THE QUADRATIC RECIPROCITY LAW AND THE ELEMENTARY THETA FUNCTION

by MARTIN EICHLER

Dedicated to Robert Rankin on his 70th Birthday

1. The rational case. This note points out a new aspect of the well-known relationship between the subjects mentioned in the title. The following result and its generalization in totally real algebraic number fields is central to the discussion. Let $\left(\frac{a}{b}\right)$ denote the Legendre symbol for relatively prime numbers a and $b \in \mathbb{Z}$ and $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ a substitution of the modular subgroup $\Gamma_0(4)$. Then, if $\gamma > 0$ and $b \equiv 1 \bmod 2$,

$$\left(\frac{a}{b}\right) = \left(\frac{A}{B}\right)\left(\frac{\gamma}{\delta}\right)(-1)^{W(b,B)} \tag{1}$$

with

$$W(b, B) = \tfrac{1}{4}(\operatorname{sign}(b)+1)(\operatorname{sign}(B)-1) - \tfrac{1}{4}(b+1)(B-1) \tag{1a}$$

and

$$A = \alpha a + \beta b, \qquad B = \gamma a + \delta b. \tag{1b}$$

According to (1), the Legendre symbol behaves somewhat like a modular function $\left(\text{apart from the known behaviour under } \frac{a}{b} \to \frac{a}{b} + 1 = \frac{a+b}{b} \text{ and } \frac{a}{b} \to \frac{-b}{a}\right)$. (1) follows (see below) from the functional equation

$$\vartheta(2\tau) = \sum_{n \in \mathbf{Z}} e(n^2\tau) = \vartheta\left(2\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) j\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \tau\right) \tag{2}$$

with

$$j\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \tau\right) = \left(\frac{\gamma}{\delta}\right) e\left(\tfrac{1}{8}(1-\varepsilon_\delta)\right)(\gamma\tau+\delta)^{-1/2} \tag{2a}$$

provided that

$$\gamma > 0 \quad \text{and} \quad -\frac{\pi}{2} < \arg(\gamma\tau+\delta)^{1/2} \leqq \frac{\pi}{2}. \tag{2b}$$

Here we used and always will use the abbreviation

$$e(x) = e^{2\pi i x}$$

and ε_δ means the absolutely least residue of δ mod 4. In the proof, Hecke [**4**] assumed $\gamma > 0$ (see also Shimura [**5**]).

Since $\vartheta(2\tau)^2$ is a modular form of weight 1 on $\Gamma_0(4)$ and character $\chi(d) = \left(\frac{-4}{d}\right)$, the essential content of (2) is the sign. On the other hand, (1) is closely related to the

Glasgow Math. J. **27** (1985) 19–30.

quadratic reciprocity law and its first supplement: for positive a, b,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{(a-1)(b-1)/4}, \qquad \left(\frac{-1}{a}\right)=(-1)^{(a-1)/2}. \tag{3}$$

Namely, with $\gamma=4b$, $\delta=a$, we have

$$A=\alpha a+\beta b, \qquad B=5ab, \qquad 4A=5\alpha a-1.$$

Now an easy calculation shows that

$$\left(\frac{A}{B}\right)=\left(\frac{-1}{a}\right)=(-1)^{1/2(a-1)}$$

and (1) becomes identical with (3).

The formulas (1)–(3) form a triad of the following nature: given the Gaussian sums

$$G(a,b)=\left(\frac{a}{b}\right)G(1,b), \qquad G(1,b)=|b|^{1/2}e(\tfrac{1}{8}(\mathrm{sign}(b)-\mathrm{sign}(\varepsilon_b))) \tag{4}$$

with ε_b the absolutely least residue of $b \bmod 4$, (1) and (2) are equivalent, while (2) follows from (3).

The essential tool in all our considerations is the theta function and its well-known relation with the Gaussian sums:

$$\lim_{\lambda\to 0}\lambda^{1/2}\vartheta\left(\frac{2a}{b}+i\lambda\right)=G(a,b)\,|b|^{-1}. \tag{5}$$

It suffices to prove only (3). The derivation of (1) from (2) and conversely is an easy straightforward calculation upon observation that $B\equiv\delta b \bmod 4$.

In the following, we will generalize (1)–(3) in totally real algebraic number fields. This time an analogue of (2) has not been given. We will therefore prove the reciprocity law and derive from it the two other formulas. In the case of the reciprocity law, we follow the approach of Kronecker and Hecke. The connection with earlier work on the subject will be commented on in §6.

2. Preliminaries. We consider a totally real algebraic number field K of degree n with conjugates K_ν. We assume that a and b are numbers in K such that

a and b are congruent to units ε_a and ε_b mod 4.

More generally, whenever the symbol ε_b occurs, this assumption on b is made.

We will use an abbreviated symbol for the sign:

$$\sigma(a)=\mathrm{sign}(a)=\pm 1 \text{ according as } a \text{ is positive or negative.}$$

We will make a further convention: if a symbol ξ_ν carries the subscript ν, attaching it to the νth conjugate field K_ν, we will write

$$S(\xi)=\sum_{\nu=1}^{n}\xi_\nu.$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

This is the trace if ξ is an element of K. But we will also write

$$S(\sigma(\xi)) = \sum_{\nu=1}^{n} \sigma(\xi_\nu).$$

Similarly we will write products as follows:

$$N(\xi) = \prod_{\nu=1}^{n} \xi_\nu, \qquad N(\gamma\tau+\delta) = \prod_{\nu=1}^{n} (\gamma_\nu\tau_\nu+\delta_\nu).$$

The different will be denoted by $\mathfrak{d}$, and $\mathfrak{g}$ will be an integral ideal equivalent with $\mathfrak{d}$. An element $g \in K$ whose ideal is

$$(g) = \mathfrak{g}\mathfrak{d}^{-1}$$

will be fixed throughout the paper.

We will consider the following subgroup of the Hilbert modular group, where $\mathfrak{o}$ is the maximal order of K:

$$\Gamma_{0,\varepsilon}(4\mathfrak{g}) = \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} : \alpha, \beta, \delta \in \mathfrak{o}, \gamma \in 4\mathfrak{g}, \delta \equiv \varepsilon_\delta \bmod 4 \right\}. \tag{6}$$

It has finite index in the full modular group.

The quadratic residue symbol is defined for prime ideals $\mathfrak{p}$ and numbers prime to $\mathfrak{p}$ by

$$\left(\frac{a}{\mathfrak{f}}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } \mathfrak{p}, \\ -1 & \text{otherwise,} \end{cases}$$

and for the prime decomposition

$$\mathfrak{b} = \mathfrak{p}_1^{h_1}\mathfrak{p}_2^{h_2}\dots$$

by

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{p}_1}\right)^{h_1}\left(\frac{a}{\mathfrak{p}_2}\right)^{h_2}\dots.$$

It is connected with the Gaussian sums

$$G_g(a, b) = \sum_{\rho \bmod b\mathfrak{o}} e\left(S\left(g\frac{a}{b}\rho^2\right)\right) \tag{7}$$

in well-known way.

LEMMA 1. *Let b be odd. Then*

$$G_g(a, b) = \left(\frac{a}{(b)}\right) G(1, b).$$

The statement implies that the quotient $G_g(a, b)/G_g(1, b)$ depends only on the ideal (b). With this in mind we may write $\left(\frac{a}{b}\right)$ instead of $\left(\frac{a}{(b)}\right)$.

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

Proof. In the sum over ρ in (7), we put

$$\rho = \rho_1 + \rho_2 + \dots, \qquad \rho_i \in b\mathfrak{p}_i^{-h_i} \bmod b\mathfrak{o},$$

h_i meaning the exact power of $\mathfrak{p}_i$ dividing b. Hence the sum becomes a product

$$G_{\mathfrak{g}}(a, b) = \prod H_{h_i}(a, b),$$

where

$$H_{h_i}(a, b) = \sum e\left(S\left(\mathfrak{g}\frac{a}{b}\rho^2\right)\right) \qquad (\rho \in b\mathfrak{p}_i^{-h_i} \bmod b\mathfrak{o})$$
$$= \sum e(S(\mathfrak{g}ab\rho^2)) \qquad (\rho \in \mathfrak{p}_i^{-h_i} \bmod \mathfrak{o}).$$

The $H_{h_i}(a, b)$ are further processed as follows (the subscript may be omitted). If $h > 1$, we take a prime element p for $\mathfrak{p}$ and put

$$\rho = \rho_1 + p^{h-1}\rho_2, \qquad \rho_1 \in \mathfrak{p}^{-h} \bmod \mathfrak{p}^{-1}, \qquad \rho_2 \in \mathfrak{p}^{-h} \bmod \mathfrak{p}^{1-h}.$$

Then

$$H_h(a, b) = \Sigma_1 e(S(\mathfrak{g}ab\rho_1^2)) + \Sigma_2 e(S(\mathfrak{g}ab(\rho_1^2 + 2p^{h-1}\rho_1\rho_2 + p^{2h-2}\rho_2^2))),$$

both sums are extended over ρ_1 and ρ_2, but, in Σ_1, ρ_1 is in $\mathfrak{p}^{1-h}$ while in Σ_2 it is not. The second sum is apparently 0. The first can be written (if $(p) = \mathfrak{q}\mathfrak{p}$)

$$H_h(a, b) = N(\mathfrak{g}) \sum e(S(\mathfrak{g}abp^{-2}(p\rho_1)^2)) \qquad (\rho_1 \in \mathfrak{q}\mathfrak{p}^{1-h} \bmod \mathfrak{q})$$
$$= N(\mathfrak{g}) \sum e(S(\mathfrak{g}abp^{-2}\rho_3^2)) \qquad (\rho_3 \in \mathfrak{q}\mathfrak{p}^{2-h} \bmod \mathfrak{q})$$
$$= N(\mathfrak{g}) H_{h-2}(a, bp^{-2}).$$

If $h = 2$, the sum over ρ_3 consists of only one summand, and

$$H_2(a, b) = N(\mathfrak{p}).$$

If $h = 1$ and a is a quadratic residue mod $\mathfrak{p}$,

$$H_1(a, b) = H_1(1, b),$$

and if a is a quadratic non-residue,

$$H_1(1, b) + H_1(a, b) = 2 \sum e(S(\mathfrak{g}\rho)) = 0 \qquad (\rho \in \mathfrak{p}^{-1} \bmod \mathfrak{o})$$

and so

$$H_1(a, b) = \left(\frac{a}{\mathfrak{p}}\right) H_1(1, b).$$

Induction on h and multiplication over all prime ideals gives

$$G_{\mathfrak{g}}(a, b) = \left(\frac{a}{(b)}\right) H(b),$$

where $H(b)$ depends only on b and the prime elements p. Inserting $a = 1$, we get the desired formula.

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

LEMMA 2. $G_g(1, b) = e(\frac{1}{8}S(\sigma(gb) - \sigma(g\varepsilon_b)))\left(\frac{b\varepsilon_b^{-1}}{g}\right)|Nb|^{1/2}$.

It will be proved in §5. From this follows

$$\left(\frac{-1}{b}\right) = \frac{\overline{G_g(1, b)}}{G_g(1, b)} = (-1)^{S(\sigma(g\varepsilon_b) - \sigma(gb))/2} = (-1)^{S(\sigma(b) - \sigma(\varepsilon_b))/2}. \tag{8}$$

The factor $\sigma(g)$ in the exponent has been omitted without changing its residue mod 2.

LEMMA 3. *For a_1, a_2 prime to b and b_1, b_2 prime to a and each other the following product rules hold:*

$$\left(\frac{a_1a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$

and

$$\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)\{b_1, b_2\}$$

with

$$\{b_1, b_2\} = \left(\frac{b_1}{b_2}\right)\left(\frac{b_2}{b_1}\right)(-1)^{w(b_1, b_2)},$$

$$w(b_1, b_2) = \tfrac{1}{4}S[(\sigma(b_1) - 1)(\sigma(b_2) - 1) - (\sigma(\varepsilon_{b_1}) - 1)(\sigma(\varepsilon_{b_2}) - 1)].$$

Proof. The first product rule is a consequence of Lemma 1.

In the sum

$$G_g(a, b_1b_2) = \sum e\left(S\left(g\frac{a}{b_1b_2}\rho^2\right)\right),$$

we put $\rho = b_2\rho_1 + b_1\rho_2$ and let ρ_1, ρ_2 run modulo b_1, b_2. Thus the sum becomes a product of two sums:

$$G_g(a, b_1b_2) = G_g(ab_2, b_1)G_g(ab_1, b_2).$$

Whence, by Lemma 1,

$$\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)\left(\frac{b_1}{b_2}\right)\left(\frac{b_2}{b_1}\right)\frac{G_g(1, b_1b_2)}{G_g(1, b_1)G_g(1, b_2)}$$

$$= \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)\left(\frac{b_1}{b_2}\right)\left(\frac{b_2}{b_1}\right)(-1)^{w'(b_1, b_2)}$$

with

$$w'(b_1, b_2) = \tfrac{1}{4}S[\sigma(g)(\sigma(b_1) - 1)(\sigma(b_2) - 1) - \sigma(g)(\sigma(\varepsilon_{b_1}) - 1)(\sigma(\varepsilon_{b_2}) - 1)].$$

The summands on the right are all congruent to 0 mod 4 and may therefore be replaced by their negatives without changing $w'(b_1, b_2)$ mod 2. So the factor $\sigma(g)$ in the sum may be dropped.

Our analogue of the simple theta function is

$$\vartheta_g(\tau) = \sum_{\omega} e(\tfrac{1}{2}S(g\omega^2\tau)), \tag{9}$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

where ω runs over all elements of the maximal order $\mathfrak{o}$ of K, and τ_ν are complex variables such that $g_\nu \tau_\nu$ have positive imaginary parts. Similar to (5), we will prove in §4 that

$$\lim_{\lambda \to 0} |N(\lambda)|^{1/2} \vartheta_g\left(2\frac{a}{b} + i\lambda\right) = G_g(a, b)\, |N(b)|^{-1} N(\mathfrak{g})^{-1/2} \tag{10}$$

with real λ_ν such that all $g_\nu \lambda_\nu > 0$.

3. The triad. The analogues of (1)–(3) are

$$\left(\frac{a}{b}\right) = \left(\frac{A}{B}\right)\left(\frac{\gamma}{\delta}\right)(-1)^{W(b,B)} \tag{11}$$

(where only $b \equiv \varepsilon_b \bmod 4$ is assumed while a is arbitrary) with

$$W(b, B) = \tfrac{1}{4}S((\sigma(b)+1)(\sigma(B)-1)) - \tfrac{1}{4}S((\sigma(\varepsilon_b)+1)(\sigma(\varepsilon_B)-1)) \tag{11a}$$

if

$$\alpha a + \beta b = A, \quad \gamma a + \delta b = B \quad \text{and} \quad \gamma_\nu > 0 \quad \text{for all} \quad \nu. \tag{11b}$$

$$\vartheta_g(2\tau) = \vartheta_g\left(2\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) j\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \tau\right) \tag{12}$$

with

$$j\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \tau\right) = \left(\frac{\gamma}{\delta}\right)\left(\frac{\delta\varepsilon_\delta^{-1}}{\mathfrak{g}}\right) e\left(\tfrac{1}{8}S(1-\sigma(\varepsilon_\delta))\right) N(\gamma\tau + \delta)^{-1/2} \tag{12a}$$

provided that, for all ν,

$$g_\nu > 0, \qquad \gamma_\nu > 0, \qquad -\frac{\pi}{2} < \arg(\gamma_\nu \tau_\nu + \delta_\nu) \leqq \frac{\pi}{2}. \tag{12b}$$

Also, we have the reciprocity law

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{w(a,b)} \tag{13}$$

with

$$w(a, b) = \tfrac{1}{4}S((\sigma(a)-1)(\sigma(b)-1)) - \tfrac{1}{4}S((\sigma(\varepsilon_a)-1)(\sigma(\varepsilon_b)-1)). \tag{3a}$$

We remind the reader that the use of ε_a and ε_b express the assumption that a and b are congruent to units ε_a and ε_b mod 4. (13) differs formally from a known formulation. That will be discussed in §6.

The equivalence of (11) *and* (12). At first it must be made clear that (12) holds up to an unknown root of unity $v(\gamma, \delta)$, which has to be shown in §4. Now we verify that (11) with this unknown factor $v(\gamma, \delta)$ follows from (12) with this same factor. This is an easy calculation in which the following points have to be observed.

(i) We study the behaviour (16) under the group

$$\begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} : \alpha'\delta' - \beta'\gamma' = 1, \qquad \alpha', \delta', \tfrac{1}{2}\beta' \in \mathfrak{o}, \qquad \gamma' \in 2\mathfrak{g}$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

acting on $\tau = 2\frac{a}{b} + i\lambda$. It is with $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \Gamma_{0\varepsilon}(4\mathfrak{g})$

$$\frac{\alpha'\tau+\beta'}{\gamma'\tau+\delta'} = 2\frac{\alpha a+\beta b}{\gamma a+\delta b} + i\lambda', \qquad \lambda' = \frac{b^2}{B^2}\lambda + O(\lambda^2).$$

(ii) The assumptions include

$$\varepsilon_B \equiv \varepsilon_\delta \varepsilon_b \bmod 4.$$

(iii) The last factor in (16) is (according to the condition (12b))

$$N(\gamma\tau+\delta)^{1/2} = N\left(\frac{B}{b} + i\gamma\lambda\right)^{1/2} = \prod_\nu \left(\frac{B_\nu}{b_\nu} + i\gamma_\nu\lambda_\nu\right)^{1/2},$$

the square root of each factor taken in the right half plane. This implies

$$\lim_{\lambda\to 0} N\left(\frac{B}{b} + i\gamma\lambda\right)^{1/2} = \left|N\left(\frac{B}{b}\right)\right|^{1/2} B(\tfrac{1}{8}S(1-\sigma(bB)))N(\sigma(g\gamma)^{(\sigma(bB)-1)/2}),$$

and $N(\ldots) = 1$ because we assume g and $\gamma \gg 0$.

(iv) The formula (10) both for

$$\vartheta_{\mathfrak{g}}\left(2\frac{a}{b} + i\lambda\right) \quad \text{and} \quad \vartheta_{\mathfrak{g}}\left(2\frac{A}{B} + i\lambda'\right)$$

translates (12) and (16) into the following relation between Gaussian sums:

$$G_{\mathfrak{g}}(a, b)\,|N(b)|^{-1}$$
$$= v(\gamma, \delta)\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta\varepsilon_\delta^{-1}}{\mathfrak{g}}\right)\left|N\left(\frac{B}{b}\right)\right|^{1/2} e(\tfrac{1}{8}S(1-\sigma(\varepsilon_\delta)+\sigma(bB)-1))G_{\mathfrak{g}}(A, B)\,|N(B)|^{-1},$$

which is evaluated by means of Lemma 2 and gives (11) with the factor $v(\gamma, \delta)$ on the right.

The derivation (13)→(11). We assume $g \gg 0$ and take $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ with the second line $\gamma = 4c^2b$, $\delta = a$, where c is the smallest rational integer divisible by $\mathfrak{g}$. Under this assumption

$$A = \alpha a + \beta b, \qquad B = (4c^2+1)ab, \qquad 4c^2A = (4c^2+1)\alpha a - 1.$$

Using Lemma 3 and (13), we have (because of (8))

$$\left(\frac{A}{B}\right) = \left(\frac{\alpha a+\beta b}{(4c^2+1)a}\right)\left(\frac{\alpha a}{b}\right) = \left(\frac{(4c^2+1)\alpha a - 1}{(4c^2+1)a}\right) = \left(\frac{-1}{(4c^2+1)a}\right) = \left(\frac{-1}{a}\right)$$

(the second factor in the second term is 1 because $\alpha a - 4c^2\beta b = 1$). With the supplementary rule (8), (11) is now

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = v(\gamma, \delta)(-1)^{w(a,b)}$$

with $w(a, b)$ as in (13a). Because of (13), the factor $v(\gamma, \delta)$ is 1.

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

Application of (11) with

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4\gamma & 1 \end{bmatrix}$$

yields

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b+4\gamma a}\right)$$

under various assumptions on a, b, and γ, for instance if these are all totally positive. This is already a weak form of the reciprocity law.

REMARK 1. The assumptions $g \gg 0$, $\gamma \gg 0$ are essential. Without them a further factor $N(\sigma(g\gamma)\ldots)$ would appear in (11), which would be inconsistent with the reciprocity law. Also a weaker assumption $g\gamma \gg 0$ would change (11) and (12).

REMARK 2. The terms $\delta(\varepsilon_b)$ etc, in Lemma 2 and (11)–(13) cannot easily be seen to be invariants of b etc. when ε_b is replaced by another unit $\varepsilon_b' \equiv \varepsilon_b \bmod 4$. Nevertheless, *Lemma* 2 *and* (11)–(13) *contain intrinsic statements and cannot depend on the choice of* ε_b. For further remarks on this point see §6.

4. The theta function. From now on we drop the assumption $g \gg 0$. We have to use two specializations of the matrix theta function

$$\vartheta(T, x, y) = \sum e(\tfrac{1}{2}T[m-y] + x^t m - \tfrac{1}{2}x^t y), \tag{14}$$

where T is an n-rowed complex matrix in the Siegel upper half space, and x and y are complex column vectors; m runs over all vectors with components in $\mathbb{Z}$, and

$$T[m-y] = (m-y)^t T(m-y).$$

Let ω^μ be a basis of the maximal order $\mathfrak{o}$ of K. With it we form the matrix $\Omega = (\omega_\nu^\mu)$ in which μ numbers the rows and ν the columns, ω_ν^μ being the νth conjugate of ω^μ. We put

$$T = \Omega \operatorname{diag}(g\tau)\Omega^t, \tag{15}$$

where $\operatorname{diag}(g\tau)$ means the diagonal matrix with the entries $g_\nu \tau_\nu$. The τ_ν are n variables, and we assume that the imaginary parts of $g_\nu \tau_\nu$ are positive.

Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ be the $2n$-rowed matrix with

$$A = \Omega \operatorname{diag}(\alpha')\Omega^{-1}, \qquad B = \Omega \operatorname{diag}(g\beta')\Omega^t,$$

$$C = \Omega^{-t} \operatorname{diag}(g^{-1}\gamma')\Omega^{-1}, \qquad D = \Omega^{-t} \operatorname{diag}(\delta')\Omega^t$$

and

$$\alpha', \delta' \in \mathfrak{o}, \qquad \beta' \in \mathfrak{g}^{-1}, \qquad \gamma' \in \mathfrak{g}.$$

It belongs to the Siegel modular group Γ_n, and even to the so-called theta subgroup $\Gamma_{\vartheta,n}$ if the symmetric matrices

$$C^t A = \Omega^{-t} \operatorname{diag}(g\alpha'\gamma')\Omega^{-1}, \qquad D^t B = \Omega \operatorname{diag}(g\beta'\delta')\Omega^t$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

have even diagonal elements, and this is the case if

$$\alpha'\gamma' \in 2\mathfrak{g}, \qquad \beta'\delta' \in 2\mathfrak{g}^{-1}.$$

But we will only demand $\alpha', \delta' \in \mathfrak{o}$ and $\beta' \in 2\mathfrak{o}$, $\gamma' \in 2\mathfrak{g}$. Under this condition the theta function satisfied the functional equation [**1**], [**2**]

$$\vartheta(T, x, y) = \chi(M)\vartheta((AT+B)(CT+D)^{-1}, Ax+By, Cx+Dy)\det(CT+D)^{-1/2}$$

with a root of unity $\chi(M)$. When T is specialized as in (15) and $x = y = 0$ it assumes the form

$$\vartheta_{\mathfrak{g}}(\tau) = \sum_{\omega} e(\tfrac{1}{2}S(\mathfrak{g}\omega^2\tau)) = \chi(M)\vartheta_{\mathfrak{g}}\left(\frac{\alpha'\tau+\beta'}{\gamma'\tau+\delta'}\right)N(\gamma'\tau+\delta')^{-1/2} \tag{16}$$

which can be written as (12) with another root of unity $v(\gamma, \delta)$ on the right and

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \frac{1}{2}\beta' \\ 2\gamma' & \delta' \end{bmatrix}.$$

In §3 it was proved that $v(\gamma, \delta) = 1$ from the reciprocity law.

A further application of the general functional equation is [**1**]

$$\vartheta(T, 0, y) = \det(-iT)^{-1/2}\vartheta(-T^{-1}, y, 0), \tag{17}$$

where the square root is positive for $T = iY$ if Y is positive definite and analytically continued in the upper half space. For T as in (15) we have, with the discriminant D of K:

$$\det(-iT)^{1/2} = |D|^{1/2} N(-i\mathfrak{g}\tau)^{1/2} = |D|^{1/2} \prod (-i\mathfrak{g}_\nu\tau_\nu)^{1/2}$$

with positive real parts. The inverse matrix is

$$T^{-1} = \Omega^{-t} \operatorname{diag}(\mathfrak{g}^{-1})\operatorname{diag}(\mathfrak{g}\tau^{-1})\operatorname{diag}(\mathfrak{g}^{-1})\Omega^{-1}.$$

Here we have

$$\Omega^{-t} \operatorname{diag}(\mathfrak{g}^{-1}) = \begin{bmatrix} \tilde{\omega}_1^1\mathfrak{g}_1^{-1} & \dots & \tilde{\omega}_n^1\mathfrak{g}_n^{-1} \\ \vdots & & \vdots \\ \tilde{\omega}_1^n\mathfrak{g}_1^{-1} & \dots & \tilde{\omega}_n^n\mathfrak{g}_n^{-1} \end{bmatrix},$$

and $\tilde{\omega}^1\mathfrak{g}^{-1}, \dots, \tilde{\omega}^n\mathfrak{g}^{-1}$ is a basis of the ideal $\mathfrak{d}^{-1}\mathfrak{g}^{-1} = \mathfrak{g}^{-1}$.

Now (17) assumes the form

$$\begin{aligned} \vartheta_{\mathfrak{g}}(\tau, \eta, \sigma) &= \sum_{\omega \in \mathfrak{o}} e(\tfrac{1}{2}S(\mathfrak{g}(\omega-\eta)^2\tau)) \\ &= |D|^{-1/2} N(-i\mathfrak{g}\tau)^{-1/2} \sum_{\omega \in \mathfrak{g}^{-1}} e\left(\frac{-1}{2} S(\mathfrak{g}\omega^2\tau^{-1}) + S(\omega\eta)\right). \end{aligned} \tag{18}$$

As a first application of (18), we consider the theta function (9) with $\tau = \dfrac{2a}{b} + i\lambda$:

$$\vartheta_{\mathfrak{g}}\left(2\frac{a}{b} + i\lambda\right) = \sum_{\rho \bmod b} e\left(S\left(\mathfrak{g}\frac{a}{b}\rho^2\right)\right) \sum_{\omega \in \mathfrak{o}} e\left(\frac{i}{2} S\left(\mathfrak{g}b^2\left(\omega + \frac{\rho}{b}\right)^2\lambda\right)\right). \tag{19}$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

The second factor is as in (18) with $\tau = i\lambda$ and gb^2 instead of g and therefore equals

$$|N(\lambda)|^{-1/2}|D|^{-1/2}|N(g)|^{-1/2}|N(b)|^{-1}\sum_{\omega\in \mathfrak{g}^{-1}} e\left(\frac{i}{2}S(g\omega^2\lambda^{-1})+S\left(\omega\frac{\rho}{b}\right)\right). \tag{20}$$

As $\lambda \to 0$, all terms in the sum vanish except that for $\omega = 0$, and so we get (10), observing that $|D|\,|N(g)| = |N(\mathfrak{g})|$.

5. The reciprocity law. We begin with $\tau = \dfrac{2a}{b} + i\lambda$, $\eta = 0$ in (18), using

$$-\tau^{-1} = -\frac{b}{2a} + i\lambda' + O(\lambda^2), \qquad \lambda' = \left(\frac{b}{2a}\right)^2\lambda$$

and

$$\lim_{\lambda\to 0} N(-ig\tau)^{1/2} = |N(g)|^{1/2}\left|N\left(\frac{2a}{b}\right)\right|^{1/2} e\left(\frac{-1}{8}S(\sigma(gab))\right).$$

In this way we get

$$\lim_{\lambda\to 0}|N(\lambda)|^{1/2}\vartheta_g\left(2\frac{a}{b}+i\lambda\right) = |D|^{-1/2}|N(g)|^{-1/2}\left|N\left(\frac{2a}{b}\right)\right|^{1/2} e(\tfrac{1}{8}S(\sigma(gab)))$$
$$\times\lim_{\lambda'\to 0}|N(\lambda')|^{1/2}\sum_{\rho} e\left(\frac{-1}{4}S\left(\frac{gb}{a}\rho^2\right)\right)\sum_{\omega\in\mathfrak{o}} e\left(\frac{i}{2}S\left(4a^2 g\left(\omega+\frac{\rho}{2a}\right)^2\lambda'\right)\right),$$

where ρ runs over the residues of $\mathfrak{g}^{-1} \bmod 2a\mathfrak{o}$ and ω over $\mathfrak{o}$ if $\mathfrak{g}$ is prime to $2a$. The second sum is similar to that in (19), (20) and yields after multiplication by $N(\lambda')^{1/2}$ the limit

$$|N(2a)|^{-1}|N(\mathfrak{g})|^{-1/2}.$$

Collecting the last results together with (10), we obtain

$$G_g(a, b)\,|N(b)|^{-1/2} = e(\tfrac{1}{8}S(\sigma(gab)))\,|N(2a)|^{-1/2}|N(\mathfrak{g})|^{-1/2}\sum_{\rho} e\left(\frac{-1}{4}S\left(\frac{ga}{b}\rho^2\right)\right), \tag{21}$$

where ρ runs over a system of representatives of $\mathfrak{g}^{-1} \bmod 2a\mathfrak{o}$.

It remains to determine the finite sum on the right. For this we put (assuming a odd and $\mathfrak{g}$ prime to $2a$)

$$\rho = \rho_0 + a\rho_1 + 2\rho_2 \quad \text{with} \quad \rho_0 \in \mathfrak{g}^{-1} \bmod \mathfrak{o},\ \rho_1 \in \mathfrak{o} \bmod 2\mathfrak{o},\ \rho_2 \in \mathfrak{o} \bmod a\mathfrak{o}.$$

Instead of ρ_0 and ρ_1 we can write $2a\rho_0$ and $a\rho_1$. So the sum becomes a product

$$|N(2a)|^{-1/2}|N(\mathfrak{g})|^{-1/2}\sum_{\rho} e\left(\frac{-1}{4}S\left(\frac{gb}{a}\rho^2\right)\right) = H\mathfrak{g}(ab)H_2(ab)G_g(-b, a)\,|N(a)|^{-1/2}$$

with the abbreviations

$$H_{\mathfrak{g}}(ab) = |N(\mathfrak{g})|^{-1/2}\sum_{\rho_0} e(-S(gab\rho_0^2)) \qquad (\rho_0 \in \mathfrak{g}^{-1} \bmod \mathfrak{o}) \tag{22}$$

https://doi.org/10.1017/S0017089500006042 Published online by Cambridge University Press

and

$$H_2(ab) = 2^{-n/2} \sum_{\rho_1} e\left(\frac{-1}{4} S(gab\rho_1^2)\right) \qquad (\rho_1 \in \mathfrak{o} \bmod 2\mathfrak{o}). \tag{23}$$

Comparison with (21) yields the nucleus of the reciprocity law

$$G_g(a, b)\,|N(b)|^{-1/2} = e(\tfrac{1}{8}S(\sigma(gab)))H_{\mathfrak{g}}(ab)H_2(ab)G_g(-b, a)\,|N(a)|^{-1/2}. \tag{24}$$

To proceed further we need the following lemma.

LEMMA 4.

$$H_{\mathfrak{g}}(b) = \left(\frac{b}{\mathfrak{g}}\right)H_{\mathfrak{g}}(1).$$

It is almost identical to Lemma 1 if there the summation is over $\rho = b\rho_1$, ρ_1 running over $b^{-1}\mathfrak{o} \bmod \mathfrak{o}$.

After this preparation we proceed with the discussion of (24). At first we insert $a = 1$, $b = \varepsilon$, a unit, and get

$$1 = e(\tfrac{1}{8}S(\sigma(g\varepsilon)))H_{\mathfrak{g}}(\varepsilon)H_2(\varepsilon). \tag{25}$$

Now we divide (24) with $a = 1$ by (25) with $\varepsilon = \varepsilon_b$ and use Lemma 4 and $H_2(b) = H_2(\varepsilon_b)$. This gives the value of Lemma 2 for the Gaussian sum.

Finally we divide (24) by (25), but with $\varepsilon = \varepsilon_a\varepsilon_b$:

$$\left(\frac{a}{b}\right)G_g(1, b)\,|N(b)|^{-1/2} = e(\tfrac{1}{8}S(\sigma(gab) - \sigma(g\varepsilon_a\varepsilon_b)))\left(\frac{ab\varepsilon_a^{-1}\varepsilon_b^{-1}}{\mathfrak{g}}\right)G_g(-b, a)\,|N(a)|^{-1/2}.$$

Knowing the Gaussian sums on both sides and the value (8) for $\left(\frac{-1}{a}\right)$, we obtain now

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{w(a,b)},$$

$$w(a, b) = \tfrac{1}{4}S[\sigma(g)(\sigma(a) - 1)(\sigma(b) - 1) - \sigma(g)(\sigma(\varepsilon_a) - 1)(\sigma(\varepsilon_b) - 1)].$$

Since the individual summands are all congruent to 0 mod 4, we may change their signs and so drop the factor $\sigma(g)$. This completes the proof of (13).

6. Remarks on the literature. An extensive survey of previous work on the reciprocity law has been given by Siegel [**6**], including an independent proof which also covers mixed real and imaginary fields. We need not repeat it, but we will only mention that the first proof in the rational case, using the theta function, has been given by Kronecker. Hecke [**3**] extended the proof to real quadratic fields.

Surprisingly there are two versions of the reciprocity law, namely (13) and

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^w, \qquad w = \tfrac{1}{4}S[(\sigma(a) - 1)(\sigma(b) - 1) + (a - 1)(b - 1)] \tag{26}$$

if $a \equiv b \equiv 1 \bmod 2$. In the mixed real and imaginary case, we must put $\sigma(a_\nu) = \sigma(b_\nu) = 1$ if K_ν is not real. The same formula has been proved by Hasse in the context of class field theory (see [**6**]).

Evidently (13) and (26) coincide in case of the rational field $\mathbb{Q}$. For $k \supset \mathbb{Q}$ the comparison of (13) and (26) implies

$$S[(\varepsilon_a - 1)(\varepsilon_b - 1)] \equiv S[(\sigma(\varepsilon_a) - 1)(\sigma(\varepsilon_b) - 1)] \bmod 8$$

for two units ε_a and ε_b which are congruent to $1 \bmod 2$. (For the notation see the convention in §2.)

In the case $K = \mathbb{Q}(\sqrt{d})$, (27) can be checked independently. It is particularly easy if $N(\varepsilon_a) = N(\varepsilon_b) = 1$. If $N(\varepsilon_a) = 1$, $N(\varepsilon_b) = -1$, ε_a is the square of another unit, and if $N(\varepsilon_a) = N(\varepsilon_b) = -1$, their quotient is a square.

The invariance of the expression for $G_g(1, b)$ in Lemma 2 under a change $\varepsilon_b \to \varepsilon_b'$ in the quadratic case is also evident, because under the assumptions made the quotient of both units is a square.

Lastly, the case $K = \mathbb{Q}(\sqrt{d})$ shows that our assumptions on a and b cover partly different cases than those of Siegel and Hasse, and sometimes even more cases.

REFERENCES

1. M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und funktionen* (Birkhäuser 1963), 55–57, *Introduction to Algebraic numbers and functions* (Academic Press, 1966), 41–43.

2. E. Freitag, *Siegelsche Modulfunktionen*, (*Springer*, 1982), 2. Anhang, Satz A 2.4.

3. E. Hecke, *Mathematische Werke* (Vandenhoek und Ruprecht, 1959), No 13.

4. E. Hecke, *Mathematische Werke* (Vandenhoek und Ruprecht, 1959) No 42, 940.

5. G. Shimura, On modular forms of half integral weight, *Ann. Math.* **97** (1973), 443.

6. C. L. Siegel, *Gesammelte Abhandlungen*, Bd. III. (Springer, 1966).

27, IM LEE
CH 4144 ARLESHEIM
SWITZERLAND