F \pmod p$ has exactly one linear factor over F_p

$\iff f_F \pmod p$ can factor in type 2).

Remark 1. Let p be a prime, except 5, 11, 47. Then, by the relation (10), $f_F \bmod p$, $f_H \bmod p$, $f_W \bmod p$ and $f_M \bmod p$ can factor over F_p in the same way. Using Fourier coefficients of $F_2(\tau)$, we have also the same arithmetic congruence relation for $f_F(x)$. On the other hand, using Fourier coefficients $A(p)$ of $F_3(\tau)$ (cf. (4)), we have the following relation:

$$\#\{x \in F_p \mid f_F(x) = 0\} = A(p)^2 + A(p) - \left(\frac{-47}{p}\right).$$

Finally the following higher reciprocity law for the Fricke polynomial $f_F(x)$ holds:

Corollary. $\text{Spl} \{f_F(x)\} = \{p \mid (-47/p) = 1 \text{ and } a(p) = 2\}$.

Remark 2. The dihedral group D_h has $(h+3)/2$ conjugate classes:

$$\{1\}, \{sr^i \mid 1 \leq i \leq h\}, \{r^j, r^{-j}\}, \quad j = 1, 2, \dots, (h-1)/2.$$

Thus we have $(h-1)/2$ irreducible representations of degree 2. Among them, here we consider the representation ρ given by the following

$$\rho(r) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \bar{\varepsilon} \end{pmatrix}, \quad \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $\varepsilon = e^{2\pi\sqrt{-1}/h}$. The corresponding character is given by the following

	$\{1\}$	$\{r^j, r^{-j}\}$	$\{sr^i \mid 1 \leq i \leq h\}$
ρ	2	$2 \cos \frac{2\pi j}{h}$	0

$$j = 1, 2, \dots, \frac{h-1}{2}.$$

Let $\phi(s)$ be the Dirichlet series associated to the new form $F(\tau)$ (cf. (2) in § 2.1) via the Mellin transform. Since the function $F(\tau)$ is an eigenfunction of all the Hecke operators T_p, U_p , the Dirichlet series $\phi(s)$ has the following Euler product:

$$\begin{aligned} \phi(s) &= \sum_{n=1}^{\infty} A(n)n^{-s} = (1 - A(q)q^{-s})^{-1} \prod_{p \neq q} \left(1 - A(p)p^{-s} + \left(\frac{-q}{p}\right)p^{-2s}\right)^{-1} \\ &= (1 - q^{-s})^{-1} \prod_{\left(\frac{-q}{p}\right) = -1} (1 - p^{-2s})^{-1} \prod_{p \in P_1} (1 - 2p^{-s} + p^{-2s})^{-1} \\ &\quad \times \prod_{p \in P_2} \left(1 + 2 \cos \frac{2\pi n}{h} p^{-s} + p^{-2s}\right)^{-1}, \end{aligned}$$

where

$$P_1 = \left\{ p \mid \left(\frac{-q}{p} \right) = 1, p = x^2 + xy + \frac{1+q}{4}y^2 \right\},$$

and

$$P_2 = \left\{ p \mid \left(\frac{-q}{p} \right) = 1, p = p\bar{p}, p \neq \text{principal}, p \in k_n \right\} \cup \{2\}.$$

Let L be the Hilbert class field of the imaginary quadratic field K , and assume that the Galois group $G(L/K)$ is a cyclic group of order h . Then L/\mathcal{Q} is a non-abelian Galois extension with D_h as Galois group. Let p be any prime number and σ_p a Frobenius map of p in L , and put

$$A_p = \frac{1}{e} \sum_{\alpha \in T} \rho(\sigma_p \alpha),$$

where T is the inertia group of p and $\#T = e$. Then, for the Galois extension L/\mathcal{Q} , the Artin L -function is defined by

$$L(s, \rho, L/\mathcal{Q}) = \prod_p \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - A_p N(p)^{-s} \right)^{-1}, \quad \text{Re}(s) > 1.$$

A prime p factorizes in L in one of the following ways:

Case 1. $\left(\frac{-q}{p} \right) = -1$. Decomposition field = K_0 , $\sigma_p = s$, $A_p = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Case 2. $p \in P_1$. Decomposition field = L , $\sigma_p = 1$, $A_p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Case 3. $p \in P_2$. Decomposition field = K . If $(p) = p\bar{p}$ with $p \in k_n^{-1}$, then $\sigma_p = r^n$ and $A_p = \begin{pmatrix} \varepsilon^n & 0 \\ 0 & \bar{\varepsilon}^n \end{pmatrix}$.

Case 4. $p = q$. Ramification exponent = 2.

$$\sigma_q = 1, \quad A_q = \frac{1}{2}(\rho(1) + \rho(s)) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

In order to have the explicit form of $L(s, \rho, L/\mathcal{Q})$, we use the above results and obtain

$$\begin{aligned} L(s, \rho, L/\mathcal{Q}) &= \prod_p \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - A_p N(p)^{-s} \right)^{-1} \\ &= \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - q^{-s} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)^{-1} \prod_{\left(\frac{-q}{p} \right) = -1} \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - p^{-s} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)^{-1} \end{aligned}$$

$$\times \prod_{p \in P_1} \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - p^{-s} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)^{-1} \prod_{p \in P_2} \det \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - p^{-s} \begin{pmatrix} \varepsilon^n & 0 \\ 0 & \varepsilon^n \end{pmatrix} \right)^{-1}.$$

It is clear that above Euler product, compared with the Euler product of $\phi(s)$, proves the following:

$$L(s, \rho, L/\mathbf{Q}) = \phi(s).$$

This is a constructive version for the dihedral case of the Deligne-Serre theorem ([8]).

Chapter 3. Indefinite modular forms

As show in Chapters 1 and 2, there are deep relations between the class fields over imaginary quadratic fields and cusp forms of weight 1. In the first half of this chapter, we study a similar problem for class fields over real quadratic field which satisfies a condition due to Shintani ([50]). In Section 3.1 we recall the definition of Hecke's indefinite modular forms of weight 1 which are associated to real quadratic fields ([16], [17], [40]). In Section 3.2 we summarize certain results of Shintani for the real quadratic problem which is transferable to the imaginary quadratic situation ([50]). In Section 3.3 we apply the result of Shintani to our problem and obtain the three representations for some dihedral cusp forms of weight 1 by positive definite theta series and indefinite theta series. Kac and Peterson in [35] gave many examples of new identities for cusp forms of weight 1 which arise from the Dedekind eta function. In Section 3.4 we shall reconstruct these examples from our point of view, by using the results of Section 3.3. In Section 3.5 we establish the higher reciprocity law for a defining equation of ray class fields over some real quadratic fields.

The second half of this chapter will be devoted to study a relation between quartic residuacity and Fourier coefficients of cusp forms of weight 1 ([23]). Let m be a positive square free integer and ε_m denote the fundamental unit of $\mathbf{Q}(\sqrt{m})$. We consider only those m for which ε_m has norm $+1$. If l is an odd prime such that $\left(\frac{m}{l}\right) = \left(\frac{\varepsilon_m}{l}\right) = 1$, we can ask for the value of the quartic residue symbol $\left(\frac{\varepsilon_m}{l}\right)_4$. Let K be the Galois extension of degree 16 over \mathbf{Q} generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$. Then its Galois group $G(K/\mathbf{Q})$ has just two irreducible representations of degree 2. We can define a cusp form of weight 1 by these representations, which will be denoted by $\Theta(\tau; K)$ and we shall show that $\Theta(\tau; K)$ has three expressions by definite and indefinite theta series and that the value of the

symbol $\left(\frac{\varepsilon_m}{l}\right)_4$ is expressed by the l th Fourier coefficient of $\theta(\tau; K)$. These results offer us new criterions for ε_m to be a quartic residue modulo l .

§ 3.1. Hecke's indefinite modular forms of weight 1

Let F be a real quadratic field with discriminant D , and \mathfrak{o}_F the ring of all integers in F . Let Q be a natural number and denote by \mathbb{U}_0 the group of totally positive unit ε of \mathfrak{o}_F such that $\varepsilon \equiv 1 \pmod{Q\sqrt{D}}$. Let α be an integral ideal of \mathfrak{o}_F , and put $|N(\alpha)| = A$. Then the Hecke modular form for the ideal α is defined by

$$\mathfrak{H}_\kappa(\tau; \rho, \alpha, Q\sqrt{D}) = \sum_{\substack{\mu \in \mathfrak{o}_F \\ \mu \equiv \rho \pmod{\alpha Q\sqrt{D}} \\ \mu \in \mathfrak{o}_F/\mathfrak{u}_0, N(\mu)\kappa > 0}} (\text{sgn } \mu) q^{N(\mu)/AQD},$$

where $\kappa = \pm 1$, $\rho \in \alpha$, $\text{Im}(\tau) > 0$ and $q = e^{2\pi i \tau}$. This is a holomorphic function of τ and satisfies

$$\begin{aligned} \mathfrak{H}_\pm\left(\frac{a\tau + b}{c\tau + d}; \rho, \alpha, Q\sqrt{D}\right) \\ = \left(\frac{D}{|d|}\right)^{\varepsilon \mp 2\pi i a b \rho \rho' / AQD} (c\tau + d) \mathfrak{H}_\pm(\tau; a\rho, \alpha, Q\sqrt{D}) \end{aligned}$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(QD)$ ([16], [17]).¹⁾ Therefore \mathfrak{H}_\pm is the cusp form of weight 1 for a certain congruence subgroup of level QD under the condition $\mathfrak{H}_\pm \neq 0$. If in particular $\alpha = \mathfrak{o}_F$, we put

$$\mathfrak{H}_\pm(\tau; \rho, Q\sqrt{D}) = \mathfrak{H}_\pm(\tau; \rho, \mathfrak{o}_F, Q\sqrt{D}).$$

§ 3.2. Ray class fields over real quadratic fields

Let there be given a real quadratic field F as described in Section 3.1. Let \mathfrak{f} be a self conjugate integral ideal of \mathfrak{o}_F which satisfies the condition:

- (1) For any totally positive unit ε of \mathfrak{o}_F , $\varepsilon + 1 \notin \mathfrak{f}$.

We denote by $H_F(\mathfrak{f})$ the narrow ray class group modulo \mathfrak{f} of F . Then, under the condition (1), the group $H_F(\mathfrak{f})$ has a character χ of the following type:

$$\chi((x)) = \text{sgn } x \quad \text{or} \quad \chi((x)) = \text{sgn } x'$$

for $x - 1 \in \mathfrak{f}$, where x' denotes the conjugate of x . We denote the Hecke L -function of F attached to χ by

¹⁾ For a general treatment of this function via Weil representation, see [35] and [40].

$$L_F(s, \chi) = \sum_{c \in H_F(\mathfrak{f})} \chi(c) \sum_{\substack{a \in c \\ a \subset \mathfrak{o}_F}} N(a)^{-s} \quad (\text{Re}(s) > 1).$$

Then the Γ -factor in the functional equation of $L_F(s, \chi)$ is of the form

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right).$$

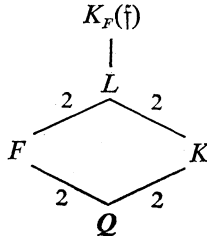
We put

$$H_F(\mathfrak{f})_0 = \{c \in H_F(\mathfrak{f}) \mid c' = c\},$$

and assume that

$$(2) \quad [H_F(\mathfrak{f}) : H_F(\mathfrak{f})_0] = 2.$$

Let $K_F(\mathfrak{f})$ denote the maximal narrow ray class field over F corresponding to $H_F(\mathfrak{f})$ and σ denote the Artin canonical isomorphism given by class field theory. Let L be the subfield of $\sigma(H_F(\mathfrak{f})_0)$ -fixed elements of $K_F(\mathfrak{f})$. Then, under the assumption (2), L is a composition of F with a suitable imaginary quadratic field k , and $K_F(\mathfrak{f})$ is an abelian extension of k ([50]).



Therefore there exists an integral ideal c of k such that $K_F(\mathfrak{f})$ is a class field over k with conductor c . Let \mathfrak{f}_χ be the conductor of χ and $\tilde{\chi}$ the primitive character of $H_{F(\mathfrak{f}_\chi)}$ corresponding to χ . We denote by ξ_χ one of the characters of the group $H_k(c)$ determined by χ in a natural manner. Let c_χ be the conductor of ξ_χ and $\tilde{\xi}_\chi$ the primitive character of $H_k(c_\chi)$ corresponding to ξ_χ . Then we have the following coincidence of two L -functions associated with the real quadratic field F and the imaginary quadratic field k ([50]):

$$(3) \quad L_F(s, \tilde{\chi}) = L_k(s, \tilde{\xi}_\chi).^{2)}$$

§ 3.3. Positive definite and indefinite modular forms of weight 1

In this section we use the same symbols as in Section 3.2. We put

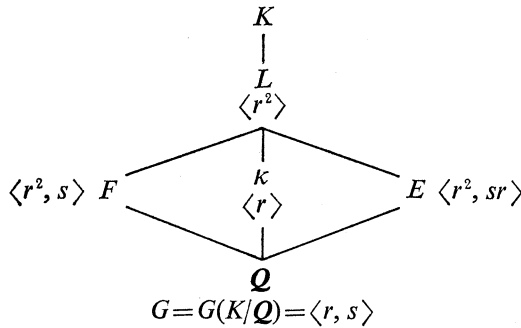
²⁾ H. Ishii proved that the coincidence (3) is equivalent to the condition (2) ([29]).

$$K = K_F(\mathfrak{f});$$

and assume that K/k is a cyclic extension. We denote by $\mathfrak{D}(F/\mathcal{Q})$ and $\mathfrak{D}(k/\mathcal{Q})$ the different of F over \mathcal{Q} and that of k over \mathcal{Q} , respectively. Then we have the following relation between the conductor c of the cyclic extension K/k and the finite part \mathfrak{f} for the conductor of the abelian extension K/F by Hasse's theorem:

Lemma 1. $\mathfrak{f} \cdot \mathfrak{D}(F/\mathcal{Q}) = c \cdot \mathfrak{D}(k/\mathcal{Q})$ as ideals in L .

Let us, temporarily, assume that K/\mathcal{Q} is a dihedral extension. Then the Galois group $G(K/\mathcal{Q})$ is the dihedral group D_4 of order 8 and we have the following diagram of fields:



Here E denotes the imaginary quadratic field determined by F and k . The conductor c of K/k is an ideal of \mathbf{Z} by Satz 7 of Halter-Koch ([36]). Now we put

$$c = (c), \quad c \in \mathbf{Z}.$$

Since, $\mathfrak{f}' = \mathfrak{f}$, $(\mathfrak{f} \cdot \mathfrak{D}(F/\mathcal{Q}))^2$ is an ideal of \mathbf{Z} , i.e.,

$$(\mathfrak{f} \cdot \mathfrak{D}(F/\mathcal{Q}))^2 = (q^2 \cdot d),$$

where q is a positive integer and d is a positive square-free integer. K/k being a cyclic extension by assumption, we have the following by Lemma 1.

Lemma 2. $c = q \cdot e_a^{-1}$ and $k = \mathcal{Q}(\sqrt{-d})$,

where

$$e_a = \begin{cases} 1 & \text{if } d \equiv 3 \pmod{4}, \\ 2 & \text{otherwise.} \end{cases}$$

We are going to discuss how to obtain an identity between cusp forms of weight 1. Take an integer μ of F such that $\mu < 0$, $\mu' > 0$ and $\mu \equiv 1 \pmod{\mathfrak{f}}$, and denote by the same letter μ the ray class modulo \mathfrak{f} represented by the principal ideal (μ) . Then, by the condition (1), μ is an element of order 2 of $H_F(\mathfrak{f})$, and by the condition (2), we have

$$H_F(\mathfrak{f}) = H_F(\mathfrak{f})_0 + H_F(\mathfrak{f})_0\mu.$$

Let $\langle \mu\mu' \rangle$ be the subgroup of $H_F(\mathfrak{f})_0$ generated by $\mu\mu'$ and let R be a complete set of representatives of $H_F(\mathfrak{f})_0 \pmod{\langle \mu\mu' \rangle}$. Since $\langle \mu\mu' \rangle$ is the subgroup of order 2 of $H_F(\mathfrak{f})_0$, we have

$$H_F(\mathfrak{f}) = R \cup R\mu \cup R\mu' \cup R\mu\mu' \quad (\text{disjoint}).$$

For $c \in H_F(\mathfrak{f})$, we put

$$\zeta_F(s, c) = \sum_{\substack{\alpha \in c \\ \alpha \subset \mathfrak{o}_F}} N(\alpha)^{-s}.$$

Then it is easily checked that

$$\zeta_F(s, \sigma\mu) = \zeta_F(s, \sigma\mu')$$

for $\sigma \in R$. Let χ be a character of $H_F(\mathfrak{f})$ with conductor $\mathfrak{f}(\infty_i)$ satisfying the condition (1). Then the Hecke L -function of F attached to χ has the following expression

$$\begin{aligned} L_F(s, \chi) &= \sum_{\sigma \in R} \chi(\sigma) \{ \zeta_F(s, \sigma) - \zeta_F(s, \sigma\mu) + \zeta_F(s, \sigma\mu') - \zeta_F(s, \sigma\mu\mu') \} \\ &= \sum_{\sigma \in R} \chi(\sigma) \{ \zeta_F(s, \sigma) - \zeta_F(s, \sigma\mu\mu') \}. \end{aligned}$$

Let σ be an element of R and let α_σ be an integral ideal of σ^{-1} . We put

$$\begin{aligned} A_\sigma^+ &= \{ \alpha \in \alpha_\sigma \mid \alpha \equiv 1 \pmod{\mathfrak{f}}, \alpha > 0, \alpha' > 0 \}, \\ A_\sigma^- &= \{ \alpha \in \alpha_\sigma \mid \alpha \equiv 1 \pmod{\mathfrak{f}}, \alpha < 0, \alpha' < 0 \} \end{aligned}$$

and

$$A_\sigma = A_\sigma^+ \cup A_\sigma^-.$$

Then it is easy to verify that

$$A_\sigma = \{ \alpha \in \mathfrak{o}_F \mid \alpha \equiv \rho_\sigma \pmod{\alpha_\sigma \mathfrak{f}}, N(\alpha) > 0 \},$$

where ρ_σ denotes an element of α_σ such that $\rho_\sigma \equiv 1 \pmod{\mathfrak{f}}$. Moreover, we have the following two bijections:

$$A_\sigma^+ \bmod E_f^+ \ni \alpha \bmod E_f^+ \longleftrightarrow \alpha \alpha_\sigma^{-1} \in \sigma \cap \mathfrak{o}_F$$

and

$$A_\sigma^- \bmod E_f^+ \ni \alpha \bmod E_f^+ \longleftrightarrow \alpha \alpha_\sigma^{-1} \in \sigma \mu \mu' \cap \mathfrak{o}_F,$$

where

$$E_f^+ = \{ \varepsilon : \text{unit of } \mathfrak{o}_F \mid \varepsilon \equiv 1 \pmod{f}, \varepsilon > 0, \varepsilon' > 0 \}.$$

From these correspondences, it is easy to see that

$$\zeta_F(s, \sigma) = \sum_{\alpha \in A_\sigma^+ \bmod E_f^+} (N(\alpha)/N(\alpha_\sigma))^{-s}$$

and

$$\zeta_F(s, \sigma \mu \mu') = \sum_{\alpha \in A_\sigma^- \bmod E_f^+} (N(\alpha)/N(\alpha_\sigma))^{-s}.$$

Hence we obtain an explicit form of $L_F(s, \chi)$:

$$\begin{aligned} L_F(s, \chi) &= \sum_{\sigma \in R} \chi(\sigma) \sum_{\alpha \in A_\sigma \bmod E_f^+} (\text{sgn } \alpha) (N(\alpha)/N(\alpha_\sigma))^{-s} \\ &= \sum_{\sigma \in R} \chi(\sigma) \sum_{\alpha} (\text{sgn } \alpha) (N(\alpha)/N(\alpha_\sigma))^{-s}, \end{aligned}$$

where α in the summation runs over all integers of F such that $\alpha \equiv \rho_\sigma \pmod{\alpha_\sigma f}$, $\alpha \bmod E_f^+$ and $N(\alpha) > 0$. We apply the inverse Mellin transformation on the above L -function and obtain the following indefinite cusp form of weight 1:

$$\begin{aligned} \theta_F(\tau) &= \sum_{\sigma \in R} \chi(\sigma) \sum_{\alpha} (\text{sgn } \alpha) q^{N(\alpha)/N(\alpha_\sigma)} \quad (q = e^{2\pi i \tau}) \\ &= \sum_{\sigma \in R} \chi(\sigma) \theta(QD_1 \tau; \rho_\sigma, \alpha_\sigma, f), \end{aligned}$$

where $f = Qf_1$, $f_1 \mid \sqrt{D}$, $D_1 = N(f_1)$ and

$$\theta(\tau; \rho_\sigma, \alpha_\sigma, f) = \sum_{\alpha} (\text{sgn } \alpha) q^{N(\alpha)/N(\alpha_\sigma) Q D_1}.$$

In particular, if we put $f_1 = \sqrt{D}$, then the above function θ is just the Hecke indefinite modular form defined in Section 3.1.

On the other hand, since K/k is a cyclic extension, we can put

$$H_k(c)/C = \langle \lambda \rangle,$$

where C denotes the subgroup of $H_k(c)$ corresponding to K . The generator λ is an element of order $4m$. The restriction of the representation of

$\text{Gal}(K/Q)$ induced from χ to $\text{Gal}(K/k)$ is a direct sum of two distinct primitive characters ξ and ξ' of $H_k(c)/C$ via the Artin map. Then we consider the Hecke L -function of k attached to ξ :

$$L_k(s, \xi) = \sum_{\alpha \subset \mathfrak{o}_k} \xi(\alpha) N(\alpha)^{-s} = \sum_{j=0}^{4m-1} \xi(\lambda^j) \sum_{\substack{\alpha \in \lambda^j \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s}.$$

For every odd j , the correspondence

$$\alpha \in \lambda^j, \alpha \subset \mathfrak{o}_k \longleftrightarrow \alpha' \in \lambda^{(2m+1)j}, \alpha' \subset \mathfrak{o}_k$$

is bijective and $\xi(\lambda^j) = (-1)^j \xi(\lambda)^{(2m+1)j}$. Hence

$$L_k(s, \xi) = \sum_{j=0}^{2m-1} \xi(\lambda^j) \sum_{\substack{\alpha \in \lambda^{2j} \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s} = \sum_{j=0}^{m-1} \xi(\lambda^2)^j \left\{ \sum_{\substack{\alpha \in \lambda^{2j} \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s} - \sum_{\substack{\alpha \in \lambda^{2m+2j} \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s} \right\}.$$

Applying the inverse Mellin transformation on the above L -function $L(s, \xi)$, we have the following positive definite modular form of weight 1:

$$\theta_k(\tau) = \sum_{j=0}^{m-1} \xi(\lambda^2)^j \{ \theta_{2j}(\tau) - \theta_{2m+2j}(\tau) \},$$

where

$$\theta_j(\tau) = \sum_{\substack{\alpha \in \lambda^j \\ \alpha \subset \mathfrak{o}_k}} q^{N(\alpha)} \quad (q = e^{2\pi i \tau}).$$

It is now clear that the above results, combined with the coincidence (3) in Section 3.2, prove the following identity:

$$\theta_F(\tau) = \theta_k(\tau).$$

From now on, we assume again that K/Q is a dihedral extension. Then $m=1$ and

$$\begin{aligned} \theta_F(\tau) &= \theta(QD_1\tau; 1, \mathfrak{o}_F, \bar{\mathfrak{f}}) \\ &= t^{-1} \mathfrak{g}_\kappa(QD_1\tau; \rho, Q\sqrt{D}), \end{aligned}$$

where $\kappa = \pm 1$, $N(\rho)\kappa > 0$, $\bar{\mathfrak{f}}\rho = (Q\sqrt{D})$ and $t = [E_{\bar{\mathfrak{f}}}^+ : \mathbb{U}_0]$. Consequently we have

Theorem 3.1 ([25]). *The notation and assumptions being as above, we*

have the following identity between positive definite and indefinite cusp forms of weight 1:

$$(4) \quad t^{-1}\vartheta_x(QD_1\tau; \rho, Q\sqrt{D}) = \theta_0(\tau) - \theta_x(\tau).$$

Theorem 3.1 gives a number theoretic explanation of the identities discovered by Kac-Peterson ([35]).

§ 3.4. Numerical examples

In this section we shall give some numerical examples based on Lemma 2 and Theorem 3.1 in Section 3.3. As the method for making of the examples is the same for each, we shall give the details only for the first example.

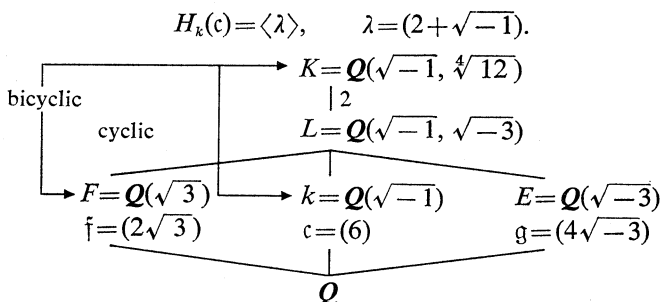
1. For the first example we set $F = \mathbf{Q}(\sqrt{3})$ and $\mathfrak{f} = (2\sqrt{3})$. The fundamental unit of F is totally positive and is given by $\varepsilon = 2 + \sqrt{3}$. It is easy to see that $\varepsilon^2 \equiv 1 \pmod{\mathfrak{f}}$. Put $\mu = (7 - 6\sqrt{3})$. Then the group $H_F(\mathfrak{f})$ is an abelian group of type $(2, 2)$:

$$H_F(\mathfrak{f}) = \{1, \mu, \mu', \mu\mu'\};$$

and

$$H_F(\mathfrak{f})_0 = \{1, \mu\mu'\}.$$

Hence the field F and the conductor \mathfrak{f} satisfy the conditions (1) and (2) in Section 3.2. By Lemma 2 we know that $k = \mathbf{Q}(\sqrt{-1})$ and $c = (6)$. Furthermore, since $H_k(c)$ is a group of order 4, we have $C = \{1\}$, and so



In the following we shall look for the explicit forms of θ_k and θ_F . First we treat the function $\theta_k(\tau)$. It is easy to see that

$$\begin{cases}
 \alpha \in (1) \longleftrightarrow \alpha = (\alpha), & \alpha \equiv 1 \pmod{6}, \\
 \alpha \in \lambda^2 \longleftrightarrow \alpha = (\alpha), & \alpha \equiv 2 + 3\sqrt{-1} \pmod{6}.
 \end{cases}$$

Hence, if $\alpha = x + 3\sqrt{-1}y$ ($(x, 3) = 1$), then we have

$$\begin{cases} (\alpha) \in (1) \longleftrightarrow x \equiv 1 \pmod{2} \text{ and } y \equiv 0 \pmod{2}, \\ (\alpha) \in \lambda^2 \longleftrightarrow x \equiv 0 \pmod{2} \text{ and } y \equiv 1 \pmod{2}. \end{cases}$$

Therefore

$$\begin{aligned} \theta_k(\tau) &= \frac{1}{2} \sum_{\substack{x, y \in \mathbb{Z} \\ (x, 3) = 1, x \not\equiv y \pmod{2}}} (-1)^y q^{x^2 + 9y^2} \\ &= \eta^2(12\tau) \quad (q = e^{2\pi i \tau}). \end{aligned}$$

Next, for the function $\theta_F(\tau)$,

$$\begin{cases} \alpha \in (1) \longleftrightarrow \alpha = (\alpha), \alpha > 0, \alpha' > 0 \text{ and } \alpha \equiv 1 \pmod{2\sqrt{3}}, \\ \alpha \in \mu\mu' \longleftrightarrow \alpha = (\alpha), \alpha > 0, \alpha' > 0 \text{ and } \alpha \equiv -1 \pmod{2\sqrt{3}}. \end{cases}$$

Therefore, if $\alpha = x + 2\sqrt{3}y$ ($x \equiv \pm 1 \pmod{6}$), we have

$$\begin{cases} (\alpha) \in (1) \longleftrightarrow x \equiv 1 \pmod{3}, \\ (\alpha) \in \mu\mu' \longleftrightarrow x \equiv -1 \pmod{6}. \end{cases}$$

Since $\alpha\varepsilon^{\pm 2} = (7x \pm 24y) + (14y \pm 4x)\sqrt{3}$, we have the following as a fundamental domain:

$$x \geq 4|y|,$$

so that

$$\begin{aligned} \theta_F(\tau) &= \mathcal{G}_+(12\tau; 1, \sqrt{12}) \\ &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \geq 4|y|, (x, 6) = 1}} \left(\frac{x}{3}\right) q^{x^2 - 12y^2}. \end{aligned}$$

Another form of $\theta_F(\tau)$ is obtained as follows. Let ρ be any positive integer in F . Then it is easy to see that

$$\theta_F(\tau) = \sum_{\beta} (\text{sgn } \beta) q^{N(\beta)/N(\rho)},$$

where β in the sum runs over all integers of F such that $\beta \equiv \rho \pmod{\mathfrak{f}\rho}$, $\beta \pmod{E^+}$ and $N(\beta)N(\rho) > 0$. Now we set $\rho = 1 + \sqrt{3}$. Put

$$\beta = \begin{cases} x + y\sqrt{3}, & \text{if } \beta > 0, \\ x - y\sqrt{3}, & \text{if } \beta < 0 \end{cases}$$

³⁾ Hecke also found this expression ([16], pp. 425–426).

for rational integers x and y . Then, for the case $\beta > 0$,

$$y > 0, \quad x \equiv 1 \pmod{6} \quad \text{and} \quad x \equiv y \pmod{4}.$$

Therefore we can put

$$x = 6l + 1, \quad y = 2k + 1 \quad \text{with} \quad k \equiv l \pmod{2}$$

for rational integers k and l . Since $\beta\varepsilon^{+2} = (7x \pm 12y) + (7y + 4x)\sqrt{3}$, we have $7y \pm 4x \geq y$, i.e., $3y \geq 2|x|$; and hence $k \geq 2|l|$. For the case $\beta < 0$, we have $y > 0$, $x \equiv 1 \pmod{6}$ and $x \equiv y + 2 \pmod{4}$. Hence we put

$$x = 6l + 1, \quad y = 2k + 1 \quad \text{with} \quad k \not\equiv l \pmod{2}$$

for rational integers k and l . Since $\beta\varepsilon^{+2} = (7x \mp 12y) + (-7y \pm 4x)\sqrt{3}$, we also have the following as a fundamental domain: $k \geq 2|l|$. Therefore we obtain the following expression of $\theta_F(\tau)$:

$$\theta_F(\tau) = \sum_{\substack{k, l \in \mathbf{Z} \\ k \geq 2|l|}} (-1)^{k+l} q^{(3(2k+1)^2 - (6l+1)^2)/2, 4}$$

For comparison, we write down the expression of the above right-hand side by Hecke's modular form:

$$\mathcal{D}_-(12\tau; 1 + \sqrt{3}, (1 + \sqrt{3}), \sqrt{12}) = \sum_{\substack{k, l \in \mathbf{Z} \\ k \geq 2|l|}} (-1)^{k+l} q^{(3(2k+1)^2 - (6l+1)^2)/2}.$$

By combining the above results and the identity (4), we have the following remarkable identities:

$$\begin{aligned} \theta_F(\tau) &= \mathcal{D}_+(12\tau; 1, \sqrt{12}) = \sum_{\substack{x, y \in \mathbf{Z} \\ x \geq 4|y|, (x, 6) = 1}} \left(\frac{x}{3}\right) q^{x^2 - 12y^2} \\ &= \sum_{\substack{k, l \in \mathbf{Z} \\ k \geq 2|l|}} (-1)^{k+l} q^{(3(2k+1)^2 - (6l+1)^2)/2} \\ &= \theta_k(\tau) = \frac{1}{2} \sum_{\substack{x, y \in \mathbf{Z} \\ (x, 3) = 1, x \equiv y \pmod{2}}} (-1)^y q^{x^2 + 9y^2} = \eta^2(12\tau), \end{aligned}$$

where $\eta(\tau)$ is Dedekind's eta function. In exactly the same way as for $\theta_k(\tau)$, we obtain

$$\begin{aligned} \theta_E(\tau) &= \sum_{k, l \in \mathbf{Z}} (-1)^{k+l} q^{(6k+1)^2 + 12l^2} \\ &= \eta(24\tau)\theta_0(24\tau) (= \eta^{12}(12\tau)), \end{aligned}$$

where

⁴⁾ Cf. Rogers ([45], p. 323).

$$\theta_0(\tau) = \sum_{m \in \mathbb{Z}} (-1)^m e^{\pi i m^2 \tau}.$$

2. We set $F = \mathcal{Q}(\sqrt{2})$ and $\mathfrak{f} = (4)$. The fundamental unit of F is given by $\varepsilon = 1 + \sqrt{2}$ and satisfies $N(\varepsilon) = -1$ and $\varepsilon^4 \equiv 1 \pmod{\mathfrak{f}}$. Thus, in the same way as for the first example, we have

$$\begin{cases} k = \mathcal{Q}(\sqrt{-2}), & c = (4), \\ E = \mathcal{Q}(\sqrt{-1}), & g = (4(1 + \sqrt{-1})), \\ K = k(\sqrt{\varepsilon}); \end{cases}$$

and obtain the following identities:

$$\begin{aligned} \theta_F(\tau) &= \mathcal{D}_+(8\tau; 2 + \sqrt{2}, 2\sqrt{8}) \\ &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \geq 6|y|, (x, 2) = 1}} \left(\frac{-1}{x}\right) q^{x^2 - 32y^2} = \sum_{\substack{m, n \in \mathbb{Z} \\ n \geq 3|m|}} (-1)^n q^{(2n+1)^2 - 32m^2} \\ = \theta_k(\tau) &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \equiv 1 \pmod{4}}} (-1)^y q^{x^2 + 8y^2} \\ &= \sum_{m, n \in \mathbb{Z}} (-1)^n q^{(4m+1)^2 + 8n^2} = \eta(8\tau)\eta(16\tau) \\ = \theta_E(\tau) &= \sum_{m, n \in \mathbb{Z}} (-1)^{m+n} q^{(4m+1)^2 + 16n^2}. \end{aligned}$$

$$3. \begin{cases} F = \mathcal{Q}(\sqrt{5}), & \mathfrak{f} = (4); \varepsilon = \frac{1 + \sqrt{5}}{2}, N(\varepsilon) = -1, \varepsilon^6 \equiv 1 \pmod{\mathfrak{f}}, \\ k = \mathcal{Q}(\sqrt{-5}), & c = (2), \\ E = \mathcal{Q}(\sqrt{-1}), & g = (10), \\ K = k(\sqrt{\varepsilon}). \end{cases}$$

$$\begin{aligned} \theta_F(\tau) &= \frac{1}{2} \mathcal{D}_+(4\tau; (5 + \sqrt{5})/2, 4\sqrt{5}) \\ &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \geq 5|y|, (x, 2) = 1}} (-1)^{y + (x-1)/2} q^{x^2 - 20y^2} \\ &= \sum_{\substack{k, l \in \mathbb{Z} \\ 2k \geq l \geq 0}} (-1)^k q^{(5(2k+1)^2 - (2l+1)^2)/4} \\ = \theta_k(\tau) &= \frac{1}{2} \sum_{\substack{x, y \in \mathbb{Z} \\ x \not\equiv y \pmod{2}}} (-1)^y q^{x^2 + 5y^2}. \end{aligned}$$

The second expression of $\theta_k(\tau)$ is obtained as follows: It is clear that $H_k(c)$ is a cyclic group of order 4 and

$$H_k(c) = \langle \lambda \rangle, \quad \lambda = [3, 1 + \sqrt{-5}].$$

By the result in Section 3.3., we have also

$$(5) \quad L_k(s, \xi) = \sum_{\substack{\alpha \in (1) \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s} - \sum_{\substack{\alpha \in \lambda^2 \\ \alpha \subset \mathfrak{o}_k}} N(\alpha)^{-s}.$$

In the following we shall calculate the right-hand side of this equality. We can put

$$\alpha = (\mu), \quad \mu = a + b\sqrt{-5} \quad (a, b \in \mathbf{Z}).$$

Thus

$$\begin{cases} \alpha \in (1) \longleftrightarrow \mu \equiv 1 \pmod{2} & \longleftrightarrow a \equiv 1 \text{ and } b \equiv 0 \pmod{2}, \\ \alpha \in \lambda^2 \longleftrightarrow \mu \equiv 2 - \sqrt{-5} \pmod{2} & \longleftrightarrow a \equiv 0 \text{ and } b \equiv 1 \pmod{2}. \end{cases}$$

The contribution of ideals α divided by λ to the first sum in (5) cancels that to the second sum in (5). Therefore we may consider the ideals α with $(\alpha, \lambda) = 1$ in the above sum (5). Hence, if we put $\mu = (2a + 1) + 2b\sqrt{-5}$ ($a, b \in \mathbf{Z}$), we have $2(a - b) + 1 \equiv 0 \pmod{3}$. On the other hand,

$$(1 - \sqrt{-5})\mu = (2a + 10b + 1) + (2(b - a) - 1)\sqrt{-5}.$$

Put $s = b - a$ and $t = a + 5b$, then $t \equiv 5s \pmod{6}$. Therefore we put $s = u + 8m$ and $t = v + 6n$. Then $v \equiv 5u \pmod{6}$ ($0 \leq u, v \leq 5$). Hence

$$2(b - a) \equiv 1 \pmod{3} \quad 2u - 1 \equiv 0 \pmod{3} \quad u = 2, 5.$$

Therefore

$$(u, v) = (0, 0), (1, 5), (3, 3) \text{ and } (4, 2);$$

and

$$N(\mu) = \{(12n + 2v + 1)^2 + 5(12m + 2u - 1)^2\}/6.$$

Now we obtain

$$\begin{aligned} \sum_{\substack{\alpha \in (1) \\ \alpha \subset \mathfrak{o}_k \\ (\alpha, \lambda) = 1}} N(\alpha)^{-s} &= \frac{1}{2} \left\{ \sum_{m, n \in \mathbf{Z}} 2 \left(\frac{(12n + 7)^2 + 5(12m + 7)^2}{6} \right)^{-s} \right. \\ &\quad \left. + \sum_{m, n \in \mathbf{Z}} 2 \left(\frac{(12n + 1)^2 + 5(12m + 1)^2}{6} \right)^{-s} \right\} \\ &= \sum_{\substack{m, n \in \mathbf{Z} \\ m \equiv n \pmod{2}}} (-1)^{m+n} \left(\frac{(6n + 1)^2 + 5(6m + 1)^2}{6} \right)^{-s} \end{aligned}$$

In the same way as above, we obtain

$$\sum_{\substack{\alpha \in \mathbb{Z}^2 \\ \alpha \subset \mathbb{Q}k \\ (\alpha, \lambda) = 1}} N(\alpha)^{-s} = \sum_{\substack{m, n \in \mathbb{Z} \\ m+n \equiv 1 \pmod{2}}} \left(\frac{(6n+1)^2 + 5(6m+1)^2}{6} \right)^{-s}.$$

Therefore we have

$$L_k(s, \xi) = \sum_{m, n \in \mathbb{Z}} (-1)^{m+n} \left(\frac{(6n+1)^2 + 5(6m+1)^2}{6} \right)^{-s}$$

Hence

$$\begin{aligned} \theta_k(\tau) &= \sum_{m, n \in \mathbb{Z}} (-1)^{m+n} q^{((6n+1)^2 + 5(6m+1)^2)/6} \\ &= \eta(4\tau)\eta(20\tau). \end{aligned}$$

4. $F = \mathcal{Q}(\sqrt{21})$, $\mathfrak{f} = \left(\frac{3 + \sqrt{21}}{2} \right)$; $\varepsilon = \frac{5 + \sqrt{21}}{2} \equiv 1 \pmod{\mathfrak{f}}$,

$k = \mathcal{Q}(\sqrt{-7})$, $c = (3)$,

$E = \mathcal{Q}(\sqrt{-3})$,

$K = k(\sqrt{\alpha})$, $\alpha = \frac{3 + \sqrt{21}}{2}$.

$$\begin{aligned} \theta_r(\tau) &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \geq 7|y|, x \equiv y \pmod{2}}} \left(\frac{-x}{3} \right) q^{(x^2 - 21x^2)/4} = \frac{1}{2} \vartheta_+(3\tau; (7 + \sqrt{21})/2, \sqrt{21}) \\ &= \theta_k(\tau) = \frac{1}{2} \sum_{\substack{x, y \in \mathbb{Z} \\ x \equiv y \pmod{2}}} \sigma(x, y) q^{(x^2 + 7y^2)/4}, \end{aligned}$$

where

$$\sigma(x, y) = \begin{cases} 1, & \text{if } 3 \mid y \text{ and } 3 \nmid x, \\ -1, & \text{if } 3 \mid x \text{ and } 3 \nmid y, \\ 0, & \text{otherwise.} \end{cases}$$

On the other hand, after a computation similar to that in Example 3, we find

$$\begin{aligned} \theta_k(\tau) &= \sum_{m, n \in \mathbb{Z}} (-1)^{m+n} q^{((6m+1)^2 + 7(6n-1)^2)/8} \\ &= \eta(3\tau)\eta(21\tau). \end{aligned}$$

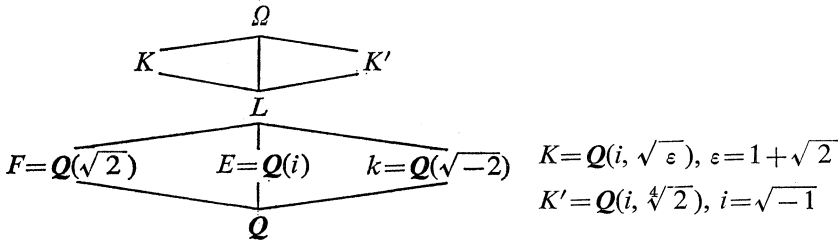
Remark 2. The indefinite representations in Example 1–3 were discovered by Kac-Peterson ([35]) by using the general theory of string functions for infinite-dimensional affine Lie algebras. A similar result was obtained for some other cases ([33]).

Remark 3. $\eta(\tau)\eta(23\tau)$, $\eta(2\tau)\eta(22\tau)$ and $\eta(6\tau)\eta(18\tau)$ are of D_3 -type and hence can not be expressed by indefinite theta series.

Remark 4. Biquadratic residue mod p and cusp forms of weight 1. In example 2, we have obtained the following identity

$$(6) \quad \sum_{m,n \in \mathbb{Z}} (-1)^n q^{(4m+1)^2 + 8n^2} = \sum_{m,n \in \mathbb{Z}} (-1)^{m+n} q^{(4m+1)^2 + 16n^2},$$

by intermediating the function $\theta_F(\tau)$. This identity appeared for the first time in Jacobi's memoir and gives a generalization of the equivalence of Gauss' two criteria for the biquadratic residuacity of 2. In the following, we shall discuss more precisely this fact from our point of view. Consider the following diagram:



Then, at the same time, Ω is the maximal ray class field over $F \pmod{4\sqrt{2}} (\infty_1)(\infty_2)$, over $k \pmod{4\sqrt{-2}}$ and over $E \pmod{8}$. Let p and r be distinct primes such that $p \equiv r \equiv 1 \pmod{4}$. We write $\left(\frac{r}{p}\right)_4 = 1$ or -1 , according as r is or is not a fourth-power residue mod p . Then it is easily checked that

$$p \text{ splits completely in } L \iff \left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = 1$$

$$\iff p \equiv 1 \pmod{8} \iff p = (4a+1)^2 + 8b^2 \iff p = (4\alpha+1)^2 + 16\beta^2;$$

and moreover

$$(7) \quad \left(\frac{\epsilon}{p}\right) = 1 \iff p \text{ splits completely in } K$$

$$\iff b \equiv 0 \pmod{2} \iff \alpha + \beta \equiv 0 \pmod{2},$$

and

$$(8) \quad \left(\frac{2}{p}\right)_4 = 1 \iff p \text{ splits completely in } K'$$

$$\iff a \equiv 0 \pmod{2} \iff \beta \equiv 0 \pmod{2}.$$

The above identity (6) gives a generalization of the equivalence (7); and the following identity gives a generalization of (8):

$$\begin{aligned} \sum_{a, \beta \in \mathbb{Z}} (-1)^\beta q^{(4a+1)^2 + 16\beta^2} &= \sum_{a, b \in \mathbb{Z}} (-1)^a q^{(4a+1)^2 + 8b^2} \\ &= \frac{1}{2} \theta_2(8\tau) \theta_0(32\tau), \end{aligned}$$

where

$$\theta_2(\tau) = \sum_{m \equiv 1 \pmod{2}} e^{\pi i m^2 \tau / 4}.$$

We shall discuss a more general case in the second half of this chapter.

§ 3.5. Higher reciprocity laws for some real quadratic fields

Let F be a real quadratic field satisfying the conditions (1) and (2). Then there exists an imaginary quadratic field k , and two L -functions associated with F and k are coincident. Suppose that K/k is a cyclic extension and K/\mathbb{Q} a dihedral extension. Let $f(x)$ be a defining polynomial with integer coefficients of K/\mathbb{Q} through the real quadratic field F . Then we have the following higher reciprocity law for $f(x)$:

Theorem 3.2. $\text{Spl } \{f(x)\} = \{p : \text{prime} \mid p \nmid D_f, a(p) = 2\}$, where D_f denotes the discriminant of f , and $a(p)$ denotes p th Fourier coefficient of Hecke's indefinite modular form $\theta_F(\tau)$ associated with F .

Proof. We put

$$\theta_k(\tau) = \sum_{\alpha \in \mathcal{O}_k} \xi(\alpha) q^{N(\alpha)} = \sum_{n=1}^{\infty} b(n) q^n.$$

Let \mathfrak{p} be any prime ideal of k unramified for K/k . Then we know that

- (i) $\xi(\mathfrak{p}) = 1 \iff \mathfrak{p} \in (1) \iff \mathfrak{p}$ splits completely in K ;
- (ii) $\xi(\mathfrak{p}) = -1 \iff \mathfrak{p} \in \lambda^2 \iff \mathfrak{p}$ splits completely in L/k and remains prime in K/L ;
- (iii) $\xi(\mathfrak{p}) = i$ or $-i \iff \mathfrak{p} \in \lambda^2$ or $\mathfrak{p} \in \lambda^3 \iff \mathfrak{p}$ remains prime in K .

Let p be a prime number and $p = \mathfrak{p}\mathfrak{p}'$ in k , where \mathfrak{p}' denotes the conjugate of \mathfrak{p} . Then

$$\mathfrak{p} \in (1) \implies b(p) = 2;$$

and vice versa. Let $F(x)$ be a defining polynomial with integer coefficients of K/k . Then it is easy to see that

$$\text{Spl } \{F(x)\} = \{p \mid p \nmid D_F, b(p) = 2\},$$

where D_F denotes the discriminant of F . On the other hand,

$$\begin{aligned} & \text{Spl} \{f(x)\} \cup \{p \mid p \text{ unramified, } p \nmid D_f\} \\ & = \text{Spl} \{F(x)\} \cup \{p \mid p \text{ unramified, } p \nmid D_p\}; \end{aligned}$$

and by Theorem 3.1, $b(p) = a(p)$ for all p . Hence we obtain

$$\text{Spl} \{f(x)\} = \{p \mid p \nmid D_f, a(p) = 2\}.$$

Example 5. We shall use the same symbols as in Example 1. Then we have the following defining equation of K/k :

$$F(x) = x^4 - 6x^2 - 3.$$

On the other hand a defining equation of K/F is given by

$$f_1(x) = x^4 - 4(1 + \sqrt{3})x^2 + 4(2 + \sqrt{3})^2.$$

Therefore the following is a defining equation on K/\mathbf{Q} through the field F :

$$\begin{aligned} f(x) &= f_1(x) \cdot f_1(x)' \\ &= x^8 - 8x^6 + 24x^4 + 160x^2 + 16. \end{aligned}$$

Hence

$$\begin{aligned} \text{Spl} \{F(x)\} &= \text{Spl} \{f(x)\} = \{p \mid a(p) = 2\} \\ &= \{p \mid p = u^2 + v^2, u \equiv 0 \pmod{6}, u, v \in \mathbf{Z}\}, \end{aligned}$$

where

$$\theta_F(\tau) = \mathcal{G}_+(12\tau; 1, \sqrt{12}) = \sum_{n=1}^{\infty} a(n)q^n.$$

Remark 5. For the defining polynomial $f(x)$ in Theorem 3.2, the following assertions hold:

- 1) $f(x) \pmod{p}$ has exactly 2 distinct quartic factors over F_p
 $\leftrightarrow a(p) = 0$ and $a(p^2) = -1$;
- 2) $f(x) \pmod{p}$ has exactly 4 distinct quadratic factors over F_p
 $\leftrightarrow 'a(p) = -2'$ or $'a(p) = 0$ and $a(p^2) = 1'$.

§ 3.6. Cusp forms of weight 1 related to quartic reisuacity

Let m be a positive square-free integer and ε_m be the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{m})$. We consider only those m for which ε_m has norm $+1$. Let K be the Galois extension of degree 16 over \mathbf{Q} generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$ and we put $G = \text{Gal}(K/\mathbf{Q})$. Then the group G is generated by three elements σ, ϕ and ρ in such way that

$$\begin{aligned} \sigma(\sqrt[4]{\varepsilon_m}) &= \sqrt{-1} \sqrt[4]{\varepsilon_m}, \\ \phi(\sqrt[4]{\varepsilon_m}) &= \sqrt[4]{\varepsilon_m}^{-1}, \\ \rho(\sqrt{-1}) &= -\sqrt{-1}, \end{aligned}$$

and has defining relations:

$$\sigma^4 = \phi^2 = \rho^2 = 1, \quad \phi\rho = \rho\phi, \quad \rho\sigma\rho = \phi\sigma\phi = \sigma^3.$$

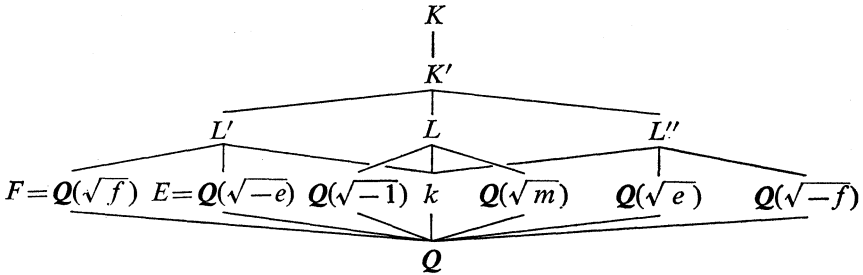
The group G has three abelian subgroups of index 2 in G , which are the following:

$$\begin{aligned} H_k &= \langle \sigma, \phi\rho \rangle \longleftrightarrow k = \mathbf{Q}(\sqrt{-m}), \\ H_F &= \langle \sigma^2, \phi, \rho \rangle \longleftrightarrow F = \mathbf{Q}(\sqrt{t+2}), \\ H_E &= \langle \sigma^2, \sigma\phi, \sigma\rho \rangle \longleftrightarrow E = \mathbf{Q}(\sqrt{-m(t+2)}), \end{aligned}$$

where $t = \text{tr}(\varepsilon_m)$. Let f and e be the square-free part of $t+2$ and $m(t+2)$, respectively, and put

$$\begin{aligned} K' &= \mathbf{Q}(\sqrt{-1}, \sqrt{\varepsilon_m}), & L &= \mathbf{Q}(\sqrt{-1}, \sqrt{-m}), \\ L' &= \mathbf{Q}(\sqrt{-m}, \sqrt{f}), & L'' &= \mathbf{Q}(\sqrt{-m}, \sqrt{-f}). \end{aligned}$$

Then we have the following diagram:



By this diagram, we have the following equivalence for any odd prime l :

$$(9) \quad l \text{ splits completely in } K' \longleftrightarrow \left(\frac{-1}{l}\right) = \left(\frac{f}{l}\right) = \left(\frac{e}{l}\right) = 1,$$

where $\left(\frac{*}{l}\right)$ denotes the Legendre symbol. The group G has the following eight representations γ_j of degree 1, where $j=1, \dots, 8$.

	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
σ	1	1	1	1	-1	-1	-1	-1
ϕ	1	1	-1	-1	1	1	-1	-1
ρ	1	-1	1	-1	1	-1	1	-1

The group G has just two irreducible representations of degree 2, which have determinant γ_4 . If we denote by ψ_0 the one of these, then the other is $\psi_0 \otimes \gamma_3$. Let σ_l denote the Frobenius substitution associated with l in K . Then we have the following table which gives the correspondence between quadratic subfields of K and $\gamma_j (2 \leq j \leq 8)$.

	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
$\gamma_j(\sigma_l)$	$\mathbf{Q}(\sqrt{-1})$ $\left(\frac{-1}{l}\right)$	$\mathbf{Q}(\sqrt{m})$ $\left(\frac{m}{l}\right)$	k $\left(\frac{-m}{l}\right)$	F $\left(\frac{f}{l}\right)$	$\mathbf{Q}(\sqrt{-f})$ $\left(\frac{-f}{l}\right)$	$\mathbf{Q}(\sqrt{e})$ $\left(\frac{e}{l}\right)$	E $\left(\frac{-e}{l}\right)$

Put $\psi_1 = \psi_0 \otimes \gamma_3$ and let $L(s, \psi_0, K/\mathbf{Q})$ (resp. $L(s, \psi_1, K/\mathbf{Q})$) denote the Artin L -function associated with ψ_0 (resp. ψ_1), and let $\theta(\tau; \psi_0)$ (resp. $\theta(\tau; \psi_1)$) denote the Mellin transformation of $L(s, \psi_0, K/\mathbf{Q})$ (resp. $L(s, \psi_1, K/\mathbf{Q})$). Then we can define the following function:

$$\theta(\tau; K) = \frac{1}{2} \{ \theta(\tau; \psi_0) + \theta(\tau; \psi_1) \}.$$

Let N denote the L.C.M. of the conductor of ψ_0 and that of ψ_1 . Then the function $\theta(\tau; K)$ is a cusp form of weight 1 on the congruence subgroup $\Gamma_0(N)$ with the character $\left(\frac{-m}{l}\right)$.

Let M be one of the three quadratic fields k, E and F . Then K is abelian over M . Let \mathfrak{o}_M be the ring of integers of M and \mathfrak{a} an ideal of \mathfrak{o}_M . If M is imaginary (resp. real), then $H_M(\mathfrak{a})$ denotes the group of ray classes (resp. narrow ray classes) modulo \mathfrak{a} of M . Let \mathfrak{b} be an ideal of M prime to \mathfrak{a} and $[\mathfrak{b}]$ the class in $H_M(\mathfrak{a})$ represented by \mathfrak{b} . If in particular b is an element of M , then the ideal class $[(b)]$ represented by the principal ideal (b) is abbreviated as $[b]$. Let $\mathfrak{f}(K/M)$ (resp. $\mathfrak{f}(K/M)$) be the conductor (resp. the finite part of conductor) of K over M . Furthermore we denote by $C_M(K)$ (resp. $C_M(K')$) the subgroup of $H_M(\mathfrak{f}(K/M))$ corresponding to K (resp. K'). The restriction ψ_0 (resp. ψ_1) to the abelian Galois group $G(K/M)$ decomposes into distinct linear representations ξ_M and ξ'_M (resp. $\xi_M \otimes \gamma_3$ and $\xi'_M \otimes \gamma_3$) of $G(K/M)$:

$$\psi_i | G(K/M) = \xi_M \otimes \gamma_3^i + \xi'_M \otimes \gamma_3^i, \quad (i=0, 1).$$

By Artin reciprocity law, we can identify ξ_M and ξ'_M with characters of $H_M(\mathfrak{f}(K/M))$ trivial on $C_M(K)$ and so we denote these characters by the same notation. Let c_M be the finite part of conductor of ξ_M . We assume that the finite part of conductor of $\xi_M \otimes \gamma_3$ is equal to c_M . Let $\widetilde{C}_M(K)$ (resp.

$\widetilde{C}_M(K')$) be the image of $C_M(K)$ (resp. $C_M(K')$) by the canonical homomorphism of $H_M(\mathfrak{f}(K/M))$ to $H_M(c_M)$. Since K is the class field over M with conductor $\mathfrak{f}(K/M)$, the Artin L -function $L(s, \psi_0, K/\mathcal{Q})$ (resp. $L(s, \psi_1, K/\mathcal{Q})$) is coincident with the L -function $L_M(s, \xi_M)$ (resp. $L_M(s, \xi_M \otimes \gamma_3)$) of M associated with the character ξ_M (resp. $\xi_M \otimes \gamma_3$), where ξ_M (resp. $\xi_M \otimes \gamma_3$) denotes the primitive character corresponding to ξ_M (resp. $\xi_M \otimes \gamma_3$). Therefore we have three expressions of $\theta(\tau; K)$.

Proposition 3.1. *The notation and the assumption being as above, we have*

$$(10) \quad \theta(\tau; K) = \sum_{\substack{\alpha \subset \mathfrak{o}_M \\ [\alpha] \in \mathcal{O}_M(K')}} \chi_M(\alpha) q^{N_{M/\mathcal{Q}}(\alpha)} \quad (q = e^{2\pi i \tau}),$$

where

$$\chi^M(\alpha) = \begin{cases} 1, & \text{if } [\alpha] \in \widetilde{C}^M(K), \\ -1, & \text{otherwise;} \end{cases}$$

and $N_{M/\mathcal{Q}}(\alpha)$ denotes the norm of α with respect to M/\mathcal{Q} .

The proof of Proposition 3.1 is quite similar to that appeared in Section 3.3.

Let $f(x)$ be a defining polynomial of $\sqrt[4]{\varepsilon_m}$ over \mathcal{Q} . Then it is easy to see that

$$f(x) = (x^4 - \varepsilon_m)(x^4 - \varepsilon_m^{-1}) = x^8 - tx^4 + 1.$$

Let $a(n)$ be the n th Fourier coefficient of the expression

$$\theta(\tau; K) = \sum_{n=1}^{\infty} a(n) q^n.$$

Then we have the following relation:

Proposition 3.2. *Let p be any prime not dividing the discriminant D_f of $f(x)$ and F_p the p -element field. Then we have*

$$(11) \quad \#\{x \in F_p \mid f(x) = 0\} = 1 + \left(\frac{m}{p}\right) + \left(\frac{f}{p}\right) + \left(\frac{e}{p}\right) + 2a(p).$$

Proof. Let H be the group generated by ρ , say $H = \langle \rho \rangle$. Then H is the subgroup of G corresponding to $\mathcal{Q}(\sqrt[4]{\varepsilon_m})$. We denote by $1_H^{\mathcal{Q}}$ the character of G induced by the identity character of H . Then we have the following scalar product formulas:

$$(1_H^g | \gamma_i) = \begin{cases} 1, & \text{if } i=1, 3, 5, 7, \\ 0, & \text{otherwise;} \end{cases}$$

$$(1_H^g | \chi_i) = 1 \quad (i=0, 1),$$

where χ_0 (resp. χ_1) denotes the character of ψ_0 (resp. ψ_1). Therefore, we have

$$1_H^g(\sigma_p) = \sum_{\substack{1 \leq i \leq 7 \\ i: \text{ odd}}} \gamma_i(\sigma_p) + \chi_0(\sigma_p) + \chi_1(\sigma_p)$$

$$= 1 + \left(\frac{m}{p}\right) + \left(\frac{f}{p}\right) + \left(\frac{e}{p}\right) + 2a(p).$$

On the other hand, it is easy to see that the left hand side of (11) is equal to $1_H^g(\sigma_p)$. This proves our proposition.

By Propositions 3.1 and 3.2 we have the following

Corollary. $\text{Spl} \{f(x)\} = \{p \mid p \nmid D_f, a(p)=2\}$.

§ 3.7. Fundamental Lemmas

In this section, we shall determine the conductors $\mathfrak{f}(K/M)$, $\mathfrak{f}(K'/M)$, $\mathfrak{f}(L'/M)$ and $\mathfrak{f}(L/M)$. Let \mathfrak{R} , \mathfrak{L} and \mathfrak{F} be fields such that $\mathfrak{R} \supset \mathfrak{L} \supset \mathfrak{F}$ and $[\mathfrak{L} : \mathfrak{F}] = 2$. Assume that \mathfrak{R} is abelian over \mathfrak{F} . We denote by $\mathfrak{d}(\mathfrak{L}/\mathfrak{F})$ the different of \mathfrak{L} over \mathfrak{F} . For a prime ideal \mathfrak{g} of \mathfrak{L} , let $f(\mathfrak{g})$ (resp. $g(\mathfrak{g})$) denote the \mathfrak{g} -exponent of $\mathfrak{f}(\mathfrak{R}/\mathfrak{L})$ (resp. $\mathfrak{d}(\mathfrak{L}/\mathfrak{F})$) and put

$$e(\mathfrak{g}) = \max \{0, g(\mathfrak{g}) - f(\mathfrak{g})\}.$$

Then we have the following

Lemma 1. $\mathfrak{f}(\mathfrak{R}/\mathfrak{F}) = \mathfrak{f}(\mathfrak{R}/\mathfrak{L})\mathfrak{d}(\mathfrak{L}/\mathfrak{F}) \prod_{\mathfrak{g}} \mathfrak{g}^{e(\mathfrak{g})}$.

We assume that \mathfrak{L} is a Galois extension over \mathcal{O} . Let $\mathfrak{o}_{\mathfrak{g}}$ be the ring of integers of \mathfrak{L} and let \mathfrak{p} be a prime ideal of $\mathfrak{o}_{\mathfrak{g}}$ dividing 2. We denote by $e_{\mathfrak{g}}$ the ramification exponent of \mathfrak{p} . Let $\mathfrak{o}_{\mathfrak{p}}$ denote the completion of $\mathfrak{o}_{\mathfrak{g}}$ with respect to \mathfrak{p} and $\Pi_{\mathfrak{p}}$ a prime element of $\mathfrak{o}_{\mathfrak{p}}$. Furthermore, for $\xi \in \mathfrak{o}_{\mathfrak{p}}^{\times}$, we put

$$S_{\mathfrak{p}}(\xi) = \max \{t \in \mathbb{Z}^+ \mid \xi \equiv \text{square mod } \Pi_{\mathfrak{p}}^t\}.$$

Then we have

Lemma 2. *If $S_{\mathfrak{p}}(\xi) < 2e_{\mathfrak{g}}$, then there exists uniquely the odd integer $t (< 2e_{\mathfrak{g}})$ such that*

$$\xi = \eta^2 + \delta \Pi_{\mathfrak{p}}^t \quad (\eta, \delta \in \mathfrak{o}_{\mathfrak{p}}^{\times});$$

and this uniquely determined t is equal to $S_{\mathfrak{p}}(\xi)$.

Lemma 3. Put

$$t_{\mathfrak{p}}(\xi) = \min \{n \in \mathbf{Z} \mid \xi \Pi_{\mathfrak{p}}^{2n} \equiv \text{square mod } \Pi_{\mathfrak{p}}^{2e_{\mathfrak{p}}}, 0 \leq n \leq e_{\mathfrak{p}}\}.$$

If $S_{\mathfrak{p}}(\xi) < 2e_{\mathfrak{p}}$, then we have

$$S_{\mathfrak{p}}(\xi) = 2e_{\mathfrak{p}} + 1 - 2t_{\mathfrak{p}}(\xi).$$

Let α be an element of $\mathfrak{o}_{\mathfrak{g}}$ such that (α) is a square-free ideal with $((\alpha), 2) = 1$ and put $\mathfrak{K} = \mathfrak{L}(\sqrt{\alpha})$. We assume that \mathfrak{K} is a Galois extension over \mathfrak{Q} . Then $S_{\mathfrak{p}}(\alpha)$ is independent of \mathfrak{p} chosen. Since \mathfrak{K} and \mathfrak{L} are the Galois extension over \mathfrak{Q} , the \mathfrak{p} -exponent $f(\mathfrak{p})$ of $\mathfrak{f}(\mathfrak{K}/\mathfrak{L})$ does not depend on \mathfrak{p} chosen. Thus we can put $S_{\mathfrak{g}}(\alpha) = S_{\mathfrak{p}}(\alpha)$ and $f(2) = f(\mathfrak{p})$.

Lemma 4. (i) The prime ideal \mathfrak{p} is ramified for $\mathfrak{K}/\mathfrak{L}$ if and only if $S_{\mathfrak{g}}(\alpha) < 2e_{\mathfrak{g}}$.

(ii) If $S_{\mathfrak{g}}(\alpha) < 2e_{\mathfrak{g}}$, then $S_{\mathfrak{g}}(\alpha)$ is equal to the odd number $t (< 2e_{\mathfrak{g}})$ determined by

$$\alpha = \eta^2 + \delta \Pi_{\mathfrak{p}}^t \quad (\eta, \delta \in \mathfrak{o}_{\mathfrak{p}}^{\times});$$

and moreover

$$f(2) = 2e_{\mathfrak{g}} + 1 - S_{\mathfrak{g}}(\alpha).$$

Proof. By the assumption on α , we have

$$\mathfrak{o}_{\mathfrak{K}} = \left\{ \frac{1}{2}(a + b\sqrt{\alpha}) \mid a, b \in \mathfrak{o}_{\mathfrak{g}}, a^2 - \alpha b^2 \equiv 0 \pmod{4} \right\}.$$

Denote by \mathfrak{P} a prime ideal of \mathfrak{K} dividing \mathfrak{p} . Let α be an ideal of \mathfrak{K} and denote by $\mathfrak{W}_{\mathfrak{P}}(\alpha)$ the \mathfrak{P} -exponent of α , and let ε be a generator of $G(\mathfrak{K}/\mathfrak{L})$. Then, by the definition of $f(\mathfrak{p})$,

$$(12) \quad f(2) = \min_{\xi \in \mathfrak{o}_{\mathfrak{K}}} \mathfrak{W}_{\mathfrak{P}}(\xi - \xi^{\varepsilon}).$$

Denote by X (resp. $X_{\mathfrak{p}}$) the group of all elements b of $\mathfrak{o}_{\mathfrak{g}}$ satisfying the condition

$$\alpha b^2 \equiv \text{square mod } 4 \text{ (resp. mod } \mathfrak{p}^{2e_{\mathfrak{g}}}).$$

Let $\mathfrak{A}_p(b)$ denote the p -exponent of (b) . Then, by (12), we have

$$f(2) = 2 \min_{b \in X} \mathfrak{A}_p(b) = 2 \min_{b \in X_p} \mathfrak{A}_p(b).$$

Therefore,

$$\begin{aligned} \mathfrak{p} \text{ is unramified for } \mathfrak{K}/\mathfrak{L} &\longleftrightarrow f(2) = 0 \\ &\longleftrightarrow \alpha \text{ is square mod } \mathfrak{p}^{2e} \longleftrightarrow S_g(\alpha) \geq 2e_g. \end{aligned}$$

If \mathfrak{p} is ramified for $\mathfrak{K}/\mathfrak{L}$, then

$$\min_{b \in X_p} \mathfrak{A}_p(b) = t_p(\alpha).$$

By Lemma 3, $S_g(\alpha) = 2e_g + 1 - f(2)$. Hence by Lemma 2 the assertion (ii) is proved.

Now we assume that $\mathfrak{L}(\sqrt[4]{\alpha})$ is a Galois extension over \mathfrak{Q} . It is easy to see that there exists a subgroup R of \mathfrak{o}_p^\times with order $\#(\mathfrak{o}_g/\mathfrak{p}) - 1$ such that $R^* = R \cup \{0\}$ is a complete system of coset representatives of $\mathfrak{o}_g \text{ mod } \mathfrak{p}$. Put

$$t = \min \{2e_g, S_g(\alpha)\} \quad \text{and} \quad u = [(t+1)/2].$$

Then there exists elements a_0, a_1, \dots, a_{u-1} of R^* such that

$$\alpha \equiv (a_0 + a_1\Pi_p + \dots + a_{u-1}\Pi_p^{u-1})^2 \text{ mod } \Pi_p^t.$$

Lemma 5. (i) *If \mathfrak{p} is unramified for $\mathfrak{K}/\mathfrak{L}$ and there exists a nonzero element in $\{a_i \mid i: \text{odd}\}$, then*

$$S_{\mathfrak{K}}(\sqrt{\alpha}) = \min \{i: \text{odd} \mid a_i \neq 0\}.$$

(ii) *If \mathfrak{p} is ramified for $\mathfrak{K}/\mathfrak{L}$ and there exists a prime element Π_p of \mathfrak{o}_p such that $\Pi_p \equiv \Pi_{\mathfrak{p}}^2 \text{ mod } \Pi_{\mathfrak{p}}^{t+1}$, then*

$$S_{\mathfrak{K}}(\sqrt{\alpha}) = S_g(\alpha).$$

Now we put

$$\mathfrak{L} = L \text{ or } K', \quad \text{and} \quad \alpha = \varepsilon_m.$$

From now on we assume that m is prime number p with $p \equiv 3 \pmod{4}$. We put $\varepsilon_p = \varepsilon = A + B\sqrt{p}$. Then it is easy to verify that A is an even number. Since $A^2 - pB^2 = 1$, we have $(A+1)(A-1) = pB^2$. Therefore we can put

$$A - 1 = r^2u,$$

$$A + 1 = s^2v,$$

with $(ru, sv) = 1$, $rs = B$ and $uv = p$ ($r, s, u, v \in \mathbb{Z}^+$). Hence, $2 = s^2v - r^2u$. By considering this relation mod 8, we have

$$(u, v) = \begin{cases} (1, p), & \text{if } p \equiv 3 \pmod{8}, \\ (p, 1), & \text{if } p \equiv 7 \pmod{8}. \end{cases}$$

Since $t = tr(\varepsilon) = 2A$, we have $t + 2 = 2s^2v$. Hence

$$(f, e) = \begin{cases} (2p, 2), & \text{if } p \equiv 3 \pmod{8}, \\ (2, 2p), & \text{if } p \equiv 7 \pmod{8}. \end{cases}$$

Therefore we have the following lemma.

Lemma 6. *With F and E as in Section 3.6, we have*

$$(F, E) = \begin{cases} (\mathcal{Q}(\sqrt{2p}), \mathcal{Q}(\sqrt{-2})), & \text{if } p \equiv 3 \pmod{8} \\ (\mathcal{Q}(\sqrt{2}), \mathcal{Q}(\sqrt{-2p})), & \text{if } p \equiv 7 \pmod{8}. \end{cases}$$

Now we shall calculate the conductors $\mathfrak{f}(K/M)$, $\mathfrak{f}(K'/M)$, $\mathfrak{f}(L/M)$ and $\mathfrak{f}(L'/M)$. Because the method of calculation is very similar for each of three cases, we shall give the details only for the case of $M = k$. If we put $\mathfrak{L} = L$, then $K' = L(\sqrt{\varepsilon})$. We can take $e_L = 2$ and $\Pi_p = 1 - \sqrt{p}$. Therefore, $\varepsilon \equiv 1 - \Pi_p \pmod{2}$. By Lemma 4, $S_L(\varepsilon) = 1$ and hence $S_{K'}(\sqrt{\varepsilon}) = 1$ by (ii) of Lemma 5. Therefore, again by Lemma 4, we have $f_{K'}(2) = 5 - 1 = 4$. Since prime factors of 2 are only ramified for K'/L , we have $\mathfrak{f}(K'/L) = (4)$, and hence $\mathfrak{d}(K'/L) = (3)$. By $e_{K'} = 4$, $f_K(2) = 9 - 1 = 8$. Therefore $\mathfrak{f}(K/K') = (4)$. Consequently, by Lemma 1, we have

$$\begin{aligned} \mathfrak{f}(K/L) &= \mathfrak{f}(K/K')\mathfrak{d}(K/L) \\ &= (4)(2) = (8). \end{aligned}$$

Thus we obtain the following:

$$\begin{cases} \mathfrak{f}(K/k) = \mathfrak{f}(K/L)\mathfrak{d}(L/k) = (16), \\ \mathfrak{f}(K'/k) = \mathfrak{f}(K'/L)\mathfrak{d}(L/k) = (8), \\ \mathfrak{f}(L/k) = \mathfrak{d}(L/k)^2 = (4). \end{cases}$$

Therefore our required conductors are as follows.

M	$\mathfrak{f}(K/M)$	$\mathfrak{f}(K'/M)$	$\mathfrak{f}(L'/M)$	$\mathfrak{f}(L/M)$	c_M
k	16	8	8	4	16
F	$p \equiv 3 \pmod{8}$	$4\mathfrak{p}_2\infty_1\infty_2$	$(2)\infty_1\infty_2$	$\infty_1\infty_2$	$4\mathfrak{p}_2$
	$p \equiv 7 \pmod{8}$	$(4\sqrt{2}p)\infty_1\infty_2$	$(2p)\infty_1\infty_2$	$(p)\infty_1\infty_2$	$4\mathfrak{p}$
E	$p \equiv 3 \pmod{8}$	$4\sqrt{-2}p$	$2p$	p	$4\mathfrak{p}$
	$p \equiv 7 \pmod{8}$	$4\mathfrak{p}_2$	2	1	$4\mathfrak{p}_2$

In the above table, \mathfrak{p} denotes a prime ideal of M dividing p , and \mathfrak{p}_2 denotes a prime ideal of M dividing 2. Further ∞_i ($i=1, 2$) denote two infinite places of F .

§ 3.8. Three expressions of $\Theta(\tau; K)$

For an integral ideal α of M , if M is imaginary (resp. real), then $P_M(\alpha)$ denotes the subgroup of $H_M(\alpha)$ generated by principal classes (resp. principal classes represented by totally positive elements). We write simply H_M and P_M in place of $H_M(\mathfrak{f}(K/M))$ and $P_M(\mathfrak{f}(K/M))$ respectively. Suppose that α divides $\mathfrak{f}(K/M)$. Then we denote by $K(\alpha)$ the kernel of the canonical homomorphism: $P_M \rightarrow P_M(\alpha)$. Moreover we put $C_M(\)^* = P_M \cap C_M(\)$. In the following, we shall obtain $C_M(K)$ and $C_M(K')$ under the assumption $p \equiv 7 \pmod{8}$.

Case 1. $M=k$ ($=\mathcal{Q}(\sqrt{-p})$).

By the assumption, we have $2 = \mathfrak{p}_2\bar{\mathfrak{p}}_2$, where $\bar{\mathfrak{p}}_2$ denotes the conjugate of \mathfrak{p}_2 . Take the two elements μ and ν of \mathfrak{o}_k such that

$$\begin{cases} \mu \equiv 5 \pmod{\mathfrak{p}_2^4}, & \nu \equiv -1 \pmod{\mathfrak{p}_2^4}, \\ \mu \equiv 1 \pmod{\bar{\mathfrak{p}}_2^4}, & \nu \equiv 1 \pmod{\bar{\mathfrak{p}}_2^4}. \end{cases}$$

Then we have

$$\begin{aligned} C_k(L)^* &= \langle [\mu], [\bar{\mu}] \rangle, \\ C_k(K')^* &= \langle [\mu]^2, [\bar{\mu}]^2, [\mu][\bar{\mu}] \rangle, \\ C_k(K)^* &\not\cong \langle [\mu]^2, [\bar{\mu}]^2 \rangle. \end{aligned}$$

Since $G(K/\mathcal{Q})$ is non-abelian and $G(K/k) \cong P_k/C_k(K)^*$, we see $[\mu]^{-1}[\bar{\mu}] \in C_k(K)^*$. Therefore, $[\mu][\bar{\mu}] \in C_k(K)^*$. Hence we have

$$C_k(K)^* = \langle [\mu][\bar{\mu}] \rangle = \langle [5] \rangle.$$

We put

$$H_k = \sum_{\mathfrak{b} \in S} [\mathfrak{b}] p_k,$$

where S denotes the index set of integral ideals \mathfrak{b} . Then

$$\begin{aligned} C_k(K') &= C_k(K) + C_k(K)[\mu]^2, \\ C_k(K) &= \sum_{\mathfrak{b} \in S} [\mathfrak{b}]^{-4} C_k(K)^*. \end{aligned}$$

Put $\omega = (1 + \sqrt{-p})/2$ and let α be an ideal of \mathfrak{o}_k with $(\alpha, 2) = 1$. Then, by the above relations, we have $[\alpha] \in C_k(K')$ if and only if there exists $\mathfrak{b} \in S$ and $\eta = x + y\omega \in \mathfrak{b}^4$ such that $x \equiv 1 \pmod{2}$, $y \equiv 0 \pmod{8}$ and $\alpha = \mathfrak{b}^{-4}(\eta)$. Moreover

$$[\alpha] \in C_k(K) \iff y \equiv 0 \pmod{16}.$$

Therefore, if $M = k$, then the right hand side of (10) is as follows:

$$(13) \quad \theta(\tau; K) = \sum_{\mathfrak{b} \in S} \sum_{4x+1+4y\sqrt{-p} \in \mathfrak{b}^4} (-1)^y q^{((4x+1)^2 + 16p^2 y^2)/N_{k/\mathcal{Q}}(\mathfrak{b})^4}.$$

Case 2. $M = F (= \mathcal{Q}(\sqrt{2}))$.

Let α be an element of \mathfrak{o}_F . Then there exists an element α^* of \mathfrak{o}_F such that

$$\begin{cases} \alpha^* \text{ is totally positive,} \\ \alpha^* \equiv \alpha \pmod{4\sqrt{2}}, \\ \alpha^* \equiv 1 \pmod{p}. \end{cases}$$

Let $p = \mathfrak{p}\bar{\mathfrak{p}}$ in F , and $r(\mathfrak{p})$ denotes a generator of the multiplicative group $(\mathfrak{o}_F/\mathfrak{p})^\times$. Take a totally positive element λ of \mathfrak{o}_F such that

$$\begin{cases} \lambda \equiv 1 \pmod{4\sqrt{2}}, \\ \lambda \equiv r(\mathfrak{p}) \pmod{\mathfrak{p}}, \\ \lambda \equiv 1 \pmod{\bar{\mathfrak{p}}}. \end{cases}$$

Then we obtain

$$C_F(L) = \langle [\varepsilon_2^*], [3^*], [5^*], [\lambda], [\bar{\lambda}], [\lambda]^2 \rangle.$$

Since the Galois group $G(K'/\mathcal{Q})$ is isomorphic to $P_F/C_F(K')$, we have

$$C_F(K') \ni [\lambda]^2, [\bar{\lambda}]^2, [\lambda]^{-1}[\bar{\lambda}].$$

Hence

$$C_F(K') = \langle [\varepsilon_2^*]^2, [3^*], [5^*], [\lambda]^2, [\bar{\lambda}]^2, [\lambda][\bar{\lambda}] \rangle.$$

Also we have

$$C_F(K) = \langle [\varepsilon_2^*]^2, [\lambda]^2, [\bar{\lambda}]^2, [3^*][\lambda][\bar{\lambda}], [5^*][\lambda][\bar{\lambda}] \rangle,$$

$$C_F(K') = C_F(K) + C_F(K)[5^*].$$

Let r be a rational integer with $r^2 \equiv 2 \pmod{p}$ and $\mu = x + y\sqrt{2}$ be a totally positive element of \mathfrak{o}_F such that $(2p, \mu) = 1$. Then we have

$$[\mu] \in C_F(K) \longleftrightarrow x: \text{ odd, } y: \text{ even} \quad \text{and} \quad \left(\frac{x^2 - 2y^2}{p}\right) = 1.$$

Further

$$[\mu] \in C_F(K) \longleftrightarrow (-1)^{v/2} \left(\frac{ry + x}{p}\right) \left(\frac{2}{x}\right) = 1.$$

We put

$$\begin{cases} E^+ = \{\varepsilon \in \mathfrak{o}_F^\times \mid \varepsilon: \text{ totally positive}\}, \\ E^0 = \{\varepsilon \in E^+ \mid \varepsilon - 1 \in \mathfrak{f}(K/F)\}, \end{cases}$$

and $e = [E^+ : E^0]$. Then, the right hand side of (10) has the following expression for $M = F$:

$$(14) \quad \Theta(\tau; K) = e^{-1} \sum_{\substack{\mu = x + 2y\sqrt{2} \\ x \equiv 1 \pmod{4} \\ N_F/Q(\mu) > 0 \\ \mu \pmod{E^0}}} (\text{sgn } x) (-1)^v \left(\frac{2ry + x}{p}\right) \left(\frac{2}{x}\right) q^{x^2 - 2y^2}.$$

Case 3. $M = E (= Q(\sqrt{-2p}))$.

By a calculation similar to that of Case 2, we have the following

$$(15) \quad \Theta(\tau; K) = \sum_{\mathfrak{a}} \sum_{4x+1+2y\sqrt{-2p} \in \mathfrak{a}} (-1)^{x+y} q^{\{(4x+1)^2 + 8y^2\}/N_E/Q(\mathfrak{a})},$$

where $\{\mathfrak{a}\}$ denotes the set of integral ideals of E which are representatives of all square classes in H_E/P_E .

Summing up (13), (14) and (15), we obtain the following theorem which is our main purpose.

Theorem 3.3. *Let p be any prime with $p \equiv 7 \pmod{8}$. Then, the notation and the assumption being kept as above, we have the three expressions of $\Theta(\tau; K)$:*

$$\begin{aligned} \Theta(\tau; K) &= \sum_{\mathfrak{a}} \sum_{4x+1+2y\sqrt{-2p} \in \mathfrak{a}} (-1)^{x+y} q^{\{(4x+1)^2 + 8py\}/N_E/Q(\mathfrak{a})} && \text{(via } E) \\ &= \sum_{\mathfrak{b}} \sum_{4x+1+4y\sqrt{-p} \in \mathfrak{b}^4} (-1)^v q^{\{4x+1\}^2 + 16py^2\}/N_E/Q(\mathfrak{b}^4)} && \text{(via } k) \end{aligned}$$

$$= e^{-1} \sum_{\substack{\mu = x + 2y\sqrt{2} \\ x \equiv 1 \pmod{4} \\ NF/Q(\mu) > 0 \\ \mu \pmod{E^0}}} (\text{sgn } x)(-1)^y \left(\frac{2ry+x}{p}\right) \left(\frac{2}{x}\right) q^{x^2-8y^2} \quad (\text{via } F).$$

Let l be an odd prime number satisfying the conditions $\left(\frac{p}{l}\right) = 1$ and $l \equiv 1 \pmod{8}$. Then we have $\left(\frac{\varepsilon_p}{l}\right) = 1$ by (9), and we have also the following from the theorem above:

$$\begin{aligned} l &= \{(4a+1)^2 + 8pb^2\}/N_{E/Q}(\alpha), \\ l &= \{(4\alpha+1)^2 + 16p\beta^2\}/N_{K/Q}(\mathfrak{b})^4, \\ l &= x^2 - 8y^2, \quad x \equiv 1 \pmod{4}, \quad \left(\frac{x^2 - 8y^2}{p}\right) = 1; \\ a(l) &= \pm 2. \end{aligned}$$

Moreover, we have the following criterions for ε_p to be a quartic residue modulo l which are our conclusion.

$$\begin{aligned} \left(\frac{\varepsilon_p}{l}\right)_4 = 1 &\longleftrightarrow a+b: \text{ even} \\ &\longleftrightarrow \beta: \text{ even} \\ &\longleftrightarrow (\text{sgn } x)(-1)^y \left(\frac{2ry+x}{p}\right) \left(\frac{2}{x}\right) = 1 \text{ and } x \equiv 1 \pmod{4} \\ &\longleftrightarrow a(l) = 2. \end{aligned}$$

For prime p with $p \equiv 3 \pmod{8}$, we shall only state the result as a remark.

Remark 6. Let $p \equiv 3 \pmod{8}$ and $p \neq 3$. Then, the following may be obtained in a way similar to the proof of the above theorem.

$$\begin{aligned} \Theta(\tau; K) &= \sum_{\substack{x, y \in \mathbb{Z} \\ x \equiv 1 \pmod{4}}} (-1)^{(x-1)/4+y} \left(\frac{x-2ry}{p}\right) q^{x^2+8y^2} \\ &= \sum_b \left\{ \sum_{\substack{\nu = (\alpha + \beta\sqrt{-p})/2 \in \mathbb{Z}^4 \\ NF/Q(\nu) \equiv 1 \pmod{8} \\ \alpha \equiv 1 \pmod{4}}} (-1)^{(\alpha-1)/4 + (N_{K/Q}(\nu)-1)/8} q^{(\alpha^2+p\beta^2)/4} N_{K/Q}(\mathfrak{b})^4 \right. \\ &\quad \left. + \sum_{4x+1+4y\sqrt{-p} \in \mathbb{Z}^4} (-1)^y q^{\{(4x+1)^2+16py^2\}/N_{K/Q}(\mathfrak{b})^4} \right\} \\ &= e^{-1} \sum_a \sum_{\substack{\mu = 4x+1+2y\sqrt{2p} \in a \\ NF/Q(\mu) > 0 \\ \mu \pmod{E^0}}} (\text{sgn } x)(-1)^{x+y} q^{\{(4x+1)^2-8py^2\}/N_{E/Q}(\alpha)}. \end{aligned}$$

Chapter 4. 2-dimensional Galois Representations and the Stark Conjecture

§ 4.1. Results of Deligne-Serre

Let \bar{Q} denote an algebraic closure of Q and put $G = \text{Gal}(\bar{Q}/Q)$. Then we have the following two theorems:

Theorem (Weil-Langlands). *Let σ be an irreducible 2-dimensional Galois representation of G with conductor N and $\varepsilon = \det(\sigma)$ odd. Assume that σ satisfies the condition*

(A): *The Artin-L-function $L(s, \sigma \otimes \lambda)$ is an entire function for all twists $\sigma \otimes \lambda$ of σ by one dimensional representation λ of G . Suppose $L(s, \sigma) = \sum_{n=1}^{\infty} a(n)n^{-s}$, and let $f(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi i n z}$. Then $f(z)$ is a normalized newform on $\Gamma_0(N)$ of weight 1 and character ε .*

Theorem (Deligne-Serre, [8]). *Let f be a normalized newform on $\Gamma_0(N)$ of weight 1 and character ε . Then there exists an irreducible odd 2-dimensional Galois representation σ of G with the conductor N and $\det(\sigma) = \varepsilon$, such that $L_f(s) = L(s, \sigma)$.*

In other words, there is a 1-to-1 correspondence between the set of normalized newforms on $\Gamma_0(N)$ of weight 1 and character ε , and the set of isomorphism classes of irreducible 2-dimensional representations of G with conductor N , determinant odd character ε , satisfying the condition (A). The finite subgroups of $GL(2, C)$ were classified by Klein; the image of

$$\delta: G \longrightarrow PGL(2, C)$$

must be

$$\delta(G) = \begin{cases} D_n, & \text{dihedral group,} \\ A_4, & \text{tetrahedral group,} \\ S_4, & \text{octahedral group,} \\ A_5, & \text{icosahedral group.} \end{cases}$$

Remark 1. Langlands and Tunnel ([54]) proved the Artin conjecture for all tetrahedral and octahedral σ by combining the above result of Deligne and Serre with a generalization of the theory of lifting automorphic forms due to Saito and Shintani.

Remark 2 (Buhler [5]). There is an icosahedral form of level 800.

Let σ be an irreducible 2-dimensional Galois representation of G with prime conductor p such that $\varepsilon = \det(\sigma)$ is odd and assume σ is non-dihedral. Then, if $p \equiv 3 \pmod{4}$, σ is of type S_4 or A_5 , and ε is the Legendre symbol $\left(\frac{n}{p}\right)$. Now we put

$$d_1 = \dim S_1(\Gamma_0(p), \varepsilon).$$

Then, Serre ([48]) obtained the following dimension formula:

$$(*) \quad d_1 = \frac{1}{2}(h-1) + 2(s+2a),$$

where h denotes the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$, s (resp. a) is the number of the normal closure of a quartic (resp. non-real quintic) fields with discriminant $-p$ (resp. p^2) whose associated representations satisfy the condition (A).

§ 4.2. The Stark conjecture in the case of weight 1

Let $\alpha \neq (1)$ be an integral ideal in $k = \mathbf{Q}(\sqrt{d})$ where $d (< 0)$ is the discriminant of k . If χ is a ray class character of $k \pmod{\alpha}$, then we may write

$$L(s, \chi) = \sum_C \chi(C) Z(s, C),$$

where C runs through the ray classes mod α and

$$Z(s, C) = \sum_{\mathfrak{b} \in C} N(\mathfrak{b})^{-s}.$$

Define $g_\chi(z)$ by the Mellin transform,

$$(2\pi)^{-s} \Gamma(s) L(s, \chi) = \int_0^\infty y^{s-1} g_\chi(iy) dy, \quad z = x + iy.$$

Then, $g_\chi(z)$ is a modular form of weight 1 on $\Gamma_1(N)$ with $N = |d|N(\alpha)$ and we have

$$L'(0, \chi) = \int_0^\infty g_\chi(iy) \frac{dy}{y}.$$

Now we are led to the following Stark conjecture ([51]).

Conjecture. *Let $f(z)$ be a cusp form of weight 1 on $\Gamma_1(N)$. Then*

$$\int_0^\infty f(iy) \frac{dy}{y} \sum_{j=1}^n \rho_j \log \varepsilon_j,$$

where the ε_j are algebraic integers and the ρ_j lie in the field generated over \mathbf{Q} by adjoining the Fourier coefficients of $f(z)$ at ∞ .

As an example, let χ be either one of the two cubic ideal class characters of $\mathbf{Q}(\sqrt{-23})$ so that

$$g_\chi(z) = \eta(z)\eta(23z),$$

where $\eta(z)$ denotes the Dedekind eta function. Then we have

$$L'(0, \chi) = \int_0^\infty g_\chi(iy) \frac{dy}{y} = \log \varepsilon_0,$$

where ε_0 is the real root of $x^3 - x - 1 = 0$.

According to the Deligne-Serre theorem, there is a normal extension K of \mathbf{Q} and an irreducible two-dimensional Galois representation σ of $\text{Gal}(K/\mathbf{Q})$ such that the Dirichlet series corresponding to $f(z)$ gives the Artin L -function $L(s, \sigma, K/\mathbf{Q})$. However from the Deligne-Serre theorem, we can expect nothing to solve the problem explicitly determining the field K by $f(z)$. The conjecture was proved by Stark when K is an abelian extension of k and it aids materially in explicitly determining K from $f(z)$.

In [6], Chinburg formulated Stark conjecture “over \mathbf{Z} ” as follows. Let $d = \sum_\sigma d_\sigma \cdot \sigma$ be a finite linear combination of ρ of dimension n and we assume $\sum_\sigma d_\sigma \cdot \sigma = \sum_\sigma d'_\sigma \cdot \sigma^\rho$ for any $\rho \in \text{Aut}(C/\mathbf{Q})$. We define $L'(s, d) = \sum_\sigma d_\sigma \cdot L'(s, \sigma)$ and $L'_d(s) = \sum_\sigma d_\sigma \cdot L'(s, \sigma) pr_\sigma$ where $pr_\sigma = \sum_{g \in \text{Gal}(K/\mathbf{Q})} \chi_\sigma(g)g$. Then for $n=1$ or 2 , $\exp(L'(0, d)) = e(d)$ is a real unit in K and $L'_d(0)v_0 = \sum_{v \in S_\infty} \log \|e(d)\|_v \cdot v$, where S_∞ is the set of infinite place of K , $\|\cdot\|_v$ is the normalized absolute value for $v \in S_\infty$ and v_0 is a fixed embedding of K into C .

Moreover, Tanigawa gave an example for two dimensional representation of S_4 -type ([52]). He considered the space of cusp forms of weight 1 on $\Gamma_0(283)$ with the character $\left(\frac{-283}{*}\right)$. This space has one primitive form h of S_3 -type and two primitive forms f and f^τ of S_4 -type, where τ is a complex conjugate. And let V and W be Galois representations attached to f and h respectively. Then $L'_d(0)$ is generated by a linear combination of $L'_d(0)$ for the following d :

- (i) $d = \delta V + \delta^\tau V^\tau$ for $\delta \in D_{\mathbf{Q}(\sqrt{-23})}^{-1}$,
- (ii) $d = W$,

$$(iii) \quad d = \frac{1}{4} (V + V^r) + \frac{1}{2} W,$$

here D_k is the different of the field k . Furthermore, he gave the minimal polynomial of $e(d)$ for the above d and checked that $e(d)$ is indeed a real unit in K .

Remark 3. The value of $L\left(\frac{1}{2}, \varepsilon\right)$

Let ε be an abelian character of a class group of a complex quadratic extension of a totally real field and $L(s, \varepsilon)$ the Artin L -function associated with ε . Then Moreno asked the values of $L\left(\frac{1}{2}, \varepsilon\right)$ and obtained the following result ([42]).

Let σ be an irreducible two-dimensional linear representation of $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $L(s, \sigma)$ be the Artin L -function associated with σ . We put

$$L(s, \sigma) = (2\pi)^{-1} \Gamma(s) \sum_{n=1}^{\infty} a(n) n^{-s}.$$

If σ is a lifting of the projective representation $\bar{\sigma}$ of G and $\text{Im}(\bar{\sigma}) = S_3$, then by the theorem of Hecke, the function

$$f(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}$$

is a normalized newform on $\Gamma_0(N)$ of weight 1 and character $\varepsilon (= \det(\sigma))$, where N denotes the conductor of σ .

On the other hand, let $E(s, z, \Gamma_0(N))$ be the non-holomorphic Eisenstein series for $\Gamma_0(N)$ corresponding to the cusp at ∞ . The Maclaurin expansion of $E(s, z, \Gamma_0(N))$ about $s=0$ is

$$E(s, z, \Gamma_0(N)) = f^*(z)s + O(s^2),$$

where $f^*(z)$ is a real analytic automorphic form for $\Gamma_0(N)$ with the eigen-

value $-1/4$ for the Laplacian $y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right)$. Then he obtained

$$A_k\left(\frac{1}{2}\right) L\left(\frac{1}{2}, \sigma\right) c\left(\frac{1}{2}\right) = \langle f^* \cdot f, f \rangle,$$

where, \langle , \rangle denotes the Petersson inner product, k the complex quadratic field corresponding to ε , $A_k(s)$ the Dedekind zeta function of k and

$$c\left(\frac{1}{2}\right) = \prod_{\substack{p|N \\ p:\text{prime}}} \frac{(1-\varepsilon(p)p^{-1/2})(1-a(p)p^{-1/2})}{(1+p^{-1/2})(1-a(p)^2p^{-1/2})}.$$

Now we ask the following non-abelian problem. We suppose that $\text{Im}(\partial) = S_4$. Then, by the theorem of Weil-Langlands-Tunnel, the function $f(z)$ corresponding to $L(s, \sigma)$ by the Mellin transformation is a normalized newform on $\Gamma_0(N)$ of weight 1 and character ε . We may naturally ask the following question:

Can one express the value of $L\left(\frac{1}{2}, \sigma\right)$ as a sum of values of a non-holomorphic modular form at special points?

Chapter 5. Dimension Formulas and $\text{tr}(T(\Gamma\alpha\Gamma))$ in the Case of Weight 1

Let Γ be a fuchsian group of the first kind. We shall denote by d_1 the dimension of the linear space of cusp forms of weight 1 on the group Γ . It is not effective to compute the number d_1 by means of the Riemann-Roch theorem. Hejhal said in his book ([18]), it is impossible to calculate d_1 using only the basic algebraic properties of Γ . Because of this reason, it is an interesting problem in its own right to determine the number d_1 by some other method.

On the other hand, the trace of the Hecke operator acting on the space of cusp forms on the group Γ has been calculated in most of the cases, but not yet for the case of weight 1. In this chapter we give some formula of d_1 and an explicit formula of the trace for the above remaining case, by using the Selberg trace formula ([1], [20], [22], [26], [27], [28], [53]).

§ 5.1. The Selberg eigenspace $\mathfrak{M}(k, \lambda)$

Let S denote the complex upper half-plane and we put $G = SL(2, \mathbf{R})$. Consider direct products

$$\tilde{S} = S \times T, \quad \tilde{G} = G \times T,$$

where T denotes the real torus. The operation of $(g, \alpha) \in \tilde{G}$ on \tilde{S} is represented as follows:

$$\tilde{S} \ni (z, \phi) \longrightarrow (g, \alpha)(z, \phi) = \left(\frac{az+b}{cz+d}, \phi + \arg(cz+d) - \alpha \right) \in \tilde{S},$$

where $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. The space \tilde{S} is a weakly symmetric Riemannian space with the \tilde{G} -invariant metric

$$ds^2 = \frac{dx^2 + dy^2}{y^2} + \left(d\theta - \frac{dx}{2y} \right)^2,$$

and with the isometry μ defined by $\mu(z, \phi) = (-\bar{z}, -\phi)$. The \tilde{G} -invariant measure $d(z, \phi)$ associated to the \tilde{G} -invariant metric is given by

$$d(z, \phi) = d(x, y, \phi) = \frac{dx \wedge dy \wedge d\phi}{y}.$$

The ring of \tilde{G} -invariant differential operators on \tilde{S} is generated by $\frac{\partial}{\partial \phi}$ and

$$\tilde{A} = y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right) + \frac{5}{4} \frac{\partial^2}{\partial \phi^2} + y \frac{\partial}{\partial \phi} \frac{\partial}{\partial x}.$$

Let Γ be a fuchsian group of the first kind not containing the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. By the correspondence

$$G \ni g \longleftrightarrow (g, 0) \in \tilde{G},$$

we identify the group G with a subgroup $G \times \{0\}$ of \tilde{G} , and so the subgroup Γ identify with a subgroup $\Gamma \times \{0\}$ of \tilde{G} . For an element $(g, \alpha) \in \tilde{G}$, we define a mapping $T_{(g, \alpha)}$ of $L^2(\tilde{S})$ into itself by $(T_{(g, \alpha)}f)(z, \phi) = f((g, \alpha)(z, \phi))$. For an element $g \in G$, we put $T_{(g, 0)} = T_g$. Then we have

$$(T_g f)(z, \phi) = f\left(\frac{az + b}{cz + d}, \phi + \arg(cz + d) \right),$$

where $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We denote by $\mathfrak{M}_\Gamma(k, \lambda) = \mathfrak{M}(k, \lambda)$ the set of all functions $f(z, \phi)$ satisfying the following conditions:

- (i) $f(z, \phi) \in L^2(\Gamma \backslash \tilde{S})$,
- (ii) $\tilde{A}f(z, \phi) = \lambda f(z, \phi)$, $(\partial/\partial \phi)f(z, \phi) = -ikf(z, \phi)$.

We call $\mathfrak{M}(k, \lambda)$ the Selberg eigenspace of Γ . We denote by $S_1(\Gamma)$ the space of cusp forms of weight 1 for Γ and put

$$d_1 = \dim S_1(\Gamma).$$

Then the following equality holds ([19], [26]):

Theorem 5.1. *The notation and the assumption being as above, we have*

$$\mathfrak{M}\left(1, -\frac{3}{2}\right) = \{e^{-i\phi}y^{1/2}F(z) \mid F(z) \in S_1(\Gamma)\},$$

and hence

$$(1) \quad d_1 = \dim \mathfrak{M}\left(1, -\frac{3}{2}\right).$$

Proof. For each $F(z) \in S_1(\Gamma)$ we denote $f(z, \phi)$ on \tilde{S} by

$$(2) \quad f(z, \phi) = e^{-i\phi}y^{1/2}F(z).$$

Then the function $f(z, \phi)$ satisfies the conditions:

- 1) $f(g(z, \phi)) = f(z, \phi)$ for all $g \in \Gamma$;
- 2) $(\partial/\partial\phi)f(z, \phi) = -if(z, \phi)$;
- 3) $\bar{\Delta}f(z, \phi) = -(3/2)f(z, \phi)$ by regularity of $F(z)$ on S ;
- 4) Since $y^{1/2}|F(z)|$ is bounded on S ,

$$\begin{aligned} \|f\| &= \frac{1}{2\pi} \int_{\Gamma \setminus \tilde{S}} |e^{-i\phi}y^{1/2}F(z)|^2 \frac{dx dy d\phi}{y^2} \\ &= \int_{\Gamma \setminus S} |y^{1/2}F(z)|^2 \frac{dx dy}{y^2} < \infty. \end{aligned}$$

Therefore, by 1)–4), the function $f(z, \phi)$ belongs to $\mathfrak{M}(1, -(3/2))$. We now prove conversely that any function in $\mathfrak{M}(1, -(3/2))$ must be of the form (2) with $F(z) \in S_1(\Gamma)$. Let $f(z, \phi)$ be a function in $\mathfrak{M}(1, -(3/2))$. Put

$$F(z) = e^{i\phi}y^{-1/2}f(z, \phi).$$

Then the Γ -invariance of $f(z, \phi)$ is equivalent to a transformation law for $F(z)$:

$$F(g(z)) = (cz + d)F(z)$$

for all $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Therefore, it is sufficient for the proof of the latter half of our theorem, to show that $F(z)$ is holomorphic with respect to the complex variable z on S , and $F(z)$ is holomorphic and vanishes at every cusp of Γ .

Let \mathfrak{g} be the Lie algebra of $SL_2(\mathbf{R}) (= G)$. Then we can take the basis α of \mathfrak{g} such that the Lie derivatives associated with the elements of α are given by the following invariant differential operators:

$$\begin{cases} X = y \cos 2\phi \frac{\partial}{\partial x} - y \sin 2\phi \frac{\partial}{\partial y} + \frac{1}{2} (\cos 2\phi - 1) \frac{\partial}{\partial \phi}, \\ Y = y \sin 2\phi \frac{\partial}{\partial x} + y \cos 2\phi \frac{\partial}{\partial y} + \frac{1}{2} \sin 2\phi \frac{\partial}{\partial \phi}, \\ \Phi = \frac{\partial}{\partial \phi}. \end{cases}$$

It is easily to see that

$$\tilde{A} = \left(X + \frac{1}{2} \Phi \right)^2 + Y^2 + \phi^2.$$

Now we put

$$A^- = 2 \left(X + \frac{1}{2} \Phi \right) + 2iY.$$

Then, the function $F(z)$ is holomorphic on S if and only if

$$(3) \quad A^- f(z, \phi) = 0.$$

To prove (3), first note that the operation of A^- depends only on the representations of the Lie algebra \mathfrak{g} . Let $L^2_d(\Gamma \backslash G)$ be the discrete part of the space $L^2(\Gamma \backslash G)$. Then $f \in L^2_d(\Gamma \backslash G)$. Let

$$L^2_d(\Gamma \backslash G) = \sum_i V_i$$

be the irreducible splitting of the space $L^2_d(\Gamma \backslash G)$ and put

$$f = \sum_i f_i \quad (f_i \in V_i).$$

Then, if $f_i \neq 0$, we have

$$\tilde{A} f_i = -\frac{3}{2} f_i, \quad \frac{\partial}{\partial \phi} f_i = -\sqrt{-1} f_i.$$

Therefore, each subspace V_i such that $f_i \neq 0$ is isomorphic to the space H_1 of the irreducible representation of the limit of discrete series. Hence it is sufficient for the proof of (3), to show that for any highest weight vector φ in H_1 ,

$$(4) \quad A^- \varphi = 0.$$

For example, by Lemma 5.6 in [32], the relation (4) is well known.

Next we shall see the condition for $F(z)$ at every cusp of Γ . Let s be

a cusp of Γ . We may assume that $s = \infty$ and the intersection of a fundamental domain for Γ and a neighborhood of ∞ is the following type

$$\{z = x + iy \mid 0 \leq x \leq 1, y \geq M\},$$

where M denotes a positive constant. Then, by the condition $f(z, \phi) \in L^2(\Gamma \setminus \tilde{S})$, we have

$$\int_M^\infty \left\{ \int_0^1 |F(z)|^2 dx \right\} \frac{dy}{y^2} < \infty.$$

Let

$$F(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}$$

be the Fourier expansion of F at ∞ . Then, we have

$$\begin{aligned} \int_0^1 |F(z)|^2 dx &= \int_0^1 \left(\sum_n a_n e^{2\pi i n z} \right) \left(\sum_m \bar{a}_m e^{-2\pi i m \bar{z}} \right) dx \\ &= \sum_{n,m} a_n \bar{a}_m \int_0^1 e^{2\pi i (n-m)x - 2\pi(n+m)y} dx \\ &= \sum_n |a_n|^2 e^{-4\pi n y}. \end{aligned}$$

Therefore

$$\int_M^\infty y \left(\sum_n |a_n|^2 e^{-4\pi n y} \right) \frac{dy}{y^2} = \sum_n |a_n|^2 \int_M^\infty y^{-1} e^{-4\pi n y} dy.$$

If $n \leq 0$, then

$$\int_M^\infty y^{-1} e^{-4\pi n y} dy = \infty.$$

So that $a_n = 0$ for all $n \leq 0$.

Q.E.D.

§ 5.2. The compact case

In this section we suppose that the group Γ' has a compact fundamental domain in the upper half-plane S . It is well known that every eigenspace $\mathfrak{M}(k, \lambda)$ defined in Section 5.1 is finite dimensional and orthogonal to each other, and also the eigenspaces span together the space $L^2(\Gamma' \setminus \tilde{S})$. We put $\lambda = (k, \lambda)$. For every invariant integral operator with a kernel function $k(z, \phi; z', \phi')$ on $\mathfrak{M}(k, \lambda)$, we have

$$\int_{\tilde{S}} k(z, \phi; z', \phi') f(z', \phi') d(z', \phi') = h(\lambda) f(z, \phi),$$

for $f \in \mathfrak{M}(k, \lambda)$. Note that $h(\lambda)$ does not depend on f so long as f is in $\mathfrak{M}(k, \lambda)$. We also know that there is a basis $\{f^{(n)}\}_{n=1}^\infty$ of the space $L^2(\Gamma \backslash \tilde{S})$ such that each $f^{(n)}$ satisfies the condition (ii) in Section 5.1. Then we put $\lambda^{(n)} = (k, \lambda)$ for such a spectra. We now obtain the following Selberg trace formula for $L^2(\Gamma \backslash \tilde{S})$:

$$(5) \quad \sum_{n=1}^\infty h(\lambda^{(n)}) = \sum_{M \in \Gamma} \int_{\tilde{D}} k(z, \phi; M(z, \phi)) d(z, \phi),$$

where \tilde{D} denotes a compact fundamental domain of Γ in \tilde{S} and $k(z, \phi; z', \phi')$ is a point-pair invariant kernel of (a)-(b) type in the sense of Selberg such that the series on the left-hand side of (5) is absolutely convergent ([46]). Denote by $\Gamma(M)$ the centralizer of M in Γ and put $\tilde{D}_M = \Gamma(M) \backslash \tilde{S}$. Then

$$(6) \quad \sum_{M \in \Gamma} \int_{\tilde{D}} k(z, \phi; M(z, \phi)) d(z, \phi) = \sum_t \int_{\tilde{D}_M} k(z, \phi; M_t(z, \phi)) d(z, \phi),$$

where the sum over $\{M_t\}$ is taken over the distinct conjugacy classes of Γ .

We consider an invariant integral operator on the Selberg eigenspace $\mathfrak{M}(k, \lambda)$ defined by

$$\omega_\delta(z, \phi; z', \phi') = \left| \frac{(yy')^{1/2}}{(z - \bar{z}')/2i} \right|^\delta \frac{(yy')^{1/2}}{(z - \bar{z}')/2i} e^{-i(\phi - \phi')}, \quad (\delta > 1).$$

It is easy to see that our kernel ω_δ is a point-pair invariant kernel of (a)-(b) type under the condition $\delta > 1$ and vanishes on $\mathfrak{M}(k, \lambda)$ for all $k \neq 1$. Since $\Gamma \backslash \tilde{G}$ is compact, the distribution of spectra (k, λ) is discrete and so we put

$$\begin{aligned} \mu_1 &= -\frac{3}{2}, & \mu_2, \mu_3, \dots, \\ d_\beta &= \dim \mathfrak{M}(1, \mu_\beta), & (\beta = 1, 2, \dots). \end{aligned}$$

Then the left-hand side of the trace formula (5) equals to $\sum_{\beta=1}^\infty d_\beta A_\beta$, where A_β denotes the eigenvalue of ω_δ in $\mathfrak{M}(1, \mu_\beta)$. For the eigenvalue A_β , using the special eigenfunction

$$f(z, \phi) = e^{-i\phi} y^{v_\beta}, \quad \mu_\beta = v_\beta(v_\beta - 1) - \frac{5}{4},$$

for a spectrum $(1, \mu_\beta)$ in $L^2(\tilde{S})$, we obtain

$$A_\beta = 2^{2+\delta} \pi \frac{\Gamma(1/2)\Gamma((1+\delta)/2)}{\Gamma(\delta)\Gamma(1+(\delta/2))} \Gamma\left(\frac{\delta-1}{2} + v_\beta\right) \Gamma\left(\frac{\delta+1}{2} - v_\beta\right).$$

If we put $v_\beta = 1/2 + ir_\beta$, then

$$(7) \quad A_\beta = 2^{2+\delta} \pi \frac{\Gamma(1/2)\Gamma((1+\delta)/2)}{\Gamma(\delta)\Gamma(1+(\delta/2))} \Gamma\left(\frac{\delta}{2} + ir_\beta\right) \Gamma\left(\frac{\delta}{2} - ir_\beta\right).$$

In general, it is known that the series $\sum_{\beta=1}^\infty d_\beta A_\beta$ is absolutely convergent for $\delta > 1$. By the Stirling formula, we see that the above series is also absolutely and uniformly convergent for all bounded δ except $\delta = \pm(2v_\beta - 1)$.

The components of trace appearing in the right-hand side of (6) are obtained already in [27] and we shall only state the results in the following.

1) Unit class: $M = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$J(I) = \int_{D_M} d(z, \phi) = \int_D d(z, \phi) < \infty.$$

2) The hyperbolic contribution $J(P)$ is expressed by the following

$$\begin{aligned} J(P) &= \sum_{\alpha=1}^\infty \sum_{k=1}^\infty J(P_\alpha^k) \\ &= \frac{2^{3+\delta} \pi^{3/2} \Gamma((\delta+1)/2)}{\Gamma((\delta+2)/2)} \sum_{\alpha=1}^\infty \sum_{k=1}^\infty \frac{(\text{sgn } \lambda_{0,\alpha})^k \log |\lambda_{0,\alpha}|}{|\lambda_{0,\alpha}^k - \lambda_{0,\alpha}^{-k}|} |\lambda_{0,\alpha}^k + \lambda_{0,\alpha}^{-k}|^{-\delta}, \end{aligned}$$

where $\{P_\alpha\}$ denotes a complete system of representatives of the primitive hyperbolic conjugacy classes in Γ and $\lambda_{0,\alpha}$ the eigenvalue ($|\lambda_{0,\alpha}| > 1$) of P_α .

3) There is no contribution from elliptic classes to d_1 .

Now we put

$$(8) \quad \zeta_1^*(\delta) = \sum_{\alpha=1}^\infty \sum_{k=1}^\infty \frac{(\text{sgn } \lambda_{0,\alpha})^k \log |\lambda_{0,\alpha}|}{|\lambda_{0,\alpha}^k - \lambda_{0,\alpha}^{-k}|} |\lambda_{0,\alpha}^k + \lambda_{0,\alpha}^{-k}|^{-\delta}.$$

Then, by the trace formula (5), the Dirichlet series $\zeta_1^*(s)$ extends to a meromorphic function on the whole δ -plane and has a simple pole at $\delta = 0$ whose residue will appear in (9) below. Finally, multiply the both sides of (5) by δ and tend δ to zero, then the limit is expressed, by the above 1), 2) and 3), as follows:

$$\dim \mathfrak{M}\left(1, -\frac{3}{2}\right) = \frac{1}{2} \text{Res}_{\delta=0} \zeta_1^*(\delta).$$

Theorem 5.2. *Let Γ be a fuchsian group of the first kind not containing the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and suppose that Γ has a compact fundamental*

domain in the upper half-plane. Let d_1 be the dimension for the linear space consisting of all holomorphic automorphic forms of weight 1 with respect to the group Γ . Then the number d_1 is given by the formula:

$$(9) \quad d_1 = \frac{1}{2} \operatorname{Res}_{s=0} \zeta_1^*(s),$$

where $\zeta_1^*(s)$ denotes the Selberg type zeta-function defined by (8).

Remark 1. Let Γ be a fuchsian group of the first kind and assume that Γ contains the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and χ be a unitary representation of Γ of degree 1 such that $\chi\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = -1$. Let $S_1(\Gamma, \chi)$ be the linear space of cusp forms of weight 1 on the group Γ with character χ , and denote by d_1 the dimension of the linear space $S_1(\Gamma, \chi)$. When the group Γ has a compact fundamental domain in the upper half plane S , we have the following dimension formula in the same way as in the case $\Gamma \neq \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$:

$$(10) \quad d_1 = \frac{1}{2} \sum_{\{M\}} \frac{\chi(M)}{\left[\Gamma(M) : \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]} \frac{\bar{\xi}}{1 - \bar{\xi}^2} + \frac{1}{2} \operatorname{Res}_{s=0} \zeta_2^*(s),$$

where the sum over $\{M\}$ is taken over the distinct elliptic conjugacy classes of $\Gamma / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, $\Gamma(M)$ denotes the centralizer of M in Γ , $\bar{\xi}$ is one of the eigenvalues of M , and $\zeta_2^*(s)$ denotes the Selberg type zeta-function defined by

$$(11) \quad \zeta_2^*(s) = \sum_{\alpha=1}^{\infty} \sum_{k=1}^{\infty} \frac{\chi(P_\alpha)^k \log \lambda_{0,\alpha}}{\lambda_{0,\alpha}^k - \lambda_{0,\alpha}^{-k}} |\lambda_{0,\alpha}^k + \lambda_{0,\alpha}^{-k}|^{-s}.$$

Here $\lambda_{0,\alpha}$ denotes the eigenvalue ($\lambda_{0,\alpha} > 1$) of representative P_α of the primitive hyperbolic conjugacy classes $\{P_\alpha\}$ in $\Gamma / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

§ 5.3. The Arf invariant and $d_1 \pmod 2$

The purpose of this section is to prove that $d_1 \pmod 2$ is just the Arf invariant of some quadratic form over a field of characteristic 2.

1. The Arf invariant of quadratic forms mod 2

Let V be a vector space of dimension m over a field F of characteristic 2, Q a quadratic form on V . Then the associated polar form

$$B(x, y) = Q(x + y) + Q(x) + Q(y)$$

is an alternating bilinear form. Let x_1, \dots, x_m be a symplectic basis of V with respect to B . It is known that the quadratic form $Q(x)$ is equivalent to

$$\sum_{i=1}^n \{Q(x_i)a_i^2 + a_i a_{n+i} + Q(x_{n+i})a_{n+i}^2\} + \sum_{i=2n+1}^m Q(x_i)a_i^2$$

for $x = \sum_{i=1}^m a_i x_i \in V$. By the radical of V we mean the subspace

$$\text{rad } V = \{x \in V \mid B(x, V) = 0\}.$$

We shall say that V is a completely regular space if $\text{rad } V = \{0\}$. We now define the Arf invariant of $Q(x)$ ([2]). Take a 2-dimensional completely regular space U over F and a basis x_1, x_2 for U . Thus

$$U = Fx_1 + Fx_2.$$

Define a multiplication on these basis elements by the following relations:

$$\begin{aligned} x_1^2 &= x_1 \otimes x_1 = Q(x_1), \\ x_2^2 &= x_2 \otimes x_2 = Q(x_2), \\ x_1 x_2 + x_2 x_1 &= B(x_1, x_2) \quad (= 1). \end{aligned}$$

Here we put

$$\omega = x_1 x_2, \quad \theta = x_1.$$

Then we obtain the quaternion algebra $C(U)$ with respect to U :

$$C(U) = F \cdot 1 + F \cdot \theta + F \cdot \omega + F \cdot \theta \omega.$$

It is clear that

$$\theta^2 = a, \quad \omega^2 = \omega + ac, \quad \theta \omega + \omega \theta = \theta, \quad \theta \omega \theta^{-1} = \omega + 1,$$

where $a = Q(x_1) (\neq 0)$ and $c = Q(x_2)$. Therefore, in the separable quadratic field $F(\omega)$ over F , we have the norm

$$N(\alpha + \beta \omega) = \alpha^2 + \alpha \beta + ac \beta^2$$

for every α, β in F . Let F^+ be the additive group of F , and ϕ a homomorphism

$$\phi: F^+ \ni e \longrightarrow e^2 + e \in F^+,$$

and put

$$\Delta(U) = Q(x_1)Q(x_2) \quad (= ac = N(\omega)).$$

Then we call the class $\Delta(U) \bmod \phi(F^+)$ the Arf invariant of U . In general, let

$$V = \bigoplus_{i=1}^n U_i \perp \text{rad } V$$

be the orthogonal splitting of the space V into 2-dimensional completely regular subspaces U_1, \dots, U_n . Put

$$\Delta(V) = \sum_{i=1}^n \Delta(U_i).$$

Then it is obvious that for a symplectic basis $\{x_1, \dots, x_m\}$ of V ,

$$\Delta(V) = \sum_{i=1}^n Q(x_i)Q(x_{n+i}).$$

Now the class $\Delta(V) \bmod \phi(F^+)$ does not depend on the symplectic basis chosen and is called the Arf invariant of Q or the pseudo-discriminant of Q , and is denoted by $\bar{\Delta}(Q)$. In this situation, we have

Theorem 5.3.¹⁾ *Let F be a perfect field, and let V be a completely regular space, so that $m=2n$. Then the following assertions hold:*

(1) *Two nondegenerate quadratic forms $Q_1(x), Q_2(x)$ on V are equivalent if and only if $\bar{\Delta}(Q_1) = \bar{\Delta}(Q_2)$.*

(2) *$Q(x) = \sum_{i=1}^n x_i x_{n+i} + \nu(x_n^2 + x_{2n}^2)$; and therefore, $\bar{\Delta}(Q) = \nu^2$.*

2. The Atiyah invariant on spin structures

Let M be a smooth closed oriented surface of genus g and F_2 the 2-element field. We write H_1 and H^1 for $H_1(M, F_2)$ and $H^1(M, F_2)$ respectively. Let UM be the principal tangential S^1 -bundle of M . \tilde{H}_1 and \tilde{H}^1 mean $H_1(UM, F_2)$ and $H^1(UM, F_2)$, respectively. Then the sequences

$$\begin{aligned} 0 \longrightarrow F_2 \longrightarrow \tilde{H}_1 \longrightarrow H_1 \longrightarrow 0, \\ 0 \longrightarrow H^1 \longrightarrow \tilde{H}^1 \xrightarrow{\delta} F_2 \longrightarrow 0 \end{aligned}$$

are exact. A spin structure of M is a cohomology class $\xi \in \tilde{H}^1$ whose restriction to each fiber is the generator of F_2 : $\delta(\xi) = 1$. We denote by Φ the set of spin structures of M . Let a be any homology class in H_1 and

¹⁾ For the proof, see Dye ([9]).

let \tilde{a} be the canonical lifting of a to \tilde{H}_1 (see [34, p. 368]). If a, b are in H_1 , then we have

$$\widetilde{(a+b)} = \tilde{a} + \tilde{b} + (a \cdot b)z,$$

where z denotes the generator of F_2 as the fiber class and $a \cdot b$ denotes the intersection number of a, b . We define a quadratic form on the symplectic space H_1 over F_2 as a function $\omega: H_1 \rightarrow F_2$ such that

$$\omega(a+b) = \omega(a) + \omega(b) + a \cdot b.$$

Now for $\xi \in \Phi$, we put

$$\omega_\xi(a) = \langle \xi, \tilde{a} \rangle, \quad a \in H_1,$$

where $\langle \cdot, \cdot \rangle$ denotes the dual pairing of \tilde{H}^1 and \tilde{H}_1 . Then the function ω_ξ is a quadratic form on H_1 in the above sense. Indeed, since $\langle \xi, z \rangle = 1$, we have

$$\begin{aligned} \omega_\xi(a+b) &= \langle \xi, \widetilde{(a+b)} \rangle \\ &= \langle \xi, \tilde{a} + \tilde{b} + (a \cdot b)z \rangle \\ &= \langle \xi, \tilde{a} \rangle + \langle \xi, \tilde{b} \rangle + (a \cdot b)\langle \xi, z \rangle \\ &= \omega_\xi(a) + \omega_\xi(b) + a \cdot b. \end{aligned}$$

Let Ω be the set of quadratic forms on H_1 . Then, D. Johnson proved in [34]:

Lemma. *The mapping $\xi \rightarrow \omega_\xi$ gives a bijection from Φ to Ω .*

Next we give the Arf invariant of ω_ξ . For the canonical lifting \tilde{a} of a in H_1 , the mapping on \tilde{H}^1

$$\tilde{a}: x \longrightarrow \langle x, \tilde{a} \rangle$$

is linear and we denote by \bar{a} the restriction of \tilde{a} to Φ . Let a_i, b_i ($i=1, \dots, g$) be a symplectic basis of H_1 , i.e.,

$$a_i \cdot a_j = b_i \cdot b_j = 0, \quad a_i \cdot b_j = \delta_{ij},$$

where δ_{ij} denotes the Kronecker symbol. We put

$$\alpha = \sum_{i=1}^g \bar{a}_i \bar{b}_i.$$

Then

$$\begin{aligned} \alpha(\xi) &= \sum_{i=1}^g \bar{a}_i(\xi) \bar{b}_i(\xi) = \sum_{i=1}^g \langle \xi, \bar{a}_i \rangle \langle \xi, \bar{b}_i \rangle \\ &= \sum_{i=1}^g \omega_\xi(a_i) \omega_\xi(b_i). \end{aligned}$$

Therefore, $\alpha(\xi) \pmod 2$ is the Arf invariant of ω_ξ .

From now on we consider the surface M as a closed Riemann surface of genus g and introduce the Atiyah invariant on M ([4], [43]). Let K be a canonical line bundle on M , and denote by $S(M)$ the set of holomorphic line bundles L on M such that $L \otimes L \cong K$. The elements of $S(M)$ are called theta-characteristic of M . Let D be a divisor on M and let $\mathcal{L}(D)$ denote the space of meromorphic functions f on M such that $D + (f) \geq 0$. We define the complete linear system of D by

$$|D| = \{D + (f) \mid f \in \mathcal{L}(D)\}.$$

Then, we have

$$\dim |D| = \dim \mathcal{L}(D) - 1.$$

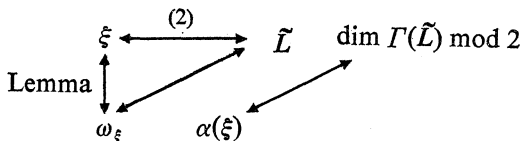
Let L be the associated line bundle to an effective divisor D and let $\Gamma(L)$ denote the space of holomorphic section of L . Then, since $|D|$ is the projective space associated to $\Gamma(L)$, we have

$$\dim |D| = \dim \Gamma(L) - 1.$$

Theorem 5.4. *The notation being as above, we have the following assertions.*

- (1) *For each theta-characteristic L of M , $\dim \Gamma(L) \pmod 2$ is stable under deformations of M and L .*
- (2) *The set Φ for M corresponds bijectively to the set of isomorphism classes in $S(M)$.*
- (3) $\#\{L \in S(M) \mid \dim \Gamma(L) \equiv 0 \pmod 2\} = 2^{g-1}(2^g + 1)$.

The first assertion (1) in Theorem 5.4 is due to Riemann. For the proofs of Theorem 5.4, refer to Atiyah ([4]) and Mumford ([43]). By (1) in Theorem 5.4, $\dim \Gamma(L) \pmod 2$ is independent of the choice of the complex structure on M . Now, by combining Lemma and (2) in Theorem 5.4, we have the following diagram:



Therefore, intermediating the spin structures $\{\xi\}$ of M , there is a bijection between the isomorphic classes $\{\tilde{L}\}$ of theta-characteristic and the quadratic forms $\{\omega_\xi\}$ on H_1 . It is obvious that the Arf invariant $\alpha(\xi) \pmod 2$ has $2^{g-1}(2^g+1)$ zeros. Therefore the Arf invariant $\alpha(\xi) \pmod 2$ is equal to the Atiyah invariant $\dim \Gamma(\tilde{L}) \pmod 2$.

3. The Arf invariant and $d_1 \pmod 2$

Let M be a closed Riemann surface of genus g and K a canonical divisor on M . Then, an effective divisor D on M such that $\dim \mathcal{L}(K-D) \neq 0$ is called special. For every special divisor D , we have $0 < \deg D \leq 2g-2$. Therefore, the Rimenn-Roch theorem says little for special divisors.

Now, let Γ be a fuchsian group of the first kind not containing the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and suppose that the fundamental domain $\Gamma \backslash S$ of Γ is a closed Riemann surface of genus g , where S denotes the upper half-plane. We denote by P_1, \dots, P_l the point of $\Gamma \backslash S$ corresponding to all the elliptic points of Γ , of order e_1, \dots, e_l , respectively. Let $A_1(\Gamma)$ denote the space of meromorphic automorphic forms of weight 1 with respect to Γ and $S_1(\Gamma)$ the space of holomorphic automorphic forms of weight 1 for Γ . We put

$$d_1 = \dim S_1(\Gamma).$$

For a non-zero element f_0 of $A_1(\Gamma)$, we have

$$\operatorname{div}(f_0) = \frac{1}{2} \operatorname{div}(\omega_{f_0}) + \frac{1}{2} \sum_{i=1}^l \left(1 - \frac{1}{e_i}\right) P_i \quad (\omega_{f_0} = f_0^2/dx),$$

and

$$S_1(\Gamma) \cong \mathcal{L}([\operatorname{div}(f_0)]),$$

where $[D] = \sum_i [n_i]P_i$ for $D = \sum_i n_i P_i$. Put $D_0 = [\operatorname{div}(f_0)]$. Then

$$D_0 = \frac{1}{2} \operatorname{div}(\omega_{f_0}) + \sum_{i=1}^l \left[\frac{1}{2} \left(1 - \frac{1}{e_i}\right) \right] P_i.$$

Therefore we have $\deg D_0 = g-1$. Hence, under $d_1 \neq 0$, the divisor D_0 is special and

$$\dim \mathcal{L}(D_0) = \dim \mathcal{L}(K-D_0)$$

by the Riemann-Roch theorem. Let L_0 be the associated line bundle of

D_0 . Then it is obvious that the line bundle L_0 is a theta-characteristic on M . Therefore, we have

$$\begin{aligned} d_1 \bmod 2 &= \dim \mathcal{L}(D_0) \bmod 2 \\ &= \dim \Gamma(L_0) \bmod 2 \\ &= \alpha(\xi_0) \bmod 2 \end{aligned}$$

for the spin structure ξ_0 corresponding to L_0 . We have thus the following

Theorem 5.5. *The notation and the assumption being as above, we have the relation*

$$d_1 \bmod 2 = \alpha(\xi_0) \bmod 2.$$

Remark 2. We know from Theorem 5.5 that $d_1 \bmod 2$ is the number expressed the topological side of d_1 .

Remark 3. By Clifford's theorem for special divisors, we have

$$0 \leq \dim \mathcal{L}(D_0) \leq \frac{g+1}{2}.$$

But it is impossible to determine $\dim \mathcal{L}(D_0)$ using only the genus g of $\Gamma \backslash S$. For $g=1$, using the above result and Theorem 5.4 we have $d_1=0$.

Now, we may naturally ask the following question:

Can one determine the Arf invariant $\alpha(\xi_0)$ by the basic topological properties of Γ ?

§ 5.4. The finite case

Let Γ be a fuchsian group of the first kind and assume that Γ contains the element $-I \left(I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$ and has a non-compact fundamental domain \tilde{D} in the space \tilde{S} . Let χ be a unitary representation of Γ of degree 1 such that $\chi(-I) = -1$. We denote by $S_1(\Gamma, \chi)$ the linear space of cusp forms of weight 1 on the group Γ with the character χ and d_1 the dimension of the space $S_1(\Gamma, \chi)$. In this section we shall give a similar formula of the number d_1 when the group Γ is of finite type reduced at infinity and $\chi^2 \neq 1$.

Since Γ is of finite type reduced at ∞ , ∞ is a cusp of Γ and the stabilizer Γ_∞ of ∞ in Γ is equal to $\pm \Gamma_0$ with $\Gamma_0 = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbf{Z} \right\}$. The Eisenstein series $E_\chi(z, \phi; s)$ attached to ∞ and χ is then defined by

$$E_\chi(z, \phi; s) = \sum_{\substack{M \in \Gamma_\infty \setminus \Gamma \\ M = \begin{pmatrix} * & * \\ c & d \end{pmatrix}}} \frac{\bar{\chi}(M)y^s}{|cz+d|^{2s}} e^{-i(\phi + \arg(cz+d))},$$

where $s = \sigma + ir$ with $\sigma > 1$. The constant term in the Fourier expansion of $E_\chi(z, \phi; s)$ at ∞ is given by

$$a_0(y, \phi; s) = e^{-\sqrt{-1}\phi}(y^s + \psi_\chi(s)y^{1-s}),$$

$$\psi_\chi(s) = -\sqrt{-1}\sqrt{\pi} \frac{\Gamma(s)}{\Gamma\left(s + \frac{1}{2}\right)} \sum_{\substack{c > 0 \\ d \pmod c \\ \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma}} \frac{\bar{\chi}(c, d)}{|c|^{2s}}.$$

In the following we only consider the case $\chi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = 1$. As shown in [26], the parabolic component $J(\infty)$ in the trace formula is given by

$$J(\infty) = \lim_{Y \rightarrow \infty} \left\{ \int_0^Y \int_0^1 \int_0^\pi 2 \sum_{\substack{M \in \Gamma \\ M \neq I}} \omega_\delta(z, \phi; M(z, \phi)) d(z, \phi) - \int_{D_Y} \tilde{H}_\delta(z, \phi; z, \phi) d(z, \phi) \right\}$$

$$= \frac{1}{4\pi} \int_{-\infty}^\infty h(r) \frac{\psi'_\chi\left(\frac{1}{2} + ir\right)}{\psi_\chi\left(\frac{1}{2} + ir\right)} dr - \frac{1}{4} h(0) \psi_\chi\left(\frac{1}{2}\right) + \varepsilon(\delta)$$

as $\lim_{\delta \rightarrow 0} \delta \varepsilon(\delta) = 0$. When we combine this with the formula (10), we are led to the following theorem which is our main purpose in this section.

Theorem 5.6. *Let Γ be a fuchsian group of the first kind containing the element $-I$ and suppose that Γ is reduced at infinity. Let χ be a one-dimensional unitary representation of Γ such that $\chi(-I) = -1$, $\chi^2 \neq 1$ and $\chi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = 1$. We denote by d_1 the dimension for the linear space consisting of cusp forms of weight 1 with respect to Γ with χ . Then the dimension d_1 is given by*

$$(12) \quad d_1 = \frac{1}{2} \sum_{\{M\}} \frac{\chi(M)}{[\Gamma(M) : \pm I]} \frac{\bar{\xi}}{1 - \bar{\xi}^2} + \frac{1}{2} \text{Res}_{s=0} \zeta_2^*(s) - \frac{1}{4} \psi_\chi\left(\frac{1}{2}\right),$$

where the sum over $\{M\}$ is taken over the distinct elliptic conjugacy classes of $\Gamma / \{\pm I\}$, $\Gamma(M)$ denotes the centralizer of M in Γ , $\bar{\xi}$ is one of the eigenvalues of M , and $\zeta_2^*(s)$ denotes the Selberg type zeta-function defined by (11) in Section 5.2.

Remark 4. For a general discontinuous group Γ of finite type containing the element $-I$, we obtain the contribution from parabolic classes to d_1 in the same way as in the case of reduced at ∞ .

Remark 5. Let Γ be a general discontinuous group of finite type not containing the element $-I$. Let d_1 be the dimension for the space consisting of all cusp forms of weight 1 with respect to Γ . Then we have the following dimension formula in a similar way as in the above case:

$$(13) \quad d_1 = \frac{1}{2} \operatorname{Res}_{s=0} \zeta_1^*(s),$$

where $\zeta_1^*(s)$ denotes the Selberg type zeta-function appeared in (8) of Section 5.2.

We may call the formulas (12) and (13) a kind of Riemann-Roch type theorem for automorphic forms of weight 1 respectively.

Remark 6. Let p be a prime number such that $p \equiv 3 \pmod{4}$, $p \neq 3$ and let $\Phi_0(p)$ be the group generated by the group $\Gamma_0(p)$ and the element $K = \begin{pmatrix} 0 & -\sqrt{p}^{-1} \\ \sqrt{p} & 0 \end{pmatrix}$. Let ε be the Legendre symbol on $\Gamma_0(p)$: $\varepsilon(L) = \left(\frac{d}{p}\right)$ for $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$. Since $\varepsilon(K^2) = \varepsilon(-I) = -1$, we can define the odd character ε^\pm on the Fricke group $\Phi_0(p)$ such that $\varepsilon^\pm(K) = \pm i$. Then we have

$$S_1(\Gamma_0(p), \varepsilon) = S_1(\Phi_0(p), \varepsilon^+) \oplus S_1(\Phi_0(p), \varepsilon^-).$$

We put

$$\mu_1^\pm = \dim S_1(\Phi_0(p), \varepsilon^\pm).$$

Then

$$d_1 = \dim S_1(\Gamma_0(p), \varepsilon) = \mu_1^+ + \mu_1^-.$$

If $\sigma^*(p)$ is the parabolic class number of $\Phi_0(p)/\{\pm I\}$, then $\sigma^*(p) = 1$. As shown in [27], the contribution from elliptic classes to μ_1^\pm is given by

$$\frac{1}{2} \sum_{\{M\}} \frac{1}{[\Gamma(M): \pm I]} \frac{\zeta}{1 - \zeta^2} \varepsilon^\pm(M) = \mp \frac{1}{4} h,$$

where h denotes the class number of $Q(\sqrt{p})$. We also have $\varphi_{\varepsilon^\pm}(1/2) = \mp 1$. Let $\{P_\alpha\}$ be a complete system of representatives of the primitive hyperbolic conjugacy classes in $\Gamma_0(p)/\{\pm I\}$ and let $\lambda_{0,\alpha}$ be the eigenvalue ($\lambda_{0,\alpha} > 1$) of representative P_α . We put

$$\mathcal{E}^*(\delta) = \sum_{\alpha=1} \sum_{k=1} \frac{\varepsilon(P_\alpha)^k \log \lambda_{0,\alpha}}{\lambda_{0,\alpha}^k - \lambda_{0,\alpha}^{-k}} |\lambda_{0,\alpha}^k + \lambda_{0,\alpha}^{-k}|^{-\delta}.$$

Then we have the following formula for d_1 by Theorem 5.6:

$$(14) \quad d_1 = \mu_1^+ + \mu_1^- = \frac{1}{2} \operatorname{Res}_{\delta=0} \mathcal{Z}^*(\delta)$$

Combining the above (14) with Serre's result (: (*) in Section 4.1), we have the following remarkable equality

$$\operatorname{Res}_{\delta=0} \mathcal{Z}^*(\delta) = (h-1) + 4(s+2a).$$

§ 5.5. The trace of Hecke operators on the space of cusp forms of weight 1

Let Γ be a fuchsian group of the first kind and assume that Γ does not contain the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ($= -I$). Let α be an element in $SL(2, \mathbf{R})$ ($= G$) such that $\alpha\Gamma\alpha^{-1}$ is commensurable with Γ and denote by Γ' the subgroup of G generated by Γ and α . Let χ be a unitary representation of Γ' of degree ν such that the kernel Γ_χ of χ in Γ is of finite index in Γ . We denote by $L^2(\Gamma \backslash \tilde{S}, \chi)$ the following set of functions f taking values in the representation space of χ :

$$\{f \in L^2(\Gamma \backslash \tilde{S}) \mid f(\gamma(z, \phi)) = \chi(\gamma)f(z, \phi) \text{ for all } \gamma \in \Gamma\},$$

and by $\mathfrak{M}_\chi(k, \lambda)$ the set of functions f satisfying the following conditions:

- (i) $f(z, \phi) \in L^2(\Gamma \backslash \tilde{S}, \chi)$,
- (ii) $\tilde{\Delta}f(z, \phi) = \lambda f(z, \phi)$, $(\partial/\partial\phi)f(z, \phi) = -\sqrt{-1}kf(z, \phi)$.

Let $S_k(\Gamma, \chi)$ be the linear space of cusp forms of odd weight k on the group Γ with χ taking values in the representation space of χ and put

$$d_k = \dim S_k(\Gamma, \chi).$$

Then

$$(15) \quad \mathfrak{M}_\chi\left(k, -k\left(k + \frac{1}{2}\right)\right) = \{e^{-\sqrt{-1}k\phi} y^{k/2} F(z) \mid F(z) \in S_k(\Gamma, \chi)\},$$

and in particular

$$d_1 = \dim \mathfrak{M}_\chi\left(1, -\frac{3}{2}\right).$$

Now we define the Hecke operator $T(\Gamma\alpha\Gamma)$ in $S_k(\Gamma, \chi)$. Let $\Gamma\alpha\Gamma = \cup_i M_i\Gamma$ be a disjoint sum. For $f(z, \phi) \in \mathfrak{M}_\chi(k, -k(k+(1/2)))$, we set

$$T(\Gamma\alpha\Gamma) \cdot f(z, \phi) = \sum_i \chi(M_i) f\left(\frac{a_i z_i + b_i}{c_i z_i + d_i}, \phi + \arg(c_i z + d_i)\right),$$

where $M_i^{-1} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$. Then by the relation (15), it equals to

$$e^{-\sqrt{-1}k\phi} y^{k/2} \sum_i \chi(M_i) F\left(\frac{a_i z + b_i}{c_i z + d_i}\right) (c_i z + d_i)^{-k}.$$

Therefore it induces the Hecke operator $T(\Gamma\alpha\Gamma)$ acting on $S_k(\Gamma, \chi)$:

$$T(\Gamma\alpha\Gamma) \cdot F(z) = \sum_i \chi(M_i) F\left(\frac{a_i z + b_i}{c_i z + d_i}\right) (c_i z + d_i)^{-k}.$$

In the following we shall only state the result for its trace on $S_1(\Gamma, \chi)$ (c.f. [1]). Let κ_i ($1 \leq i \leq h$) be a complete system of Γ -inequivalent cusps of Γ and let Γ_i be the stabilizer in Γ of κ_i . We put $\Gamma_{i,0} = \Gamma_i \cap \Gamma_\chi$ and denote by $\Gamma'_{1,0}$ a subgroup of index 2 in $\Gamma_{i,0}$. We take an element $\sigma_i \in G$ such that $\sigma_i \infty = \kappa_i$ and such that $\sigma_i^{-1} \Gamma_i \sigma_i$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ over \mathbb{Z} according to κ_i regular or irregular. Let $E_i(z, \phi; s)$ be the Eisenstein series attached to the cusp κ_i and χ , and denote by $\varphi_{ii}^*(s)$ the constant term of the Fourier expansion at κ_i of $\sum_j \chi(M_j) E_j(M_j^{-1}(z, \phi); s)$. Then we have the following

Theorem 5.7. *Suppose that Γ does not contain the element $-I$.¹⁾ Then the following trace formula holds:*

$$\begin{aligned} \text{tr}(T(\Gamma\alpha\Gamma)) &= \frac{1}{2} \sum_{[M]_{\Gamma'}: \text{elliptic}} \frac{\text{tr } \chi(M)}{[\Gamma(M): I]} \frac{1}{\zeta - \bar{\zeta}} + \frac{1}{2} \text{Res}_{s=0} \zeta^*(s) \\ &\quad - \sum_{\kappa_i: \text{regular}} \left\{ \frac{\sqrt{-1}}{4r_i} \sum_{\{M\} \in \mathcal{B}_i/\Gamma_{i,0}} s(M) \text{tr } \chi(M) \cot\left(\frac{\pi\mu(M)}{r_i}\right) \right\} \\ &\quad - \sum_{\kappa_i: \text{irregular}} \left\{ \frac{\sqrt{-1}}{8r_i} \sum_{\{M\} \in \mathcal{B}_i/\Gamma'_{i,0}} s(M) \text{tr } \chi(M) \cot\left(\frac{\pi\mu(M)}{r'_i}\right) \right\} \\ &\quad - \frac{1}{4} \sum_i \text{tr } \varphi_{ii}^*\left(\frac{1}{2}\right). \end{aligned}$$

The notation used here is defined as follows:

$[M]_{\Gamma}$: the elliptic conjugacy class in $\Gamma\alpha\Gamma$,

$\Gamma(M)$: the centralizer of M in Γ ,

$\zeta, \bar{\zeta}$: the eigenvalues of M ,

$r_i = [\Gamma_i: \Gamma_{i,0}]$,

¹⁾ For the case $\Gamma \ni -I$, refer to [1].

$$r'_i = \begin{cases} r_i, & \text{if } r_i: \text{ even,} \\ 2r_i, & \text{if } r_i: \text{ odd,} \end{cases}$$

$$B_i = \{M \in \Gamma\alpha\Gamma \mid M\kappa_i = \kappa_i, \text{ parabolic or } I\},$$

$$s(M) \text{ and } \mu(M) \text{ are defined by } \sigma_i^{-1}M\sigma_i = s(M) \begin{pmatrix} 1 & \mu(M) \\ 0 & 1 \end{pmatrix}, s(M) = \pm 1;$$

$$\zeta^*(s) = \sum_{\{M\}_\Gamma: \text{hyperbolic}} \frac{\text{sgn } \lambda \cdot \text{tr } \chi(M) \log |\lambda_0|}{|\lambda - \lambda^{-1}| |\lambda + \lambda^{-1}|^s},$$

where the sum over $\{M\}_\Gamma$ is taken over the distinct hyperbolic conjugacy classes of $\Gamma\alpha\Gamma$, λ is one of the eigenvalues of M and λ_0 is the eigenvalue (>1) of generator of $\Gamma(M)$.

Acknowledgements. I would like to express deep appreciation to Professor T. Kubota who gave me an opportunity to write a paper for this volume. I also acknowledge to Professors M. Eichler and H. Shimizu for their hearty encouragements, and to Professor Y. Mimura for several stimulating conversations in Kobe.

References

- [1] S. Akiyama, T. Hiramatsu and Y. Tanigawa, On traces of Hecke operators on the space of cusp forms of weight 1, preprint.
- [2] C. Arf, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, Teil I, *J. Reine Angew. Math.*, **183** (1941), 148–167.
- [3] J. Arthur, Automorphic representations and number theory, in Proc. 1980 Seminar on Harmonic Analysis, CMS-AMS, 1981, 3–51.
- [4] M. F. Atiyah, Riemann surfaces and spin structures, *Ann. scient. Éc. Norm. Sup.*, 4^e séries, t. 4 (1971), 47–62.
- [5] J. P. Buhler, Icosahedral Galois representations, *Lecture Notes in Math.*, **654**, Springer-Verlag, 1978.
- [6] T. Chinburg, Stark's conjecture for L -functions with first-order zeros at $s=0$. *Adv. in Math.*, **48** (1983), 82–113.
- [7] S. Chowla and M. Cowles, On the coefficient c_n in the expansion $x \prod_{n=1}^{\infty} (1-x^n)^2 \times (1-x^{11n})^2 = \sum_{n=0}^{\infty} c_n x^n$, *J. Reine Angew. Math.*, **292** (1977), 209–220.
- [8] P. Deligne et J.-P. Serre, Formes modulaires de poids 1, *Ann. scient. Éc. Norm. Sup.*, 4^e séries, t. 7 (1974), 507–530.
- [9] R. H. Dye, On the Arf invariant, *J. Algebra*, **53** (1978), 36–39.
- [10] M. Eichler, Der Hilbertsche Klassenkörper eines imaginärquadratischen Zahlkörper, *Math. Z.*, **64** (1956), 229–242.
- [11] R. Fricke, *Lehrbuch der Algebra III*, Braunschweig, 1928.
- [12] S. Gelbert, Automorphic forms and Artin's conjecture, *Lecture Notes in Math.*, **627**, Springer-Verlag, 1978, 242–276.
- [13] H. Hasse, Neue Begründung der komplexen Multiplikation, I, *J. Reine Angew. Math.*, **157** (1927), 115–139; II, *Ibid.*, **165** (1931), 64–88.
- [14] —, Über der Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47 , *Acta Arith.*, **9** (1964), 419–434.
- [15] — and J. Liang, Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47 (Fortsetzung), *Acta Arith.*, **16** (1969), 89–97.

- [16] E. Hecke, Über einen neuen Zusammenhang zwischen elliptischen Modulfunktionen und indefiniten quadratischen Formen, *Math. Werke*, no. **22** (1925), 418–427.
- [17] —, Theorie der elliptischen Modulfunktionen, *Ibid.*, no. **23** (1926), 428–460.
- [18] D. A. Hejhal, The Selberg trace formula for $PSL(2, \mathbf{R})$ I, *Lecture Notes in Math.*, **548**, Springer-Verlag, 1976.
- [19] T. Hiramatsu, Eichler classes attached to automorphic forms of dimension -1 , *Osaka J. Math.*, **3** (1966), 39–48.
- [20] — and Y. Mimura, On automorphic forms of weight one II, The Arf invariant and $d_0 \pmod 2$, *Math. Seminar Notes, Kobe Univ.*, **9** (1981), 259–267.
- [21] —, Higher reciprocity law and modular forms of weight one, *Comment. Math. Univ. St. Pauli*, **31** (1982), 75–85.
- [22] —, On some dimension formula for automorphic forms of weight one I, *Nagoya Math. J.*, **85** (1982), 213–221.
- [23] — and N. Ishii, Quartic residuacity and cusp forms of weight one, *Comment. Math. Univ. St. Pauli*, **34** (1985), 91–103.
- [24] — and Y. Mimura, The modular equation and modular forms of weight one, *Nagoya Math. J.*, **100** (1985), 145–162.
- [25] —, N. Ishii and Y. Mimura, On indefinite modular forms of weight one, *J. Math. Soc. Japan*, **38** (1986), 67–83.
- [26] —, On some dimension formula for automorphic forms of weight one II, *Nagoya Math. J.*, **105** (1987), 169–186.
- [27] —, A formula for the dimension of spaces of cusp forms of weight 1. to appear in *Adv. Studies in Pure Math.*
- [28] — and S. Akiyama, On some dimension formula for automorphic forms of weight one III, to appear in *Nagoya Math. J.*
- [29] H. Ishii, On the coincidence of L-functions, *Japan. J. Math.*, **12** (1986), 37–44.
- [30] N. Ishii, Cusp forms of weight one, quartic reciprocity and elliptic curves, *Nagoya Math. J.*, **98** (1985), 117–137.
- [31] H. Ishikawa, On the trace formula for Hecke operators, *J. Fac. Sci. Univ. Tokyo, Sec. I* **20** (1973), 217–238.
- [32] H. Jacquet and R. P. Langlands, Automorphic forms on $GL(2)$, *Lecture Notes in Math.*, **114**, Springer-Verlag, 1970.
- [33] M. Jimbo and T. Miwa, Irreducible decomposition of fundamental modules for $A_i^{(1)}$ and $C_i^{(1)}$ and Hecke modular forms, *Publ. Res. Inst. Math. Sci.*, **434**, Kyoto Univ., 1983.
- [34] D. Johnson, Spin structures and quadratic form on surfaces, *J. London Math. Soc.*, **22** (1980), 365–373.
- [35] V. G. Kac and D. H. Peterson, Infinite-dimensional Lie algebras, theta functions and modular forms, *Adv. in Math.*, **53** (1984), 125–254.
- [36] F. H. Koch, Arithmetische Theorie der Normkörper von 2-Potenzgrad mit Diedergruppe, *J. Number Theory*, **3** (1971), 412–443.
- [37] M. Koike, Congruences between cusp forms and linear representations to the Galois group, *Nagoya Math. J.*, **64** (1976), 63–85.
- [38] —, Higher reciprocity law, modular forms of weight 1 and elliptic curves, *Nagoya Math. J.*, **98** (1985), 109–115.
- [39] T. Kubota, *Elementary theory of Eisenstein series*, Tokyo-New York: Kodansha and Halsted, 1973.
- [40] G. Lion and M. Vergne, *The Weil representation, Maslov index and theta series*, Boston: Birkhäuser, 1980.
- [41] C. J. Moreno, The higher reciprocity laws: an example, *J. Number Theory*, **12** (1980), 57–70.

- [42] —, The value of $L(1/2, \chi)$ for Abelian L-functions of complex quadratic fields, *J. Number Theory*, **18** (1984), 269–288.
- [43] D. Mumford, Theta characteristics of an algebraic curve, *Ann. scient. Éc. Norm. Sup.*, 4^e série, t. **4** (1971), 181–192.
- [44] H. Petersson, Über Eisensteinsche Reihen und automorphe Formen von der Dimension -1 , *Comment. Math. Helv.* **31** (1956), 111–144.
- [45] L. J. Rogers, Second memoir on the expansion of certain infinite products. *Proc. London Math. Soc.*, **25** (1894), 318–343.
- [46] A. Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, *J. Indian Math. Soc.* **20** (1956), 47–87.
- [47] —, Discontinuous groups and harmonic analysis, in *Proc. Int. Math. Congr.*, Stockholm, 1962, 177–189.
- [48] J.-P. Serre, Modular forms of weight one and Galois representations, in *Proc. Symposium on Algebraic Number Fields*, Academic Press, 1977, 193–268.
- [49] H. Shimizu, On traces of Hecke operators, *J. Fac. Sci. Univ. Tokyo, Sec. I* **10** (1963), 1–19.
- [50] T. Shintani, On certain ray class invariants of real quadratic fields, *J. Math. Soc. Japan*, **30** (1978), 139–167.
- [51] H. M. Stark, Class fields and modular forms of weight one, *Lecture Notes in Math.*, **601**, Springer-Verlag, 1977, 277–287.
- [52] Y. Tanigawa, On cusp forms of octahedral type, *Proc. Japan Akad.*, **57**, Ser. A, no. **7** (1986), 270–273.
- [53] — and H. Ishikawa, The dimension formula of the space of cusp forms of weight one for $\Gamma_0(p)$, to appear in *Nagoya Math. J.*
- [54] T. Tunnel, Artin's conjecture for representations of octahedral type, *Bull. Amer. Math. Soc.*, **5** (1981), 173–175.
- [55] —, A classical Diophantine problem and modular forms of weight $3/2$, *Invent. Math.*, **72** (1983), 323–334.
- [56] H. Weber, *Lehrbuch der Algebra III*, Braunschweig, 1908.
- [57] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Annalen*, **168** (1967), 149–156.
- [58] B. F. Wyman, What is a reciprocity law? *Amer. Math. Monthly*, **79** (1972), 571–586.
- [59] N. Yui, Explicit form of the modular equation, *J. Reine Angew. Math.*, **299/300** (1978), 185–200.
- [60] H. Zassenhaus and J. Liang, On a problem of Hasse, *Math. comp.*, **23** (1969), 515–519.
- [61] Seminar on Complex Multiplication, *Lecture Notes in Math.*, **21**, Springer-Verlag, 1966 (for the Institute Seminar by Borel, Chowla, Herz, Iwasawa and Serre, held in 1957–1958).

Department of Mathematics
Faculty of Science
Kobe University
Rokko, Kobe 657
Japan