A Quick Proof of Reciprocity for Hecke Gauss Sums

Hatice Boylan* and Nils-Peter Skoruppa

Abstract

In this note we present a short and elementary proof of Hecke's reciprocity law for Hecke-Gauss sums of number fields.

In Chapter VIII of his book [Hec70], Hecke introduced and studied certain Gauss sums associated to arbitrary number fields. In particular, he discovered a reciprocity law for these sums [Hec70, Satz 163, p. 240], which he proved by analyzing the values of suitable theta functions in the cusps. The purpose of the present note is to give a short and elementary proof of Hecke's reciprocity law. Our proof is based on Milgram's formula [MH73, p. 127]

$$\frac{1}{\sqrt{L^\sharp/L}} \sum_{x \in L^\sharp/L} \mathbf{e}\big(B(x,x)/2\big) = \mathbf{e}(s/8), \tag{1}$$

where (L, B) is an even integral lattice (i.e. L is a free $\mathbb{Z}$-module of finite rank and B a symmetric non-degenerate integer valued bilinear form on L such that $B(x,x)$ is even for all x in L), $L^\sharp$ denotes the dual lattice $\{y \in L : B(y, L) \subseteq \mathbb{Z}\}$, s is the signature of L, and $\mathbf{e}(x) = \exp(2\pi i x)$ as usual.

Hecke's Gauss sum was defined by the formula

$$C(\omega) = \sum_{\mu \bmod \mathfrak{a}} \mathbf{e}\left(\mathrm{tr}(\mu^2\omega)\right)$$

where K is an arbitrary number field and ω a non-zero element of K. Here N and tr denote the (absolute) norm and the trace of K and $\mathfrak{a}$ denotes the denominator of $\omega\mathfrak{d}$, where $\mathfrak{d}$ is the different of K. The sum is to be taken

*During the preparation of the paper the first author was supported by the Scientific and Technological Research Council of Turkey TÜBİTAK

Key words and phrases. Gauss and Kloosterman sums; generalizations

AMS 2000 subject classifications. 11L05

over a complete set representatives for the ring O of integers of K modulo $\mathfrak{a}$. (Recall that the denominator of $\omega\mathfrak{d}$ is the unique integral ideal $\mathfrak{a}$ such that $\omega\mathfrak{d} = \mathfrak{b}/\mathfrak{a}$ with an integral ideal $\mathfrak{b}$ relatively prime to $\mathfrak{a}$.) It is easily checked that the terms of the sum $C(\omega)$ depend only on the residue class $\mu + \mathfrak{a}$.

We state Hecke's reciprocity law in a renormalized form that is somewhat clearer than the original formulation. We begin with the following lemma whose short proof will be given at the end of the paper.

Lemma. *For a non-zero ω of K, the number $C(\omega)$ is non-zero if and only if the homomorphism*

$$\widetilde{\mathfrak{a}} := \mathfrak{a}/(2,\mathfrak{a}) \to \{\pm 1\}, \quad \mu \mapsto \mathbf{e}\left(\mathrm{tr}(\omega\mu^2)\right) \tag{2}$$

is non-trivial. If this condition is satisfied, then $\mathbf{e}\left(\mathrm{tr}(\omega\mu^2)\right)$ depends only on $\mu \bmod \widetilde{\mathfrak{a}}$, and $|C(\omega)| = \sqrt{\mathrm{N}(\widetilde{\mathfrak{a}})} \cdot [\widetilde{\mathfrak{a}} : \mathfrak{a}]$.

For ω satisfying the condition of the lemma, we set

$$B(\omega) := \frac{1}{\sqrt{\mathrm{N}(\widetilde{\mathfrak{a}})}} \sum_{\mu \bmod \widetilde{\mathfrak{a}}} \mathbf{e}\left(\mathrm{tr}(\mu^2\omega)\right) = \frac{C(\omega)}{|C(\omega)|}\,.$$

(In fact, $B(\omega)$ is an eighth root of unity, with an explicit formula as $\mathbf{e}(s/8)$, where s is the signature of a certain lattice,[1] but this fact does not seem to lead to an alternative proof of the reciprocity and will not be used in the sequel.) We also set

$$\mathrm{Sign}(\omega) = \sum_{\sigma} \mathrm{sign}\,\sigma(\omega),$$

where the sum runs over all real embeddings σ of K. With these notations, Hecke's reciprocity law can be restated as follows.

Theorem. *For any non-zero ω in K such that the homomorphism* (2) *is non-trivial, one has*

$$B(\omega) = \mathbf{e}\left(\mathrm{Sign}(\omega)/8\right)\, B\left(-\gamma^2/4\omega\right),$$

where γ denotes any number in K such that $\gamma\mathfrak{d}$ is integral and relatively prime to the denominator of $(4\omega\mathfrak{d})^{-1}$.

[1] Namely, it is easy to show that $\left(O/\widetilde{\mathfrak{a}}, \mu + \widetilde{\mathfrak{a}} \mapsto \mathrm{tr}(\omega\mu^2) + \mathbb{Z}\right)$ is a non-degenerate finite quadratic module and hence, by a theorem of Wall [Wal63, Theorem (6)], isomorphic to the discriminant module of an even integral lattice. Then $B(\omega) = \mathbf{e}(s/8)$ by Milgram's formula, where s is the signature of this lattice.

Note that under the stated hypothesis $C(\gamma^2/4\omega)$ is different from 0, and hence that $B(\gamma^2/4\omega)$ is defined. In fact, if $\mathrm{tr}(\omega\mu^2)$ is integral for all μ in $\widetilde{\mathfrak{a}}$, then on setting $\mu = \gamma\nu/2\omega$ we see that $\mathrm{tr}(\gamma^2\nu^2/4\omega)$ is integral for all ν in $2\omega\widetilde{\mathfrak{a}}/\gamma = 2\mathfrak{b}/(2,a)\gamma\mathfrak{d} \subseteq 2\mathfrak{b}/(2,\mathfrak{a})$. But the last ideal is the denominator of $\gamma^2/4\omega$, as we will see in the course of the proof.

Proof. Using the obvious identity $\overline{B(\omega)} = B(-\omega)$ we can rewrite the reciprocity formula more symmetrically as

$$B(\omega)B\left(\gamma^2/4\omega\right) = \mathbf{e}\left(\mathrm{Sign}(\omega)/8\right). \tag{3}$$

We assume first of all that the class number of K is 1, i.e. that every ideal of the ring of integers O of K is principal. Let $\mathfrak{d} = \delta O$ and write $\omega\delta = \frac{\beta}{\alpha}$ with relatively prime integers α and β in K. We can then choose $\gamma = 1/\delta$ and the left hand side of (3) becomes

$$\frac{1}{\sqrt{|\mathrm{N}(2\alpha\beta)|}} \sum_{\substack{\mu \bmod \alpha \\ \nu \bmod 2\beta}} \mathbf{e}\left(\mathrm{tr}\left(\mu^2\frac{\beta}{\alpha\delta} + \nu^2\frac{\alpha}{4\beta\delta}\right)\right),$$

provided α is odd (so that 4β is the exact denominator of $\frac{\gamma^2\delta}{4\omega} = \frac{\alpha}{4\beta}$ and $\widetilde{\mathfrak{a}} = \mathfrak{a} = \alpha O$), which we assume for the moment. By writing

$$\mu^2\frac{\beta}{\alpha\delta} + \nu^2\frac{\alpha}{4\beta\delta} \equiv \frac{(2\mu\beta+\nu\alpha)^2}{4\alpha\beta\delta} \bmod \frac{1}{\delta}O$$

and on noticing that $(\mu,\nu) \mapsto 2\mu\beta + \nu\alpha$ defines an isomorphism of $O/\alpha O \times O/2\beta O$ with $O/2\alpha\beta O$, we see that the last double sum becomes

$$\frac{1}{\sqrt{|\mathrm{N}(2\alpha\beta)|}} \sum_{\tau \bmod 2\alpha\beta} \mathbf{e}\left(\mathrm{tr}\left(\frac{\tau^2}{4\alpha\beta\delta}\right)\right).$$

Consider the lattice $L = (O,B)$, where B is the bilinear form on O defined by $B(x,y) = \mathrm{tr}(2\alpha\beta xy/\delta)$. It is easily checked that B is non-degenerate and takes on even integral values. Moreover, for the dual $O^\sharp$ of O with respect to B we find

$$O^\sharp = \{y \in \mathbb{Q} \otimes_{\mathbb{Z}} O : B(y,O) \subseteq \mathbb{Z}\} = (2\alpha\beta)^{-1}O.$$

Using these notations the last sum may be rewritten as

$$\frac{1}{\sqrt{|O^\sharp/O|}} \sum_{x \in O^\sharp/O} \mathbf{e}\left(B(x,x)/2\right).$$

But according to the formula (1) this sum equals $\mathbf{e}(s/8)$, where s denotes the signature of the quadratic form $B(x,x)$ on $\mathbb{R}\otimes_{\mathbb{Z}} O$. It is easily checked that $s = \mathrm{Sign}(\omega)$ which then proves (3).

To prove the general case we rewrite the left hand side of (3) as

$$\frac{1}{\sqrt{\mathrm{N}(\widetilde{\mathfrak{a}}\,\widetilde{\mathfrak{b}}_1)}}\sum_{\substack{\mu \bmod \widetilde{\mathfrak{a}}\\ \nu \bmod \widetilde{\mathfrak{b}}_1}} \mathbf{e}\left(\mathrm{tr}\left(\omega\mu^2+\frac{\gamma^2\nu^2}{4\omega}\right)\right), \tag{4}$$

where we write as before $\omega\mathfrak{d} = \mathfrak{b}\mathfrak{a}^{-1}$ with relatively prime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$, and where $\mathfrak{b}_1$ denotes the denominator of $\gamma^2\mathfrak{d}/4\omega$. Recall that, for any ideal $\mathfrak{c}$, we use $\widetilde{\mathfrak{c}} = \mathfrak{c}/(2,\mathfrak{c})$. Since, by definition, $\gamma\mathfrak{d}$ is integral and relatively prime to the denominator of $(4\omega\mathfrak{d})^{-1}$, we find that the denominator $\mathfrak{b}_1$ of $\gamma^2\mathfrak{d}(4\omega)^{-1} = (\gamma\mathfrak{d})^2(4\omega\mathfrak{d})^{-1}$ equals the denominator of $(4\omega\mathfrak{d})^{-1} = \mathfrak{a}(4\mathfrak{b})^{-1}$. From this and the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, we obtain

$$\mathfrak{b}_1 = \frac{4\mathfrak{b}}{(4,\mathfrak{a})}, \quad \widetilde{\mathfrak{b}}_1 = \frac{2\mathfrak{b}}{(2,\mathfrak{a})}.$$

(The second identity follows from the first one on writing $\widetilde{\mathfrak{b}}_1 = \frac{\mathfrak{b}_1}{(2,\mathfrak{b}_1)} = \frac{4\mathfrak{b}/(4,\mathfrak{a})}{(2,4\mathfrak{b}/(4,\mathfrak{a}))} = \frac{2\mathfrak{b}}{(4,\mathfrak{a},2\mathfrak{b})} = \frac{2\mathfrak{b}}{(2,\mathfrak{a})}$.) We write

$$\omega\mu^2+\frac{\gamma^2\nu^2}{4\omega} \equiv \frac{(2\omega\mu+\gamma\nu)^2}{4\omega} \bmod \mathfrak{d}^{-1}.$$

Now the map $(\mu,\nu)\mapsto 2\omega\mu+\gamma\nu$, $O\times O\to 2\omega O+\gamma O$ induces a map

$$\phi : O/\widetilde{\mathfrak{a}}\times O/\widetilde{\mathfrak{b}}_1 \to \frac{2\omega O+\gamma O}{2\omega\widetilde{\mathfrak{a}}+\gamma\widetilde{\mathfrak{b}}_1}.$$

We claim that ϕ is a isomorphism. Since ϕ is obviously surjective it suffices to prove that

$$\mathrm{N}(\widetilde{\mathfrak{a}}\widetilde{\mathfrak{b}}_1) = \frac{\mathrm{N}(2\omega\widetilde{\mathfrak{a}}+\gamma\widetilde{\mathfrak{b}}_1)}{\mathrm{N}(2\omega O+\gamma O)}.$$

But this follows from:

$$2\omega O+\gamma O = \frac{2\mathfrak{b}}{\mathfrak{a}\mathfrak{d}}+\gamma O = \frac{2\mathfrak{b}+\gamma\mathfrak{a}\mathfrak{d}}{\mathfrak{a}\mathfrak{d}} = \frac{2\mathfrak{b}/(2,\mathfrak{a})+\gamma\widetilde{\mathfrak{a}}\mathfrak{d}}{\widetilde{\mathfrak{a}}\mathfrak{d}} = \frac{1}{\widetilde{\mathfrak{a}}\mathfrak{d}},$$
$$2\omega\widetilde{\mathfrak{a}}+\gamma\widetilde{\mathfrak{b}}_1 = \frac{2\mathfrak{b}}{(2,\mathfrak{a})\mathfrak{d}}+\frac{2\gamma\mathfrak{b}}{(2,\mathfrak{a})} = \frac{\widetilde{\mathfrak{b}}_1}{\mathfrak{d}}(O+\gamma\mathfrak{d}) = \frac{\widetilde{\mathfrak{b}}_1}{\mathfrak{d}}.$$

For the last identity of the first line we use $2\mathfrak{b}/(2,\mathfrak{a})+\gamma\mathfrak{d}\widetilde{\mathfrak{a}} = O$ since $\widetilde{\mathfrak{a}}$ and $\gamma\mathfrak{d}$ are relatively prime to $2\mathfrak{b}/(2,\mathfrak{a}) = \widetilde{\mathfrak{b}}_1$.

Using this isomorphism ϕ we can rewrite (4) as

$$\frac{1}{\sqrt{|M|}} \sum_{x \in M} \mathbf{e}\left(\operatorname{tr}\left(\frac{x^2}{4\omega}\right)\right),$$

where $M = (\widetilde{\mathfrak{a}}\mathfrak{d})^{-1}/\widetilde{\mathfrak{b}}_1\mathfrak{d}^{-1}$. But $M = L^\sharp/L$, where L denotes the even integral lattice $\left(\widetilde{\mathfrak{b}}_1\mathfrak{d}^{-1}, 2\operatorname{tr}\left(\frac{xy}{4\omega}\right)\right)$. Hence, we can again apply formula (1) to deduce that the last sum equals $\mathbf{e}(s/8)$, where s is the signature of the lattice L.

Finally, to compute the signature s we note that a Gram matrix for L is given by $\Delta^t D \Delta$, where D is the diagonal matrix with $\sigma_i(1/2\omega)$ on the diagonal and σ_i running through the embeddings of K into $\mathbb{C}$, and where $\Delta = (\sigma_i(\alpha_j))_{i,j}$ with $\{\alpha_j\}$ denoting a $\mathbb{Z}$-basis of $\widetilde{\mathfrak{b}}_1\mathfrak{d}^{-1}$. But the signature of $\Delta^t D \Delta$ equals $\operatorname{Sign}(1/4\omega) = \operatorname{Sign}(\omega)$, as is obvious if K is totally real and an easy exercise in the general case. This proves the theorem. □

Proof of Lemma. Using $\overline{C(\omega)} = C(-\omega)$ we find that $|C(\omega)|^2$ equals

$$\sum_{\mu,\nu \bmod \mathfrak{a}} \mathbf{e}\left(\operatorname{tr}\left(\omega(\mu-\nu)(\mu+\nu)\right)\right) = \sum_{\mu \bmod \mathfrak{a}} \mathbf{e}\left(\operatorname{tr}(\omega\mu^2)\right) \sum_{\nu \bmod \mathfrak{a}} \mathbf{e}\left(2\operatorname{tr}(\omega\mu\nu)\right),$$

where the right hand side is obtained by substituting $\mu + \nu \mapsto \mu$ in the left hand side. The inner sum on the right equals $\mathrm{N}(\mathfrak{a})$ if $2\mu\omega\mathfrak{d}$ is integral, i.e. if $\mu \in \widetilde{\mathfrak{a}} = \mathfrak{a}/(2,\mathfrak{a})$, and is 0 otherwise. We have therefore

$$|C(\omega)|^2 = \mathrm{N}(\mathfrak{a}) \sum_{\mu \in \widetilde{\mathfrak{a}}/\mathfrak{a}} \mathbf{e}\left(\operatorname{tr}(\omega\mu^2)\right).$$

It is easily checked that the application $\mu \mapsto \mathbf{e}\left(\operatorname{tr}(\omega\mu^2)\right)$ defines a group homomorphism $\widetilde{\mathfrak{a}}/\mathfrak{a} \mapsto \{\pm 1\}$. Hence the last sum is different from 0 if and only if $\operatorname{tr}(\omega\mu^2) \in \mathbb{Z}$ for all $\mu \in \widetilde{\mathfrak{a}}$, in which case $|C(\omega)|^2 = \mathrm{N}(\mathfrak{a}) \cdot [\widetilde{\mathfrak{a}} : \mathfrak{a}] = \mathrm{N}(\widetilde{\mathfrak{a}}) \cdot \mathrm{N}\left((2,\mathfrak{a})\right)^2$. The remaining statement of the lemma is obvious. □

References

[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.

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms.* Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[Wal63] C. T. C. Wall. Quadratic forms on finite groups, and related topics. *Topology*, 2:281–298, 1963.