EXPLICIT FORMULAS FOR HECKE GAUSS SUMS IN QUADRATIC NUMBER FIELDS

HATICE BOYLAN AND NILS-PETER SKORUPPA

Abstract. We derive an explicit formula for Hecke Gauss sums of quadratic number fields. As an immediate consequence we obtain a quadratic reciprocity law in quadratic number fields which generalizes the classical one given by Hecke. The proofs use, apart from the well-known formulas for ordinary Gauss sums, only elementary algebraic manipulations.

1. Introduction and statement of results

Gauss's fourth proof of the quadratic reciprocity law involved the calculation of quadratic Gauss sums

$$\tau_a(b) = \sum_{t=0}^{a-1} e^{2\pi i b t^2/a}. \tag{1}$$

For relatively prime $a > 0$ and b, we know [Gau11]

$$\tau_a(b) = \begin{cases} \left(\frac{b}{a}\right)\sqrt{a} & \text{if } a \equiv 1 \bmod 4 \\ \left(\frac{b}{a}\right) i\sqrt{a} & \text{if } a \equiv 3 \bmod 4 \\ \left(\frac{b}{2a}\right) e^{2\pi i b/8}\sqrt{2a} & \text{if } a = 2^n,\ n \geq 2 \end{cases} \tag{2}$$

(see below for the definition of the generalized Legendre symbol $\left(\frac{a}{b}\right)$). Using the easily proved identities $\tau_a(b) = \left(\frac{b}{a}\right)\tau_a(1)$ and

$$\tau_{aa'}(b) = \tau_a(a'b)\tau_{a'}(ab) \tag{3}$$

for pairwise coprime integers b, a, a' with $a, a' > 0$, the quadratic reciprocity law becomes an immediate consequence. Indeed, for different odd prime numbers p and q, we write

$$\tau_{pq}(1) = \tau_p(q)\tau_q(p) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_p(1)\tau_q(1).$$

Then inserting the values (2) for $\tau_a(1)$, we obtain the quadratic reciprocity law.

The Gauss sums (1) appeared in Dirichlet's work on class number formulas for quadratic number fields, and in the related proof of the theorem on primes in arithmetic progressions, in which he introduced the L-series that bear his name. Gauss sums show up in the functional equation of these L-series. Ishii [Ish98] showed that the facts needed for Gauss's fourth proof of the reciprocity law can all be read off from the functional equation of the L-series of the biquadratic number field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Dirichlet found proofs for Gauss's result (2) based on the Poisson summation formula [Dir35], [Dir40]. Cauchy gave another proof using theta functions [Cau40]. Hecke generalized Cauchy's method to arbitrary algebraic number fields by introducing *Hecke Gauss sums*, in which the modulus a in (1) is replaced by an ideal $\mathfrak{a}$

2000 *Mathematics Subject Classification.* 11L05.

Key words and phrases. Hecke reciprocity, Gauss sums.

During the preparation of this article the first author was supported by TÜBİTAK, the Scientific and Technological Research Council of Turkey, and the University of Siegen.

in the number field. He then used theta functions to prove a reciprocity formula for these Gauss sums and used these results for showing the existence of quadratic class fields and for proving a quadratic reciprocity law in general number fields. Hecke's results can be found in [Hec70, 195-238] and the expositions given by Hasse [Has65] and (in a different language) by Neukirch [Neu99, 470-493]. However, Hecke did not obtain explicit formulas for his Gauss sums like the ones in (2). It is remarkable that, to the authors' knowledge, no such formulas are known for number fields different from $\mathbb{Q}$.

Before introducing Gauss sums of arbitrary number fields, Hecke studied first of all such sums for quadratic number fields [Hec83, Nr. 13]. Namely, if K is a quadratic number field, say $K = \mathbb{Q}(\sqrt{D})$, where D is the discriminant of K, Hecke considered the sums

$$G(\omega) := \sum_{\mu \bmod \mathfrak{a}} e^{2\pi i \mathrm{Tr}(\mu^2\omega/\sqrt{D})},$$

where $\omega \in K^*$ and $\mathfrak{a}$ is the denominator of ω (see Section 2). Here, for α in K, we use $\mathrm{Tr}(\alpha) = \alpha + \alpha'$, where α' is the conjugate of α. We shall also use $\mathrm{N}(\alpha) = \alpha\alpha'$.

The main purpose of this article is to derive an explicit formula for these sums. Namely, we shall prove:

Theorem. *Let ω be a nonzero element of $K = \mathbb{Q}(\sqrt{D})$, and let M be the smallest positive rational integer such that $M\omega$ is integral. Then*

$$G(\omega)/\sqrt{\mathrm{N}\big(\mathfrak{a}\,\gcd(2,\mathfrak{a})\big)} = \frac{1}{\sqrt{u}} \sum_{\Delta_1} \left(\tfrac{\Delta_1}{A}\right) \left(\tfrac{4\mathrm{N}(\beta)/\Delta_1}{N/|\Delta_1|}\right) \sqrt{\mathrm{sgn}(\Delta_1)}. \tag{4}$$

Here $N = M/2$ if D, M and $\mathrm{Tr}(M\omega/\sqrt{D})$ are even, and $N = M$ otherwise. Furthermore, $\beta = N\omega$. The sum is over all integers Δ_1 such that $|\Delta_1| = \gcd(N, 4\mathrm{N}(\beta))$ and such that Δ_1 and $4\mathrm{N}(\beta)/\Delta_1$ are squares modulo 4. Moreover, A denotes any integer relatively prime to N such that $A = \mathrm{Tr}(\beta\mu^2/\sqrt{D})$ for some integer μ in K. Finally, $u = 2$ if there are two terms in the sum and $u=1$ otherwise.

We explain some notations and implicit statements used in the theorem. By $\sqrt{x}$, for a real number $x \neq 0$, we mean always the square root which is positive or has positive imaginary part. For integers $a > 0$ and b, we use $\left(\frac{b}{a}\right)$ for the generalized Legendre symbol, i.e. the symbol which is multiplicative in a and in b, which equals the usual Legendre symbol if a is an odd prime, and which, for $a = 2$, equals 1, -1 or 0 accordingly as $b \equiv \pm 1 \bmod 8$, $b \equiv \pm 3 \bmod 8$ or b is even, respectively. It is not hard to show that $\mathrm{Tr}(\beta\mu^2/\sqrt{D})$ is an integral quadratic form on the ring of integers of K, whose discriminant equals $4\mathrm{N}(\beta)$ and whose content is relatively prime to N (see Lemma 1 in Section 2). In particular, this form represents indeed integers A which are relatively prime to N as implicitly claimed in the theorem.

Note that the sum in formula (4) contains at most 2 terms, and that $B(\omega) := G(\omega)/\sqrt{\mathrm{N}\big(\mathfrak{a}\,\gcd(2,\mathfrak{a})\big)}$ is an eighth root of unity if $G(\omega) \neq 0$. In fact, the sum contains two terms, and then $B(\omega)$ is a primitive eighth root of unity, if D or $a := \mathrm{Tr}(M\omega/\sqrt{D})$ is odd, if $4|M$ and the 2-part of M divides $n := \mathrm{N}(M\omega)$ (see Lemma 3). The sum contains no terms, and hence $G(\omega) = 0$, if D or a is odd, and $M = 2$ or M is exact divisor of $2n$. Otherwise the sum contains exactly one term and $B(\omega)$ is a fourth root of unity.

For those ω, which can be written as quotient β/α with relatively prime integers α and β in K[1], the integer α being odd, the formula (4) can be rewritten in

[1]If the class number of K is 1, then every number in K can be written in the form β/α with relatively prime integers β and α. Note that the reverse statement holds also true. Indeed, if $\mathfrak{a}$ is an integral ideal, say, $\mathfrak{a} = (\alpha_0, \beta_0)$, and if we can write $\beta_0/\alpha_0 = \beta/\alpha$ with relatively prime integers α and β, then $\beta_0 = \beta\mathfrak{a}$ and $\alpha_0 = \alpha\mathfrak{a}$, and hence $\mathfrak{a}$ is a principal ideal.

a different and surprisingly simple way. For explaining this we need some more notation. Recall from [Hec70, §54] that, for relatively prime integers β and odd α in K, one uses $\left(\frac{\beta}{\alpha}\right)$ for the product of the symbols $\left(\frac{\beta}{\mathfrak{p}}\right)$, where $\mathfrak{p}$ runs through all (not necessarily different) prime ideals dividing α, and where $\left(\frac{\beta}{\mathfrak{p}}\right)$ equals $+1$ or -1 accordingly as β is a square modulo $\mathfrak{p}$ or not.

For an odd integer α in K, we denote by ε_α that integer in $\{\pm 1\}$ such that $\varepsilon_\alpha \mathrm{N}(\alpha) \equiv 1 \bmod 4$. If the discriminant D is exactly divisible by 4 then every odd integer α in K has norm congruent to 1 modulo 4 and consequently $\varepsilon_\alpha = +1$, and vice versa. If D is not exactly divisible by 4, then there exist a unique Dirichlet character χ_- modulo 4 on the ring of integers in K such that, for every integer α in K whose norm is congruent to -1 modulo 4, one has $\chi_-(\alpha) \equiv \mathrm{Tr}\big(\alpha\mu^2/\sqrt{D}\big) \bmod 4$ for all integers μ such that the right hand side is odd. See Lemma 5 in Section 2 for a more detailed explanation and the proof of the statements made in this paragraph. For any D, we use χ_+ for the trivial Dirichlet character modulo 1 on the ring of integers in K.

Finally, for nonzero real numbers a and b we set $(a,b)_\infty$ equal to -1 if a and b are both negative and equal to $+1$ otherwise, i.e. $(a,b)_\infty$ denotes the Hilbert symbol for the field of real numbers. For odd α, the formula (4) can then be restated as follows:

Supplement to the theorem. *For relatively prime integers α and β of $\mathbb{Q}\big(\sqrt{D}\big)$, the integer α being odd, one has*

$$G(\beta/\alpha) = \left(\frac{\beta}{\alpha}\right) \chi_{\varepsilon_\alpha}(\alpha)\, \big(A, \mathrm{N}(\alpha)\big)_\infty \big(\varepsilon_\alpha, -\mathrm{N}(\alpha)\big)_\infty \sqrt{\varepsilon_\alpha \mathrm{N}(\alpha)}. \tag{5}$$

Here A denotes any nonzero number represented by the quadratic form $Q(\mu) := \mathrm{Tr}(\alpha\mu^2/\sqrt{D})$.

Note that the discriminant of $Q(\mu)$ equals $4\mathrm{N}(\alpha)$. Hence $\big(A, \mathrm{N}(\alpha)\big)_\infty$ equals -1 if and only if Q is negative definite. In particular, this symbol does not depend on the choice of A. For the (not obvious) deduction of (5) from (4) see Section 2.

Mimicking the proof of quadratic reciprocity sketched in the beginning the formula of the supplement to the theorem implies a quadratic reciprocity law for quadratic number fields which generalizes the one given by Hecke [Hec70, Satz 165]. Namely, it is easily proved [Hec70, Eq. (169)] that

$$G(1/\alpha\beta) = G(\beta/\alpha)G(\alpha/\beta). \tag{6}$$

Inserting (5) into the last identity, we obtain the following reciprocity law (see section 2 for the details of the proof).

Corollary (Quadratic Reciprocity)**.** *For any pair of relatively prime odd integers α and β in a quadratic number field K, one has*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \chi_{\varepsilon_\alpha}(\beta)\chi_{\varepsilon_\beta}(\alpha)\, (\varepsilon_\alpha, \varepsilon_\beta)_\infty \prod_\sigma \big(\sigma(\alpha), \sigma(\beta)\big)_\infty. \tag{7}$$

Here σ runs through the real embeddings of K, and the product is taken as 1 if K is complex.

Note that (7) generalizes the quadratic reciprocity law given in [Hec70, Satz 165], where it is assumed that at least one of the numbers α or β is a square modulo 4. Indeed, if, say, α is a square modulo 4, then $\mathrm{N}(\alpha) \equiv 1 \bmod 4$ and $\epsilon_\alpha = +1$. Accordingly, the right hand side of (7) reduces to the product, which is the formula [Hec70, Satz 165].

Our proof of the main theorem and, in particular, for the quadratic reciprocity law uses, apart from elementary algebraic manipulations, only the formulas (2)

for the ordinary Gauss sums and ordinary quadratic reciprocity, which, however, follows from (2). It is remarkable, that hence, as a consequence, the quadratic reciprocity law for quadratic number fields is not a genuine new reciprocity law. This is in contrast to what is suggested by Hecke's proof which makes extensive use of theta series associated to number fields.

A formula similar to the one in the theorem, but for general Gauss sums associated to arbitrary rational binary quadratic forms was proved in [SZ89, §4, Theorem 3]. It is possible (though not completely obvious) to deduce our main theorem from the formula in [SZ89]. However, this would give an essentially different proof of our formula (4) since the authors make intensive use of the theory of theta functions for deducing their formula.

We finally remark that we also verified the formulas (4) and (5) experimentally for several thousands of numbers ω, α and β using [S$^+$09].

Acknowledgment. The first author would like to express her gratitude to Franz Lemmermeyer for introducing her to the subject and for many helpful discussions.

2. Proof of the Theorem and its Consequences

As in the theorem, K denotes a quadratic number field, say $K = \mathbb{Q}(\sqrt{D})$, where D is the discriminant of K. As in Section 1, for $\beta \in K$, we use β' for its conjugate, so that $\mathrm{Tr}(\beta) = \beta + \beta'$ and $\mathrm{N}(\beta) = \beta\beta'$. Recall that $O = \mathbb{Z} + \mathbb{Z}\gamma$, where $\gamma = \sqrt{D}/2$, for $D \equiv 0 \bmod 4$ and $\gamma = 1 + \sqrt{D}/2$ for $D \equiv 1 \bmod 4$.

Also as in the theorem we fix for the following an element $\omega \neq 0$ in K. We use $\mathfrak{a}$ for its denominator, i.e. for the integral ideal such that $\omega O = \mathfrak{b}\mathfrak{a}^{-1}$ with an integral ideal $\mathfrak{b}$ which is relatively prime to $\mathfrak{a}$, and we use M for the smallest positive rational integer such that $M\omega$ is integral.

The proof of the theorem is based on the following Lemmas 1, 2, 3 and 4, the middle two of which cover the special case of the theorem that the denominator of ω is odd respectively contains only even prime ideal powers. The general case can then be reduced to these cases using the easily proved multiplicativity of the Hecke Gauss sums as recalled in Lemma 4. For the proof of the Lemmas 2 and 3 we determine in Lemma 1 invariants of the quadratic form $\mathrm{Tr}(\mu^2 M\omega/\sqrt{D})$ and reduce the calculation of the Hecke Gauss sums in question by elementary manipulations to the formulas (2).

Lemma 1. *The function $Q(\mu) = \mathrm{Tr}(\mu^2 M\omega/\sqrt{D})$ is an integral quadratic form on O with discriminant $4\mathrm{N}(M\omega)$. Its content is relatively prime to M unless D, M and $Q(1)$ are simultaneously even. In the latter case, the greatest common divisor of M and the content of Q is 2.*

Proof. Set $\beta := M\omega$. It is clear that $Q(\mu) = \mathrm{Tr}(\mu^2\beta/\sqrt{D})$ is an integral quadratic form on O. If we write $\mu = x + y\gamma$, then $Q(\mu) = ax^2 + bxy + cy^2$, where $(a, b, c) = \big(\mathrm{Tr}(\beta/\sqrt{D}), \mathrm{Tr}(2\beta\gamma/\sqrt{D}), \mathrm{Tr}(\beta\gamma^2/\sqrt{D})\big)$. Let $\Delta = b^2 - 4ac$ denote the discriminant of the form. Note that

$$T := \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \gamma & \gamma' \end{pmatrix} \begin{pmatrix} \beta/\sqrt{D} & 0 \\ 0 & (\beta/\sqrt{D})' \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 1 & \gamma' \end{pmatrix}. \tag{8}$$

Hence $\Delta = -4\det(T) = 4\mathrm{N}(\beta)$. Let $\mathrm{cont}(Q)$ denote the content of the form Q, i.e. the greatest common divisor of a, b and c) and $g := \gcd(M, \mathrm{cont}(Q))$. If we write $\beta = u + v\gamma$, we obtain

$$(a, b, c) = \begin{cases} \big(v, 2u, \frac{vD}{4}\big) & \text{if } D \equiv 0 \bmod 4 \\ \Big(v, 2(u+v), u + \frac{v(D+3)}{4}\Big) & \text{if } D \equiv 1 \bmod 4. \end{cases} \tag{9}$$

Suppose p is an odd prime divisor of g. Then $p|\beta$, since, by equation (9), $p|u$ and $p|v$. But then we have $\omega = \frac{\beta/p}{M/p}$ and $\mathfrak{a}|\frac{M}{p}$. But this contradicts the minimality of M. So g is a power of 2.

Suppose that one of D, v or M is odd. If 2 divided g, then M would be even and, again by equation (9), v would be even too, hence D would be odd, and thus u even and 2 would divide β. As before we conclude that $\mathfrak{a}$ would divide $M/2$, which contradicts the minimality of M.

Lastly, we suppose that D, M and $v = \mathrm{Tr}(\beta/\sqrt{D})$ are even. So 2 divides g. If u were even, then β would also be even, since v is even. As before, ω would then be the quotient of the integers $\beta/2$ and $M/2$, and this would imply $\mathfrak{a}|\frac{M}{2}$, which contradicts the minimality of M. So u must be odd. But this implies $g = 2$. □

Lemma 2. *The identity* (4) *holds true if M is odd, i.e. one has*

$$G(\omega)/\sqrt{\mathrm{N}(\mathfrak{a})} = \left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{\Delta/\Delta_1}{M/(M,\Delta)}\right)\sqrt{\mathrm{sgn}(\Delta_1)}.$$

Here A is as in the theorem, moreover $\Delta = 4\mathrm{N}(M\omega)$, and Δ_1 is the unique integer such that $\Delta_1 \equiv 1 \bmod 4$ and $|\Delta_1| = \gcd(M, \Delta)$.

Proof. On summing over a set of representatives μ for O/MO instead of $O/\mathfrak{a}$ and setting $\mu = x + y\gamma$, we can write

$$G(\omega)M^2/\mathrm{N}(\mathfrak{a}) = \sum_{x,y \bmod M} e_M(ax^2 + bxy + cy^2),$$

where we use $e_M(*) = e^{2\pi i(*)/M}$. Since M is odd the quadratic form $f = ax^2 + bxy + cy^2$ is equivalent to a form $Ax^2 + By^2$ modulo $\mathrm{GL}(2, \mathbb{Z}/M\mathbb{Z})$. Usually this appears in the literature for the case of M being an odd prime power. However, by applying the Chinese remainder theorem, this is true for arbitrary odd M. Here AB is congruent to $-\Delta l^2$ modulo M for an integer l coprime to M. Since by Lemma 1 the form f is primitive modulo M, we can assume that M and A are coprime. (In fact, this can obviously be assumed if M is a prime power. Again, by the Chinese remainder theorem we can assume it in general). Note that then $\gcd(M, B) = \gcd(M, \Delta) = |\Delta_1|$. We therefore obtain

$$G(\omega)M^2/\mathrm{N}(\mathfrak{a}) = |\Delta_1| \sum_{x \bmod M} e_M(Ax^2) \sum_{x \bmod M'} e'_M(B'y^2),$$

where we set $M' = M/|\Delta_1|$ and $B' = B/|\Delta_1|$. Inserting here the identity (2) we obtain

$$G(\omega)/v = \left(\tfrac{A}{M}\right)\sqrt{\left(\tfrac{-4}{M}\right)}\left(\tfrac{B'}{M'}\right)\sqrt{\left(\tfrac{-4}{M'}\right)},$$

where $v = \mathrm{N}(\mathfrak{a})|\Delta_1|\sqrt{MM'}/M^2$. Note that $v = \sqrt{\mathrm{N}(\mathfrak{a})}$. For verifying this it is enough to show $M^2 = \mathrm{N}(\mathfrak{a})\gcd(M, \Delta)$. Indeed, we have

$$\begin{aligned}\mathrm{N}(\mathfrak{a})\gcd(M,\Delta) &= \gcd\left(\mathrm{N}(\mathfrak{a})M, \mathrm{N}(\mathfrak{a})\Delta\right) = \gcd\left(\mathrm{N}(\mathfrak{a})M, \mathrm{N}(\mathfrak{a})\mathrm{N}(M\omega)\right)\\ &= \gcd\left(\mathrm{N}(\mathfrak{a})M, M^2\mathrm{N}(\mathfrak{b})\right) = M\gcd\left(\mathrm{N}(\mathfrak{a}), M\right) = M^2,\end{aligned}$$

where for the last equation we used that $M\mathbb{Z} = \mathfrak{a} \cap \mathbb{Z}$ contains $\mathrm{N}(\mathfrak{a})$. Writing $\left(\frac{A}{M}\right) = \left(\frac{\Delta_1}{A}\right)\left(\frac{A}{M'}\right)$ and $\left(\frac{-4}{M}\right) = \left(\frac{-4}{M'}\right)\left(\frac{-4}{|\Delta_1|}\right)$ the right hand side of the last equation for $G(\omega)$ becomes

$$\left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{AB'}{M'}\right)\sqrt{\left(\tfrac{-4}{M'}\right)\left(\tfrac{-4}{|\Delta_1|}\right)}\sqrt{\left(\tfrac{-4}{M'}\right)}.$$

Since $\left(\frac{AB'}{M'}\right) = \left(\frac{-\Delta/|\Delta_1|}{M'}\right)$ the lemma becomes now obvious. □

Lemma 3. *The identity* (4) *holds true if M is a power of* 2. *In this case the possible values of $G(\omega)$ are given by the following table:*

Assumptions		$G(\omega)/\sqrt{\mathrm{N}(\mathfrak{a}\gcd(\mathfrak{a},2))}$
D or a odd	$\Delta_2 \mid M$	$\left(\frac{\Delta_2}{A}\right)\left(\frac{\Delta/\Delta_2}{M/\lvert\Delta_2\rvert}\right)\sqrt{\mathrm{sgn}(\Delta_2)}$
	$4 \mid M$ *and* $4M \mid \Delta$	$\left(\frac{A}{2M}\right)e^{2\pi i A/8}$
	$M = 2$ *or* $2M \mid\mid \Delta$	0
D and a even		$\left(\frac{\Delta/4}{2M}\right)$

Here A is as in the theorem, $a = \mathrm{Tr}(M\omega/\sqrt{D})$, and we use $\Delta = 4\mathrm{N}(M\omega)$. Finally, Δ_2 is the integer such that $|\Delta_2|$ is the exact 2-power dividing Δ and $\Delta/\Delta_2 \equiv 1 \bmod 4$.

Remark. Note that $\Delta/4 = \mathrm{N}(M\omega)$ is odd if D and a are even. Indeed, if D is even (so that $\mathfrak{a}$ is a power of the single prime ideal above 2), then by the very definition of M the norm $\mathrm{N}(M\omega)$ is either odd or exactly divisible by 2, and as discriminant of the integral form $\mathrm{Tr}(M\omega\mu^2/2\sqrt{D})$ (see Lemma 1) it is a square modulo 4.

Proof of Lemma 3. To compute $G(\omega)$ we proceed as in Lemma 2, i.e. we sum over a set of representatives μ for O/MO instead of $O/\mathfrak{a}$ and set $\mu = x + y\gamma$. We thus have

$$G(\omega) \approx \sum_{x,y \bmod M} e_M(ax^2 + bxy + cy^2). \tag{10}$$

Here, a, b, c are the integers as in the proof of Lemma 1. As in the proof of the preceding lemma we use $e_M(*) = e^{\frac{2\pi i(*)}{M}}$. Moreover, for two complex numbers w and z we write $w \approx z$ to indicate that $w = rz$ for some positive real number r. By [Cas78, §8, section 8.4, lemma 4.1] a binary integral quadratic form whose content is odd is equivalent modulo $\mathrm{GL}(2,\mathbb{Z}_2)$ to a diagonal form, to xy or to x^2+xy+y^2 accordingly as its discriminant is even, equals 1 modulo 8, or equals 5 modulo 8. Recall from Lemma 1 that the gcd of the contents of the form $f(x,y) = ax^2 + bxy + cy^2$ and M is 1 if D or a is odd, and equals 2 otherwise. Recall also that the discriminant of f equals $4\mathrm{N}(\beta)$, where we use $\beta = M\omega$. We therefore find

$$f \sim \begin{cases} Ax^2 + By^2 & \text{if } D \text{ or } a \text{ is odd} \\ 2xy & \text{if } D \text{ and } a \text{ are even, and } \mathrm{N}(\beta) \equiv 1 \bmod 8 \\ 2(x^2+xy+y^2) & \text{if } D \text{ and } a \text{ are even, and } \mathrm{N}(\beta) \equiv 5 \bmod 8, \end{cases}$$

where $\sim$ indicates to be equivalent modulo $\mathrm{GL}(2, \mathbb{Z}/2^t\mathbb{Z})$ for a sufficiently big t (in fact, $2^t = 4M$ suffices for the following computations). Here we used that, for even D and a, the form $f/2$ is integral (see Lemma 1) and that $\mathrm{N}(\beta)$ is odd (see the remark following the lemma). We now calculate $G(\omega)$ following the above three cases.

Case 1: $f \sim Ax^2 + By^2$. We can assume that A is odd (since f is primitive modulo 2 in this case). Let $\delta = \gcd(M, B)$ and set $B' = B/\delta$ and $M' = M/\delta$. We can then write

$$G(\omega) \approx \sum_{x \bmod M} e_M(Ax^2) \sum_{y \bmod M'} e_{M'}(B'y^2).$$

Using equation (2) we find, for $M, M' \geq 4$ the identity

$$G(\omega) \approx \left(\tfrac{A}{2M}\right)\left(\tfrac{B'}{2M'}\right) e_8\big(A + B'\big) = \left(\tfrac{A}{\delta}\right)\left(\tfrac{\Delta/4\delta}{2M'}\right) e_8\big(A(1 - \Delta/4\delta)\big).$$

Here, for the second identity we write $M = \delta M'$ in the left hand side and use that $AB' \equiv -l^2\Delta/4\delta \bmod 2M'$ for an odd l. We note that $M' \geq 4$ implies $4\delta \mid M$ and hence $|\Delta_2| = \gcd(M, -4AB) = 4\delta$. In particular, we see $\Delta_2 \mid M$. Vice versa, $\Delta_2 \mid M$ implies that $M, M' \geq 4$. We thus have to verify that the right hand side of our last

formula equals the formula given in the first row of the table. Indeed, this follows from $|\Delta_2| = 4\delta$ distinguishing the cases $\Delta_2 > 0$ (and hence $\Delta/4\delta \equiv 1 \bmod 4$) and $\Delta_2 < 0$ (and hence $\Delta/4\delta \equiv 3 \bmod 4$) and using that, for any integer a, the symbol $\left(\frac{a}{2}\right) e_8(a)$ depends only on a modulo 4.

If $M \geq 4$ but $M' = 1$, then

$$G(\omega) \approx \left(\tfrac{A}{2M}\right) e_8(A).$$

Finally, if M or M' equals 2 then $G(\omega) = 0$. Note that $M' = 1$ and $M' = 2$ are equivalent to $4M|\Delta$ and $2M||\Delta$, respectively, as stated in the table.

Case 2: $f \sim 2xy$. Here $\Delta/4 \equiv 1 \bmod 8$ and we have

$$G(\omega) \approx \sum_{x,y \bmod M/2} e_{M/2}(xy) \approx 1,$$

as claimed.

Case 3: $f \sim 2(x^2 + xy + y^2)$. In this case we have $\Delta/4 \equiv -3 \bmod 8$, and we find

$$G(\omega) \approx \sum_{x,y \bmod M/2} e_{M/2}(x^2 + xy + y^2) \approx \left(\tfrac{-3}{2M}\right).$$

For proving the second identity write $(x, y) = r + u$, where r runs through a set of representatives for $Z^2/N\mathbb{Z}^2$, and where u runs through a set of representatives for $N\mathbb{Z}^2/M/2\mathbb{Z}^2$. Here N is the smallest positive integer whose square is divisible by $M/2$. By some obvious calculations the sum in the above formula for $G(\omega)$ is then reduced to the same sum but with $M/2$ replaced by 2 or 4, which can be immediately computed.

It remains to prove that $|G(\omega)|^2$ equals $\mathrm{N}\big(\mathfrak{a}\gcd(2, \mathfrak{a})\big)$ (unless it is 0). This can either be easily proved directly by writing $|G(\omega)|^2 = G(\omega)G(-\omega)$ and doing some obvious transformations in the double sum (or by going again through the above calculations and using equalities instead of $\approx$). For the details of the direct proof see [BS09, Lemma]. This proves the lemma. □

For deducing the general formula (4) from the preceding two Lemmas we use

Lemma 4. *Write the denominator $\mathfrak{a}$ of ω as $\mathfrak{a} = \mathfrak{a}_1\,\mathfrak{a}_2$ with relatively prime integral ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$. Choose elements α_i in $\mathfrak{a}_i$ such that the ideals $\alpha_i/\mathfrak{a}_i$ are relatively prime to $\mathfrak{a}$. Then one has*

$$G(\omega) = G(\omega\alpha_1^2)\, G(\omega\alpha_2^2)$$

(Note that $\omega\alpha_1^2$ and $\omega\alpha_2^2$ have denominators $\mathfrak{a}_2$ and $\mathfrak{a}_1$, respectively).

Remark. Note that numbers α_i as in the lemma always exist. In fact, we can e.g. choose any prime ideal $\mathfrak{p}_i$ amongst the infinitely many prime ideals in the ideal class of $\mathfrak{a}_i^{-1}$ which does not divide $\mathfrak{a}$ and set $\alpha_i = \mathfrak{a}_i\mathfrak{p}_i$.

Proof of Lemma 4. This follows from [Hec70, eq. (169)]. □

Proof of the Theorem. Let us denote the expression on the right hand side of equation (4) as $F(\omega)$, and set

$$B(\omega) = G(\omega)/\sqrt{\mathrm{N}\big(\mathfrak{a}\,\gcd(2, \mathfrak{a})\big)}.$$

By Lemma 2 and Lemma 3 we know that $B(\omega) = F(\omega)$ if the denominator of ω is either odd or else a product of even prime ideals. It follows from Lemma 4 that

$$B(\omega) = B(\omega\alpha_1^2)B(\omega\alpha_2^2)$$

whenever we decompose the denominator $\mathfrak{a}$ of ω as $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ with relatively prime ideals $\mathfrak{a}_i$, and choose numbers α_i in $\mathfrak{a}_i$ such that the $\alpha_i\mathfrak{a}_i^{-1}$ are prime to $\mathfrak{a}$. If we can prove that

$$F(\omega) = F(\omega\alpha_1^2)F(\omega\alpha_2^2), \tag{11}$$

holds true for any such decomposition of $\mathfrak{a}$ with an odd $\mathfrak{a}_1$ and an $\mathfrak{a}_2$ which is a product of even prime ideals, it is clear that the claimed formula (4) follows then for arbitrary $\mathfrak{a}$.

To prove equation (11) (for odd $\mathfrak{a}_1$ and a product of even prime ideals $\mathfrak{a}_2$) we use M, N, β, Δ_1 and A as defined in the theorem. We use M_e, N_e, β_e, Δ_e and A_e for the corresponding quantities associated to $\omega_e := \omega\alpha_e^2$, where $\alpha_e = \alpha_1$ (so that the denominator of ω_e contains only even primes). Similarly we use M_o, N_o $(= M_o)$ etc. for the corresponding quantities associated to $\omega_o := \omega\alpha_o^2$, where $\alpha_o = \alpha_2$. If there are two integers Δ_1 and Δ_e satisfying these conditions, respectively, we choose the positive ones. We also set $F = F(\omega)$ and $F_i = F(\omega\alpha_i^2)$ $(i = e, o)$. Finally, we can also assume that the ideals $\alpha_e/\mathfrak{a}_1$ and $\alpha_o/\mathfrak{a}_2$ are relatively prime to $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$ and relatively prime to the norm of each other. In particular, α_e is then relatively prime to 2, and the norms of $\alpha_e/\mathfrak{a}_1$ and $\alpha_o/\mathfrak{a}_2$ are relatively prime to $\mathrm{N}(\mathfrak{a})$ and $\mathrm{N}(\mathfrak{b})$.

These quantities are correlated as follows:

$$M = M_eM_o,\ N = N_eM_o, \tag{12}$$

$$\mathrm{N}(\beta_e)\mathrm{N}(\beta) = \big(N_eN\mathrm{N}(\mathfrak{b})\mathrm{N}(\alpha_e/\mathfrak{a}_1)/\mathrm{N}(\mathfrak{a}_2)\big)^2, \tag{13}$$

$$\mathrm{N}(\beta_o)\mathrm{N}(\beta) = \big(N_oN\mathrm{N}(\mathfrak{b})\mathrm{N}(\alpha_o/\mathfrak{a}_2)/\mathrm{N}(\mathfrak{a}_1)\big)^2, \tag{14}$$

$$\Delta_1 = \pm\Delta_e\Delta_o, \tag{15}$$

$$4\mathrm{N}(\beta)/\Delta_1 = t \cdot 4\mathrm{N}(\beta_e)/\Delta_e \text{ with an odd } t. \tag{16}$$

Moreover, note that

(i) M_e is a power of 2 and M_o is odd.
(ii) If D is even, then $a := \mathrm{Tr}(M\omega/\sqrt{D})$ and $a_e := \mathrm{Tr}(\beta_e/\sqrt{D})$ have the same parity.

The statement (i) and the first identity in equation (12) are obvious. For (ii), assume D is even. If a is even, then by Lemma 1, the quadratic form $Q(\mu) = \mathrm{Tr}(M\omega\mu^2/\sqrt{D})$ is even, hence $Q(\alpha_e)$ and then also $a_e = Q(\alpha_e)/M_o$ is even. Vice versa, if a_e is even, then $Q_e(\mu) := \mathrm{Tr}(M_e\omega\alpha_e^2\mu^2/\sqrt{D})$ is even. Since we have chosen α_e relatively prime to 2 we find a μ_0 such that $\alpha_e\mu_0 \equiv 1 \bmod 2$, and then $M_oQ_e(\mu_0) \equiv a \bmod 2$, hence a is even. The second identity of (12) follows from (ii). equations (13), (14) follow by straightforward calculation. For proving (15), we find by a simple calculation

$$\begin{aligned}\Delta_e\Delta_o &= \pm\gcd\big(M_e, 4\mathrm{N}(\beta_e)\big)\gcd\big(M_o, 4\mathrm{N}(\beta_o)\big)\\ &= \gcd\big(M, 4\mathrm{N}(\beta)\mathrm{N}(\alpha_o)^2/M_e, 4\mathrm{N}(\beta)\mathrm{N}(\alpha_e)^2/M_o, 16\mathrm{N}(\beta)\mathrm{N}(\omega\alpha_e^2\alpha_o^2)\big).\end{aligned}$$

Since we have chosen α_e and α_o such that $\mathrm{N}(\alpha_o)$ and $\mathrm{N}(\alpha_e)$ are relatively prime, the gcd of the last three entries equals $4\mathrm{N}(\beta)$, and we recognize the claimed identity. Finally, from (15) we deduce that (16) holds true with $t = M_o^2/\mathrm{N}(\alpha_e^2)\Delta_o$, which is odd (note that α_e has been chosen relatively prime to 2).

We assume first of all that D or a_e are odd. Then $N_e = M_e$, and, using (12), we also have $N = M$. Note that always $N_o = M_o$.
Case 1: The 2-part of $4\mathrm{N}(\beta_e)$ divides M_e. In this case, by Lemmas 2 and 3, we have

$$F_eF_o = \left(\tfrac{\Delta_e}{A_e}\right)\left(\tfrac{4\mathrm{N}(\beta_e)/\Delta_e}{M_e/|\Delta_e|}\right)\sqrt{\mathrm{sgn}(\Delta_e)}\left(\tfrac{\Delta_o}{A_o}\right)\left(\tfrac{4\mathrm{N}(\beta_o)/\Delta_o}{M_o/|\Delta_o|}\right)\sqrt{\mathrm{sgn}(\Delta_o)}.$$

Since $M_oA_e = Q(\alpha_e)$ is relatively prime to Δ_e we have $\left(\frac{\Delta_e}{M_oA_e}\right) = \left(\frac{\Delta_e}{A}\right)$. By a similar argument we find $\left(\frac{\Delta_o}{M_eA_o}\right) = \left(\frac{\Delta_o}{A}\right)$. We shall show in a moment

$$\Delta_1 = \Delta_e\Delta_o. \tag{17}$$

This implies in particular $\sqrt{\mathrm{sgn}(\Delta_e)}\sqrt{\mathrm{sgn}(\Delta_o)} = (\Delta_e, \Delta_o)_\infty\sqrt{\mathrm{sgn}(\Delta_1)}$, where we use $(\Delta_e, \Delta_o)_\infty$ for the Hilbert symbol at infinity, i.e. it equals -1 if Δ_e, Δ_o are both negative, and equals $+1$ otherwise. Using these identities we find

$$F_eF_o = UV\left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{4\mathrm{N}(\beta)/\Delta_1}{M/|\Delta_1|}\right)\sqrt{\mathrm{sgn}(\Delta_1)},$$

where

$$U = \left(\tfrac{\Delta_e}{M_0}\right)\left(\tfrac{\Delta_o}{M_e}\right)(\Delta_e, \Delta_o)_\infty$$
$$V = \left(\tfrac{4\mathrm{N}(\beta)/\Delta_1\cdot 4\mathrm{N}(\beta_e)/\Delta_e}{M_e/|\Delta_e|}\right)\left(\tfrac{4\mathrm{N}(\beta)/\Delta_1\cdot 4\mathrm{N}(\beta_o)/\Delta_o}{M_o/|\Delta_o|}\right).$$

Using (13), (14), we can write

$$V = \left(\tfrac{\Delta_o}{M_e/|\Delta_e|}\right)\left(\tfrac{\Delta_e}{M_o/|\Delta_o|}\right).$$

We thus find

$$UV = \left(\tfrac{\Delta_e}{|\Delta_o|}\right)\left(\tfrac{\Delta_o}{|\Delta_e|}\right)(\Delta_e, \Delta_o)_\infty.$$

From this identity it is easily checked that $UV = 1$. From (16), we recognize that $4\mathrm{N}(\beta)/\Delta_1$ is odd, so that sum defining F contains only one term, and that the last formula for F_eF_o equals F.

It remains to show (17). From (15) we have $\Delta = s\Delta_e\Delta_o$. Since $\mathrm{N}(\beta_e)/\Delta_e$ and $\mathrm{N}(\beta)/\Delta_1$ are both equal to 1 modulo 4, we have $s\Delta_o \equiv \mathrm{N}(\beta_e)\mathrm{N}(\beta)/\Delta_e^2 \bmod 4$. Since the right hand side is a perfect square by (13) we deduce that $s\Delta_o$ is 1 modulo 4. Since Δ_o is already 1 modulo 4 we conclude $s = 1$.

Case 2: $4|M_e$ and $M_e|\mathrm{N}(\beta_e)$. Here $\Delta_e = M_e$. Moreover, by (15) and (16) $4|M$ and $4\mathrm{N}(\beta)/\Delta$. The sum defining F contains hence two terms and Δ_1 is positive.

Again by Lemmas 2 and 3, we have

$$F_eF_o = \left(\tfrac{A_e}{2M_e}\right)e^{2\pi iA_e/8}\left(\tfrac{\Delta_o}{A_o}\right)\left(\tfrac{4\mathrm{N}(\beta_o)/\Delta_o}{M_o/|\Delta_o|}\right)\sqrt{\mathrm{sgn}(\Delta_o)}.$$

As in Case 1 we have $\left(\frac{M_oA_e}{2M_e}\right) = \left(\frac{A}{2M_e}\right)$ and $\left(\frac{\Delta_o}{M_eA_o}\right) = \left(\frac{\Delta_o}{A}\right)$. Writing $\Delta_e\Delta_0 = s\Delta_1$, where s is the sign of Δ_o, we find by a straightforward calculation (using (14))

$$F_eF_o = \left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{4\mathrm{N}(\beta)/\Delta_1}{M/\Delta_1}\right)W,$$

where

$$W = \left(\tfrac{4s}{AM/\Delta_1}\right)\sqrt{s}\cdot\left(\tfrac{A_e}{2}\right)e^{2\pi iA_e/8}.$$

If $A = Q(\mu)$, then choose a ν such that $\alpha_e\nu \equiv \mu \bmod 4$, so that $A \equiv M_oQ_e(\nu) \bmod 4$. Since $Q_e(\nu)$ is odd, we can assume that it equals A_e. Hence $A \equiv A_eM_o \bmod 4$. Since Δ_o is 1 modulo 4 we can write $sM/\Delta_1 = M_o/\Delta_o \equiv M_o \bmod 4$. A fortiori $A_e \equiv sAM/\Delta_1 \bmod 4$. The last two factors of W depend only on A_e modulo 4 and become therefore $\left(\frac{sAM/\Delta_1}{2}\right)e^{2\pi isAM/8\Delta_1}$. From this it becomes in turn obvious that $W = \left(\frac{AM/\Delta_1}{2}\right)e^{2\pi iAM/8\Delta_1}$. Inserting this in the last identity for F_eF_o, we obtain

$$F_eF_o = \left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{4\mathrm{N}(\beta)/\Delta_1}{M/\Delta_1}\right)\left(\tfrac{AM/\Delta_1}{2}\right)e^{2\pi i\frac{AM/\Delta_1}{8}},$$

and using $\left(\frac{a}{2}\right)e^{2\pi ia/8} = \left(1 + \left(\frac{-4}{a}\right)i\right)/\sqrt{2}$ for $a = AM/\Delta_1$, we recognize that the right hand side of this identity for F_eF_o equals F as given in the theorem.

Case 3: $M_e = 2$ or $M_e || 2\mathrm{N}(\beta_e)$. Here, by Lemma 3, we have $F_e = 0$. We have to show $F = 0$. If $M_e = 2$, then by (i) and (12) also $2||M$ and hence the sum defining F contains indeed no terms. If $M_e||2\mathrm{N}(\beta_e)$, then $M_e||2\mathrm{N}(\beta)$ (by (16)). But this implies that $4\mathrm{N}(\beta)/\Delta$ is exactly divisible by 2, and hence again the sum defining F contains no terms.

We finally assume that D and a_e are even, so that by (ii) also a is even. Here $N = M/2$ and $N_e = M_e/2$. Also, by the remark following Lemma 3, $4\mathrm{N}(\beta)$ and $4\mathrm{N}(\beta_e)$ are odd. The latter implies $\Delta_e = 1$, and, by (15), then $\Delta_1 = \Delta_o$ (note that we have equality here since both sides are congruent 1 modulo 4). By Lemmas 2, 3, we have

$$F_e F_o = \left(\tfrac{4\mathrm{N}(\beta_e)}{2M_e}\right)\left(\tfrac{\Delta_o}{A_o}\right)\left(\tfrac{4\mathrm{N}(\beta_o)/\Delta_o}{M_o/|\Delta_o|}\right)\sqrt{\mathrm{sgn}(\Delta_o)}$$

Since $N_e A_o = Q(\alpha_o)/2$ is represented by the form $Q(\mu)/2$ and relatively prime to Δ_o, we have $\left(\frac{\Delta_o}{N_e A_o}\right) = \left(\frac{\Delta_o}{A}\right)$. Hence, writing Δ_1 for Δ_0, we obtain

$$F_e F_o = \left(\tfrac{\Delta_1}{A}\right)\left(\tfrac{4\mathrm{N}(\beta_e)\Delta_1}{N_e}\right)\left(\tfrac{4\mathrm{N}(\beta_o)/\Delta_1}{M_o/|\Delta_1|}\right)\sqrt{\mathrm{sgn}(\Delta_1)}$$

For verifying that this equals F we need to show that the two Legendre symbols in the middle equal $\left(\frac{4\mathrm{N}(\beta)/\Delta_1}{N/|\Delta_1|}\right)$, i.e. that

$$\left(\tfrac{4\mathrm{N}(\beta_e)\Delta_1 \cdot 4\mathrm{N}(\beta)/\Delta_1}{N_e}\right)\left(\tfrac{4\mathrm{N}(\beta_o)/\Delta_1 \cdot 4\mathrm{N}(\beta)/\Delta_1}{M_o/|\Delta_1|}\right) = 1.$$

But this follows immediately from equations (13) and (14). This concludes the proof of the theorem. □

We finally prove the supplement and the corollary of the theorem. For this we need the following lemma.

Lemma 5. *If the discriminant D of K is congruent to 4 modulo 8, then all odd integers in K have norm congruent to $+1$ modulo 4. Otherwise, there exists integers α in K with $\mathrm{N}(\alpha) \equiv -1 \bmod 4$. For every such integer the quadratic form $\mathrm{Tr}(\alpha\mu^2/\sqrt{D})$, viewed as quadratic form on the residue class ring $O/(4)$, is $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$-equivalent to $n(\alpha)(x^2 + y^2)$ or $n(\alpha)x^2 + 2(x + y)y$ for a suitable $n(\alpha)$ in $\{\pm 1\}$. There is one and only one Dirichlet character χ modulo 4 on O such that $\chi(\alpha) = n(\alpha)$ for all α with $\mathrm{N}(\alpha) \equiv -1 \bmod 4$.*

Proof. If $D \equiv 4 \bmod 8$, then, for every integer $\alpha = u + v\frac{\sqrt{D}}{2}$ in K, we have $\mathrm{N}(\alpha) = u^2 - \frac{D}{4}v^2 \equiv u^2 + v^2 \bmod 4$. If α is odd, then u and v have different parity, and hence $\mathrm{N}(\alpha) \equiv +1 \bmod 4$.

Assume for the rest of the proof that $D \not\equiv 4 \bmod 8$. The elements $1 + \frac{\sqrt{D}}{2}$ (if $D \equiv 0 \bmod 8$) and $2 + \sqrt{D}$ (if $D \equiv 1 \bmod 4$) have norm modulo 4 equal to -1.

Let α be an integer such that $\mathrm{N}(\alpha) \equiv -1 \bmod 4$, and write $\mathrm{Tr}\big(\alpha(x+y\gamma)^2/\sqrt{D}\big) = ax^2 + bxy + cy^2 =: f$. From $b^2 - 4ac = 4N(\alpha)$ we deduce that b is even and hence $(b/2)^2 - ac \equiv -1 \bmod 4$. If b is divisible by 4, then $ac \equiv 1 \bmod 4$ and $f \equiv a(x^2 + y^2) \bmod 4$. If $b/2$ is odd, then $ac \equiv 2 \bmod 4$, and hence $f \equiv ax^2 + 2(x + y)y \bmod 4$ (if a is odd) or $f \equiv 2(x + y)y + cy^2 \bmod 4$ (if c is odd).

We determine the structure of the group $\big(O/(4)\big)^*$ of units in $O/(4)$. Note that its order is 8, 4 and 12 accordingly as D equals 0, 1 or 5 modulo 8. The map $x \mapsto \gamma$ induces an isomorphism $A[x]/(g) \simeq O/(4)$, where $A = \mathbb{Z}/4\mathbb{Z}$ and (i) $g = x^2 + 2$ (if $D \equiv 0 \bmod 8$), (ii) $g = x^2 - x$ (if $D \equiv 1 \bmod 16$), (iii) $g = x^2 - x + 2$ (if $D \equiv 9 \bmod 16$), (iv) $g = x^2 - x - 1$ (if $D \equiv 5 \bmod 16$), and (v) $g = x^2 - x + 1$ (if $D \equiv 13 \bmod 9$). The map $x \mapsto x + 2$ defines isomorphisms between the rings with g as in (ii) and (iii) and with g as in (iv) and (v), respectively. One verifies that $\big(A[x]/(g)\big)^* = \langle -1\rangle \times \langle z\rangle$, where $z = 1 + x$ for $g = x^2 + 2$ and $g = x^2 - x - 1$, and

where $z = 1 + 2x$ for $g = x^2 - x$. Indeed, if for example $g = x^2 - x - 1$, then the order of the group of units equals 12, and we have to verify that z has order 6 and $z^3 \neq -1$. But $(1+x)^2 = 2 + 3x$ and $(1+x)^3 = 2x + 3$. The other cases can be treated similarly.

Thus we find in any case that $\big(O/(4)\big)^* = \langle[-1]\rangle \times \langle[\delta]\rangle$ for a suitable δ. Here $[\alpha]$, for any integer α, denotes the residue class of α. Since O contains elements with norm equal to -1 modulo 4 we know that δ is such an element. By replacing δ by $-\delta$ if necessary, we may assume that $n(\delta) = +1$. Let χ be the character on $\big(O/(4)\big)^*$ which maps $[-1]$ to -1 and $[\delta]$ to $+1$. If α is an odd integer, we can find rational integers s and $t \geq 0$ such that $\alpha \equiv (-1)^s \delta^t \bmod 4$. Then $\mathrm{Tr}\big(\alpha\mu^2/\sqrt{D}\big) \equiv (-1)^s \mathrm{Tr}(\delta^t\mu^2/\sqrt{D}) \bmod 4$. If $\mathrm{N}(\alpha) \equiv -1 \bmod 4$, then t is odd, say, $t = 1 + 2k$, and hence $(-1)^s\mathrm{Tr}(\delta^t\mu^2/\sqrt{D}) = (-1)^s\mathrm{Tr}(\delta(\delta^k\mu)^2/\sqrt{D})$ is equivalent modulo 4 to $(-1)^s\mathrm{Tr}(\delta\mu^2/\sqrt{D})$, and hence $n(\alpha) = (-1)^s = \chi(\alpha)$.

Since $\chi(\pm\delta) = n(\pm\delta)$ and $\chi(-1) = \overline{\chi}(\delta)\chi(-\delta)$ the property $\chi(\alpha) = n(\alpha)$ characterizes χ uniquely. This proves the lemma. □

Proof of the supplement to the theorem. It is not hard to prove that $G(\beta/\alpha) = \left(\frac{\beta}{\alpha}\right) G(1/\alpha)$ [Hec70, Satz 155]. It suffices therefore to prove Formula (5) for $\beta = 1$. For an odd α the equation (4) reads

$$G(1/\alpha)/\sqrt{|\mathrm{N}(\alpha)|} = \left(\tfrac{\varepsilon \mathrm{N}(M/\alpha)}{A}\right)\left(\tfrac{4\varepsilon}{M/|\mathrm{N}(M/\alpha)|}\right)\sqrt{\varepsilon n}, \tag{18}$$

where $\varepsilon = \varepsilon_\alpha$ and $n = \mathrm{sign}\,\big(\mathrm{N}(\alpha)\big)$, where M is the smallest positive integer such that M/α is integral, and where A denotes any number relatively prime to M and represented by $Q(\mu) = \mathrm{Tr}(M\mu^2/\alpha\sqrt{D})$. In particular, $Q(\mu)$ is equivalent to $[A, B, C]$ for suitable B, C. Since $B^2 - 4AC = 4\mathrm{N}(M/\alpha)$ (cf. Lemma 1) we have $\left(\frac{4\mathrm{N}(M/\alpha)}{|A|}\right) = 1$, and then $\left(\frac{4\mathrm{N}(M/\alpha)}{A}\right) = \sigma$, where $\sigma = -1$ if Q is negative definite and where $\sigma = +1$ otherwise. Using the Hilbert symbol for the real numbers we find $\sigma = \big(A, N(\alpha)\big)_\infty$. If $\varepsilon = +1$ we now recognize the claimed formula.

If $\varepsilon = -1$ then the content of Q is odd (otherwise the discriminant $\mathrm{N}(M/\alpha)$ of $Q/2$ would be congruent to 1 modulo 4). We can therefore assume that A is odd, and then the first factor of the right hand side of (18) becomes $\left(\frac{-4}{A}\right)\sigma$, and the right hand side can be written in the form

$$\left(\tfrac{-4}{A}\right)\left(\tfrac{-4}{M/|\mathrm{N}(M/\alpha)|}\right)\sigma\sqrt{-n} = \left(\tfrac{-4}{A\mathrm{N}(\alpha)/M}\right)\sigma n\sqrt{-n}.$$

If $A = \mathrm{Tr}(M\mu_0^2/\alpha\sqrt{D})$, then $\left(\frac{-4}{A\mathrm{N}(\alpha)/M}\right) = -\left(\frac{-4}{a}\right)$, where $a = \mathrm{Tr}(\alpha{\mu'_0}^2/\sqrt{D})$. We now recognize the claimed formula provided $\left(\frac{-4}{a}\right) = \chi_-(\alpha)$. But from Lemma 5 we know that $D \not\equiv 4 \bmod 8$ and, in the notations of the lemma, that $n(\alpha) = \left(\frac{-4}{a}\right)$, which equals $\chi_-(\alpha)$. This proves the supplement. □

Proof of the corollary to the theorem. Inserting (5) into (6) we find

$$\begin{aligned}\left(\tfrac{\alpha}{\beta}\right)\left(\tfrac{\beta}{\alpha}\right) &= \frac{\chi_{\varepsilon_{\alpha\beta}}(\alpha\beta)}{\chi_{\varepsilon_\alpha}(\alpha)\chi_{\varepsilon_\beta}(\beta)}\,\frac{\big(A_{\alpha\beta}, \mathrm{N}(\alpha\beta)\big)_\infty}{\big(A_\alpha, \mathrm{N}(\alpha)\big)_\infty\big(A_\beta, \mathrm{N}(\beta)\big)_\infty} \\ &\times \frac{\big(\varepsilon_{\alpha\beta}, -\mathrm{N}(\alpha\beta)\big)_\infty}{\big(\varepsilon_\alpha, -\mathrm{N}(\alpha)\big)_\infty\big(\varepsilon_\beta, -\mathrm{N}(\beta)\big)_\infty}\,\frac{\sqrt{\varepsilon_{\alpha\beta}\mathrm{N}(\alpha\beta)}}{\sqrt{\varepsilon_\alpha\mathrm{N}(\alpha)}\sqrt{\varepsilon_\beta\mathrm{N}(\beta)}},\end{aligned} \tag{19}$$

where A_α, A_β etc. denotes any nonzero number represented by $\mathrm{Tr}\big(\alpha\mu^2/\sqrt{D}\big)$ etc.. Since $\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta$, and hence $\chi_{\varepsilon_{\alpha\beta}} = \chi_{\varepsilon_\alpha}\chi_{\varepsilon_\beta}$, the first factor on the right of (19) reduces to $\chi_{\varepsilon_\alpha}(\beta)\chi_{\varepsilon_\beta}(\alpha)$.

Since the Hilbert symbol is bilinear the third factor on the right hand side of (19) can be reduced to $\big(\varepsilon_\alpha, \mathrm{N}(\alpha)\big)_\infty\big(\varepsilon_\beta, \mathrm{N}(\beta)\big)_\infty$ (where one uses $\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta$). For

two nonzero real numbers a and b one has $\sqrt{ab}/\sqrt{a}\sqrt{b} = (a,b)_\infty$. From this we see that the fourth factor in (19) combined with the third factor becomes $\big(\varepsilon_\alpha, \varepsilon_\beta\big)_\infty \big(\mathrm{N}(\alpha), \mathrm{N}(\beta)\big)_\infty$. This proves already the claimed formula (7) if K is a complex quadratic field since then the norms of elements in K are positive. Suppose from now on that K is real. Since the Hilbert symbol is bilinear we can write

$$\big(\mathrm{N}(\alpha), \mathrm{N}(\beta)\big)_\infty = (\alpha, \beta')_\infty (\alpha', \beta)_\infty \prod_\sigma \big(\sigma(\alpha), \sigma(\beta)\big)_\infty.$$

For proving the claimed reciprocity formula (7), it remains to verify the identity

$$\frac{\big(A_{\alpha\beta}, \mathrm{N}(\alpha\beta)\big)_\infty}{\big(A_\alpha, \mathrm{N}(\alpha)\big)_\infty \big(A_\beta, \mathrm{N}(\beta)\big)_\infty} = (\alpha, \beta')_\infty (\alpha', \beta)_\infty.$$

The symbol $\big(A_\alpha, \mathrm{N}(\alpha)\big)_\infty$ equals -1 if and only if $\alpha\alpha' < 0$ and $\mathrm{Tr}\big(\alpha/\sqrt{D}\big) = (\alpha - \alpha')/\sqrt{D} < 0$. Thus, $\big(A_\alpha, \mathrm{N}(\alpha)\big)_\infty = -1$ if and only if $\alpha < 0 < \alpha'$, i.e. we have $\big(A_\alpha, \mathrm{N}(\alpha)\big)_\infty = \big(\alpha, -\alpha'\big)_\infty$. Applying this formula also to the other two Hilbert symbols on the left of the last identity, it becomes

$$\frac{\big(\alpha\beta, -\alpha'\beta'\big)_\infty}{\big(\alpha, -\alpha'\big)_\infty \big(\beta, -\beta'\big)_\infty} = (\alpha, \beta')_\infty (\alpha', \beta)_\infty.$$

But this identity holds obviously true since the Hilbert symbol is bilinear. This proves the corollary. □

References

[BS09] Hatice Boylan and Nils-Peter Skoruppa. A quick proof of reciprocity for Hecke Gauss sums. preprint, 2009.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[Cau40] Augustin-Louis Cauchy. Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des equationes binômes. *C. R. Acad. Sci. Paris*, 10:560–572, 1840.

[Dir35] Johann Peter Gustav Lejeune Dirichlet. Ueber eine neue anwendung bestimmter integrale auf die summation endlicher oder unendlicher reihen. *Abh. K. Preussischen Akad. Wiss.*, 21:391–407, 1835.

[Dir40] Johann Peter Gustav Lejeune Dirichlet. Recherches sur diverses applications de l'analyse infinitśimale à la théorie des nombres. *J. Reine Angew. Math.*, 21:134–155, 1840.

[Gau11] Carl-Friedrich Gauss. Summatio quarundam serierum singularium. *Com soc. rec. sci. Göttingensis rec.*, 1, 1811.

[Has65] Helmut Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz*. Physica-Verlag, Würzburg, 1965.

[Hec70] Erich Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen*. Chelsea Publishing Co., Bronx, N.Y., 1970. Second edition of the 1923 original, with an index.

[Hec83] Erich Hecke. *Mathematische Werke*. Vandenhoeck & Ruprecht, Göttingen, third edition, 1983. With introductory material by B. Schoeneberg, C. L. Siegel and J. Nielsen.

[Ish98] Hidenori Ishii. Functional equations and the law of quadratic reciprocity. *Mem. Inst. Sci. Eng., Ritsumeikan Univ.*, 57:1–3, 1998.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[S+09] W. A. Stein et al. *Sage Mathematics Software (Version 3.3)*. The Sage Group, 2009. `http://www.sagemath.org`.

[SZ89] Nils-Peter Skoruppa and Don Zagier. A trace formula for Jacobi forms. *J. Reine Angew. Math.*, 393:168–198, 1989.

Fachbereich Mathematik, Universität Siegen, 57072 Siegen, Germany
and

Matematik Bölümü, Bilkent Üniversitesi, Ankara, Turkey
E-mail address: hatice.boylan@uni-siegen.de

Fachbereich Mathematik, Universität Siegen, 57072 Siegen, Germany
E-mail address: nils.skoruppa@uni-siegen.de