THETA FUNCTIONS AND REPRESENTATIONS

MICHAEL BARZ

Abstract. Hecke was able to give a proof of quadratic reciprocity in arbitrary number fields by relating Gauss sums to theta functions. In this note, we show how Weil simplified Hecke's proof using the adelic philosophy and by relating theta functions to representation theory.

Contents

1. Hecke's Proof of Quadratic Reciprocity

precise knowledge of the behavior of an analytic function in the neighborhood of its singular points is often a source of number-theoretic theorems.

Hecke, [3] p. 201

In [3], chapter VIII, Hecke gives a proof of quadratic reciprocity for arbitrary number fields by evaluating generalized Gauss sums using theta functions. The purpose of this note is to showcase Weil's reframing of this argument in terms of adeles and representation theory; but before we do that, we give an idea as to what Hecke originally did, by showing his argument over $\mathbb{Q}$.

The crux of Hecke's proof is exploring singularities of the Jacobi ϑ function (and, in the general number field case, suitable generalizations of this function). Let[1]

$$\vartheta(\tau) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \tau}.$$

It's easy to see that if $\Re\tau > 0$, then this series converges absolutely. Thus, we will want to understand what ϑ looks like near the line $\Re\tau = 0$, where the singularities occur.

[1] Most modern sources give a slightly different definition of ϑ, but we will use the definition that Hecke used in his write up of the proof.

Recall the powerful theta inversion formula

$$\vartheta(\tau) = \frac{1}{\sqrt{\tau}}\vartheta\left(\frac{1}{\tau}\right),$$

where here we use the branch of the square root function on the $\Re\tau > 0$ plane for which $\sqrt{1} = 1$.

In analogy with computing the residue of a meromorphic function at a pole, we try to compute, for a real number t, the limit

$$\lim_{\tau\to it^+} \sqrt{\tau}\vartheta(\tau) = \lim_{\tau\to it^+} \vartheta\left(\frac{1}{\tau}\right),$$

where τ approaches it from the $\Re\tau > 0$ plane.

The simplest case is when $t = 0$. Here, we simply compute

$$\begin{aligned}\vartheta\left(\frac{1}{\tau}\right) &= \sum_{n\in\mathbb{Z}} e^{-\pi n^2/\tau} \\ &= 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2/\tau}.\end{aligned}$$

That latter sum goes to 0 as $\tau \to 0^+$, which we prove as follows. First note that for τ sufficiently close to 0, the quantity $|e^{-\pi/\tau}|$ will be strictly below 1, and so

$$\begin{aligned}\left|\sum_{n=1}^{\infty} e^{-\pi n^2/\tau}\right| &\leq \sum_{n=1}^{\infty} |e^{-\pi/\tau}|^{n^2} \\ &\leq \sum_{n=1}^{\infty} |e^{-\pi/\tau}|^{n} \\ &= |e^{-\pi/\tau}|\frac{1}{1-|e^{-\pi/\tau}|}.\end{aligned}$$

As $\tau \to 0^+$, the above clearly tends to $0 \cdot \frac{1}{1-0} = 0$. Hence

$$\lim_{\tau\to 0^+} \sqrt{\tau}\vartheta(\tau) = 1 + 2\cdot 0 = 1.$$

We then move this series over, and compute the 'residue' of the singularity at a general point it as follows.

Proposition 1.1. *For a rational number $q = a/b$ written in lowest terms with $b > 0$, define*

$$C(q) = \sum_{r=0}^{b-1} e^{2\pi i a r^2/b}.$$

For all $q \in \mathbb{Q}$, we have

$$\lim_{\tau\to 0^+} \sqrt{\tau}\cdot\vartheta\left(\tau - 2iq\right) = \frac{C(q)}{b}.$$

Proof. First write

$$\vartheta\left(\tau - i\frac{2a}{b}\right) = \sum_{n\in\mathbb{Z}} \exp\left(-\pi n^2\tau\right)\exp\left(i\pi n^2\frac{2a}{b}\right).$$

The term $e^{2\pi i n^2 a/b}$ only depends on the value of n modulo b, which inspires us to group terms as

$$\vartheta\left(\tau - i\frac{2a}{b}\right) = \sum_{r=0}^{b-1} \exp\left(i\pi r^2 \frac{2a}{b}\right) \sum_{q\in\mathbb{Z}} \exp\left(-\pi(bq+r)^2\tau\right). \tag{1.2}$$

By Poisson summation,

$$\sqrt{\tau}\sum_{q\in\mathbb{Z}} \exp\left(-\pi(bq+r)^2\tau\right) = \frac{1}{b}\sum_{q\in\mathbb{Z}} \exp\left(-\frac{\pi q^2}{b^2\tau}\right) \exp\left(\frac{2\pi i q r}{b}\right).$$

A similar analysis to the one used to compute $\lim_{\tau\to 0^+}\sqrt{\tau}\vartheta(\tau) = 1$ shows that in the right hand sum, all the $q \neq 0$ terms vanish as $\tau \to 0^+$ so that

$$\lim_{\tau\to 0^+} \sqrt{\tau}\sum_{q\in\mathbb{Z}} \exp\left(-\pi(bq+r)^2\tau\right) = \frac{1}{b}.$$

Substituing this into (1.2), we derive

$$\lim_{\tau\to 0^+} \sqrt{\tau}\vartheta\left(\tau - i\frac{a}{b}\right) = \frac{1}{b}\sum_{r=0}^{b-1} \exp\left(2\pi i r^2 \frac{a}{b}\right),$$

as desired. □

Combining this limit with theta inversion gives a very nice reciprocity law for these sums $C(q)$. Our treatment at this point very closely follows [3], chapter VIII.

Proposition 1.3. *Take a, b coprime positive integers, and write $b/4a$ in lowest terms as b_1/a_1. Then*

$$\frac{C(a/b)}{\sqrt{b}} = \frac{\sqrt{2a}}{a_1} e^{\pi i/4} C\left(-\frac{b}{4a}\right).$$

Remark 1.4. Most sources on quadratic reciprocity via theta functions written after Hecke use instead the Landsberg-Schaar relation, which is very similar to but not exactly the equation of this proposition. See [5] for a proof along these lines.

Proof. By theta inversion,

$$\vartheta\left(\frac{1}{\tau - i\frac{2a}{b}}\right) = \sqrt{\tau - i\frac{2a}{b}} \cdot \vartheta\left(\tau - i\frac{2a}{b}\right).$$

As $\tau \to 0^+$, it's easy to note (using positivity of a, b) that

$$\sqrt{\tau - 2ai/b} \to \sqrt{-2ai/b} = e^{-i\pi/4}\sqrt{\frac{2a}{b}}.$$

Substituting this into Proposition 1.1 gives

$$\frac{1}{b}C(a/b) = e^{i\pi/4}\sqrt{\frac{b}{2a}} \lim_{\tau\to 0^+} \sqrt{\tau} \cdot \vartheta\left(\frac{1}{\tau - i\frac{2a}{b}}\right),$$

or

$$\lim_{\tau\to 0^+} \sqrt{\tau} \cdot \vartheta\left(\frac{1}{\tau - i\frac{2a}{b}}\right) = \frac{\sqrt{2a}}{b\sqrt{b}} C(a/b) e^{-i\pi/4}.$$

Now, we evaluate that limit another way, as

$$\begin{aligned}
\lim_{\tau\to 0^+} \sqrt{\tau}\cdot\vartheta\left(\frac{1}{\tau - i\frac{2a}{b}}\right) &= \lim_{\tau\to(-2ai/b)^+} \sqrt{\tau+2ai/b}\cdot\vartheta\left(\frac{1}{\tau}\right)\\
&= \lim_{\tau\to(ib/(2a))^+} \sqrt{\tau^{-1}+2ai/b}\cdot\vartheta\left(\tau\right)\\
&= \lim_{\tau\to(ib/(2a))^+} \sqrt{\frac{\tau^{-1}+2ai/b}{\tau - ib/(2a)}}\cdot \lim_{\tau\to(ib/(2a))^+} \sqrt{\tau - ib/(2a)}\cdot\vartheta(\tau)\\
&= \frac{2a}{b}\cdot\frac{1}{a_1}C(-b/4a),
\end{aligned}$$

where in the last line the limit of the square root is computed with l'Hopital's rule, and the second limit is an instance of Proposition 1.1.

Equating these two expressions for the same limit, we deduce the desired relation

$$\frac{C(a/b)}{\sqrt{b}} = e^{i\pi/4}\frac{\sqrt{2a}}{a_1}C(-b/4a).$$

□

Proposition 1.3 allows quick computation of the quadratic Gauss sum

$$g(p) = \sum_{r=0}^{p-1} e^{2\pi i r^2/p} = C(1/p),$$

since we find that for p an odd prime,

$$\begin{aligned}
g(p) &= C(1/p)\\
&= \frac{\sqrt{2p}}{4}e^{\pi i/4}C(-p/4)\\
&= \frac{\sqrt{2p}}{4}e^{\pi i/4}\left(2+2e^{-2\pi i p/4}\right).
\end{aligned}$$

If $p\equiv 1 \pmod 4$, then $e^{-2\pi i p/4} = -i$ and this simplifies to

$$g(p) = \frac{\sqrt{2p}}{4}e^{\pi i/4}(2-2i) = \sqrt{p}.$$

If $p\equiv 3 \pmod 4$, then $e^{-2\pi i p/4} = i$ and we get $g(p) = i\sqrt{p}$.

We have now evaluated the sign of the quadratic Gauss sum; we can also get quadratic reciprocity. Applying Proposition 1.3 to $C(p/q)$, for p, q two distinct odd primes with $q\equiv 1 \pmod 4$, gives

$$\left(\frac{p}{q}\right)\frac{g(q)}{\sqrt{q}} = \frac{e^{\pi i/4}\sqrt{2}}{\sqrt{p}}\left(\frac{q}{p}\right)C(-1/4p). \tag{1.5}$$

The sign of $C(-1/4p)$ can be computed by noting

$$\frac{C(1/4p)}{2\sqrt{p}} = e^{\pi i/4}\sqrt{2}C(-p/1) = e^{\pi i/4}\sqrt{2}.$$

Hence the sign of $C(1/4p)$ is $e^{\pi i/4}$, and so $C(-1/4p)$ has sign $e^{-i\pi/4}$. Taking signs of the terms in (1.5) then gives (using our prior computation of the sign of the Gaus sum $g(q)$)

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

which is quadratic reciprocity (at least when $q \equiv 1 \pmod 4$); a similar derivation works in the other case).

Hecke actually did this computation over arbitrary number fields, by using a generalized theta series in place of Jacobi's ϑ function. This introduces considerable analytic complications that Weil is able to overcome via representation theory, as we focus on now.

2. Weil's Approach

Weil [6] recasts Hecke's proof in the context of the representation theory of Heisenberg groups, inspired by the surprising fact that the Jacobi ϑ function arises in a natural way from the so-called theta representation of the classical Heisenberg group.

We will start by giving some general definitions, and then explain the connection between ϑ and this perspective. In this section, we very closely follow Weil's original paper [6], though with added remarks on the connection with Hecke's ϑ function perspective.

2.1. **Standard notations.** Throughout this note, G is a locally compact abelian group, $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ is the torus, and G^* is the Pontryagin dual of G. We fix a Haar measure on G, and select a dual measure on G^* so that Plancherel's theorem holds in the form

$$\int_G |\Phi(x)|^2\, dx = \int_{G^*} |\widehat{\Phi}(x^*)|^2\, dx^*.$$

If $\alpha : G \to G^*$ is an *isomorphism* of topological groups, then we define the modulus $|\alpha|$ by the formula

$$\int_{G^*} F(x^*)\, dx^* = |\alpha| \int_G F(\alpha(x))\, dx$$

for all $F \in L^1(G^*)$. Such an $|\alpha|$ exists by uniqueness of Haar measure, since the rule

$$F \mapsto \int_G F(\alpha(x))\, dx$$

is a positive linear functional $C_c(G^*) \to \mathbb{C}$, invariant under translations since

$$\int_G F(\alpha(x) + g^*)\, dx = \int_G F(\alpha(x + \alpha^{-1} g))\, dx = \int_G F(\alpha(x))\, dx$$

by translation invariance of dx; hence this must be some positive real number times the integral F in the measure dx^*.

Finally, we say that a continuous function $f : G \to \mathbb{T}$ is a *character of second degree* if $f(x + y) f^{-1}(x) f^{-1}(y)$ is a character in x for every fixed y. We define $\rho : G \to G^*$ so that

$$\rho(y)(x) = f(x + y) f^{-1}(x) f^{-1}(y).$$

Note that ρ is *symmetric*, i.e. $\rho(y)(x) = \rho(x)(y)$.

Remark 2.1. These characters of second degree are analogous to the functions $e^{-\pi n^2 \tau}$ appearing in the Jacobi ϑ function; although note that only when $\Re\tau = 0$ do we actually get a character of second degree–generally, writing $\tau = \sigma + it$, we can think of

$$e^{-\pi n^2 \tau} = e^{-\pi i n^2 t} e^{-\pi n^2 \sigma}$$

as some character $e^{-\pi i n^2 t}$ of degree 2, weighted with the Gaussian $e^{-\pi n^2\sigma}$ for convergence.

2.2. **Theta series and their transformations.** Hecke's proof of quadratic reciprocity is a reduction

$$\text{theta inversion} \implies \text{a Gauss sum identity} \implies \text{quadratic reciprocity.}$$

We thus start by trying to generalize theta inversion. Theta inversion is classically proven in two parts: first, compute the Fourier transform of a Gaussian; then Poisson sum.

As mentioned in Remark 2.1, the Gaussians are replaced by some character of degree two mollified by a Schwartz function. Weil gets a surprisingly elegant identity on the Fourier transform of such a mollification.

Theorem 2.2. *Let $f : G \to \mathbb{T}$ be a character of degree two, and suppose that the associated morphism $\rho : G \to G^*$ is an isomorphism. Define $F(x^*) = f(x^*\rho^{-1})^{-1}$. Then there is some $\lambda(f) \in \mathbb{T}$ so that for any Schwartz function $\Phi : G \to \mathbb{C}$ and any $x^* \in G^*$,*

$$\widehat{f\Phi}(x^*) = \int_G f(x)\Phi(x)\cdot x^*(x)\,dx = \gamma(f)|\rho|^{-1/2}[F * \Phi](x^*),$$

and furthermore

$$\widehat{f * \Phi}(x^*) = \int_G (\Phi * f)(x)\cdot x^*(x)\,dx = \gamma(f)|\rho|^{-1/2}\widehat{\Phi}(x^*)f(\rho^{-1}(x^*))^{-1}. \tag{2.3}$$

Remark 2.4. Taking $x^* = 0$ in (2.3), we derive the important identity

$$\int_G (\Phi * f)(x)\,dx = \gamma(f)|\rho|^{-1/2}\int_G \Phi(x)\,dx. \tag{2.5}$$

This identity will allow us to easily explicitly compute $\gamma(f)$.

We will delay a proof of Theorem 2.2 to Section 4, since it is quite involved. The proof of this theorem is where Heisenberg groups enter the picture.

Anyways, the second part of establishing theta inversion is using Poisson summation to lift the Fourier transform identity into a transformation law of the associated theta series. The rest of this section will be concerned with doing this.

2.3. **Weil's Θ functions.** Take $\Gamma \leq G$ a discrete subgroup. Define

$$\Gamma_* = \{x^* \in G^* \mid x^*(\gamma) = 1 \text{ for all } \gamma \in \Gamma\}.$$

Let $d\dot{g}$ be a Haar measure on the quotient G/Γ and $d\gamma$ a Haar measure on Γ, appropriately normalized so that $dg = d\gamma d\dot{g}$.

Remark 2.6. At this point, Weil [6] works in much more generality than we will need. Following [2], we will only prove the special case of the results of Weil which we need to prove quadratic reciprocity, which considerably shortens the argument and allows for the analogies with Hecke's proof to be more transparent.

As in Tate's thesis, one of the central simplifications to Hecke's original argument we make is that *our Poisson summation will now be done adelically.*

Specifically, fix $f : G \to \mathbb{T}$ a character of second degree, associated to a symmetric isomorphism $\rho : G \to G^*$ so that $\rho(\Gamma) = \Gamma_*$ and $f(\gamma) = 1$ for all $\gamma \in \Gamma$. As discussed before, we take some $\Phi \in \mathcal{S}(G)$, and then Poisson sum $f\Phi$.

The restrictions placed on f do *not* hold for a character of second degree like $e^{2\pi i x^2/p}$ on $\mathbb{R}$ with $\Gamma = \Gamma_* = \mathbb{Z}$. But, if we work adelically, then as we show later, the corresponding character *will* be trivial on the subgroup $\Gamma = \mathbb{Q}$, and so our following arguments will yield something interesting in that setting.

Before Poisson summing, it will be helpful to prove a simplifying identity.

Lemma 2.7. *The modulus $|\rho|$ of ρ is the same whether or not ρ is viewed as an isomorphism between G, G^* or Γ, Γ_*.*

Remark 2.8. Thanks to Prof. Hirschfeldt, who showed me last year the main idea behind this lemma in a slightly different context.

Proof. Since Γ is discrete, we may find some U open so that $U \cap \Gamma = \{0\}$. Then, noting that $(x, y) \mapsto x - y$ is a continuous map $G \times G \to G$, we can find some open $V \subseteq U$ containing 0 so that $V - V \subseteq U$. Furthermore, by local compactness we may assume that V has finite measure.

Set $W = \bigcup_{\gamma\in\Gamma}(V + \gamma)$. We claim the translates $V + \gamma$ are pairwise disjoint; indeed, if $v \in V \cap (V+\gamma)$, then $v = w+\gamma$ for some $w \in V$, implying that $v-w = \gamma$, which (since $(V-V)\cap\Gamma = \{0\}$ by our construction) implies $\gamma = 0$.

Because Γ is discrete, we find that there are constants m_γ making

$$\int_\Gamma f(\gamma)\, d\gamma = \sum_{\gamma\in\Gamma} f(\gamma) m_\gamma$$

true for every choice of $f \in L^1(\Gamma)$. Define $F' : G \to \mathbb{C}$ as

$$F'(x) = \begin{cases} \frac{F(\gamma)m_\gamma}{\mu_G(V)} & x \in V + \gamma, \\ 0 & \text{otherwise}, \end{cases}$$

where this is well-defined since the $V + \gamma$ translates are pairwise disjoint as shown above. Then we know that

$$\int_G F'(x)\, dx = \int_\Gamma F(\gamma)\, d\gamma.$$

But also

$$\int_G F'(x)\, dx = |\rho^{-1}| \int_{G^*} F'(\rho^{-1}(x))\, dx^* = |\rho^{-1}| \int_{\Gamma_*} F'(\rho^{-1}(\gamma))$$

for $|\rho^{-1}|$ the modulus of ρ^{-1}. Hence, the modulus of ρ^{-1} is the same whether you view it as an isomorphism between G^*, G or Γ_*, Γ. Since $|\rho| = |\rho^{-1}|^{-1}$, the lemma follows. $\square$

With this, we can make certain changes of variables in our Poisson summation without worrying about whether or not $|\rho|$ should be computed on G or Γ.

By Poisson summation and Theorem 2.2, if we define $F(x^*) = f(x^*\rho^{-1})^{-1}$, then

$$\int_\Gamma f\Phi = \int_{\Gamma_*} \widehat{f\Phi}(\gamma^*)\, d\gamma^* = \gamma(f)|\rho|^{-1/2} \int_{\Gamma_*} [F * \widehat{\Phi}](\gamma^*)\, d\gamma^*.$$

Now we compute that convolution. We claim

$$[F * \widehat{\Phi}](x^*) = F(x^*) \cdot \mathcal{F}(F\widehat{\Phi})(-x^*\rho^{-1}).$$

Indeed, recalling that ρ's defining identity is

$$f(x + y)f(x)^{-1}f(y)^{-1} = (y\rho)(x),$$

we find

$$\begin{aligned}
F(x^*)\cdot\mathcal{F}(F\widehat{\Phi})(-x^*\rho^{-1}) &= F(x^*)\int_{G^*} F(g^*)\widehat{\Phi}(g^*)\cdot g^*(-x^*\rho^{-1})\,dg^* \\
&= F(x^*)\int_{G^*} F(-g^*)\widehat{\Phi}(-g^*)\cdot g^*(x^*\rho^{-1})\,dg^* \\
&= \int_{G^*} f(x^*\rho^{-1})^{-1}f(-g^*\rho^{-1})^{-1}\widehat{\Phi}(-g^*)\cdot g^*(x^*\rho^{-1})\,dg^* \\
&= \int_{G^*} F(x^*-g^*)g^*(-x^*\rho^{-1})\cdot\widehat{\Phi}(g^*)\cdot g^*(x^*\rho^{-1})\,dg^* \\
&= \int_{G^*} F(x^*-g^*)\cdot\widehat{\Phi}(g^*)\,dg^* \\
&= [F*\widehat{\Phi}](x^*).
\end{aligned}$$

Thus,

$$\begin{aligned}
\int_\Gamma f\Phi &= \gamma(f)|\rho|^{-1/2}\int_{\Gamma_*} F(\gamma^*)\mathcal{F}(F\widehat{\Phi})(-\gamma^*\rho^{-1})\,d\gamma^* \\
&= \gamma(f)|\rho|^{-1/2}\int_{\Gamma_*} \mathcal{F}(F\widehat{\Phi})(-\gamma^*\rho^{-1})\,d\gamma^* \\
&= \gamma(f)|\rho|^{1/2}\int_{\Gamma} \mathcal{F}(F\widehat{\Phi})(-\gamma)\,d\gamma.
\end{aligned}$$

We can Poisson sum the last expression *twice more* to find that

$$\begin{aligned}
\int_\Gamma f\Phi &= \gamma(f)|\rho|^{1/2}\int_{\Gamma} \mathcal{F}(F\widehat{\Phi})(-\gamma)\,d\gamma \\
&= \gamma(f)|\rho|^{1/2}\int_{\Gamma_*} F(\gamma^*)\widehat{\Phi}(\gamma^*)\,d\gamma^* \\
&= \gamma(f)|\rho|^{1/2}\int_{\Gamma_*} \widehat{\Phi}(\gamma^*)\,d\gamma^* \\
&= \gamma(f)|\rho|^{1/2}\int_{\Gamma} \Phi,
\end{aligned}$$

and so (recalling $f\equiv 1$ on Γ)

$$\int_\Gamma \Phi = \int_\Gamma f\Phi = \gamma(f)|\rho|^{1/2}\int_\Gamma \Phi,$$

implying that $\gamma(f)|\rho|^{1/2} = 1$ so long as we pick Φ to not have integral 0. But then of course $\gamma(f) = 1$, since $|\gamma(f)| = 1$ and $|\rho|^{1/2}$ is a positive real.

Remark 2.9. The above also implies $|\rho| = 1$. Weil directly proves $|\rho| = 1$ in his version of Lemma 2.7, although in doing so requires a more complicated argument.

We summarize the central result of our calculation.

Theorem 2.10. *Take $\Gamma \le G$ a discrete subgroup. If $f : G \to \mathbb{T}$ is a character of second degree so that $f \equiv 1$ on Γ, and so that the associated morphism $\rho : G \to G^*$ is an isomorphism carrying Γ onto Γ_*, then $\gamma(f) = 1$.*

3. Quadratic Reciprocity, Weil's Way

Now that we have suitably generalized theta inversion to get Theorem 2.10, we derive quadratic reciprocity.

Remark 3.1. Weil proves reciprocity of the Hilbert 2-symbol from Theorem 2.10. We instead prove quadratic reciprocity in the form Hecke states it in [3].

Start by fixing a number field k. Let v denote a place of k.

We will want to consider quadratic forms, and so we take X_v to be a finite-dimensional vector space over k_v. Fix a nontrivial character χ_v of the additive group of k_v. Note that if f_v is a quadratic form over X_v, then $\chi_v \circ f_v$ is a character of X_v of second degree. We say that f_v is *nondegenerate* if $\chi_v \circ f_v$'s associated morphism ρ_v is an isomorphism.

We write $\gamma(f_v)$ for the gamma factor in Theorem 2.2.

3.1. Computing γ.

We now compute $\gamma(f_v)$ at a few places, using the formula (from Remark 2.4)

$$\int_{X_v}\int_{X_v} \Phi(x-y)(\chi_v \circ f_v)(y)\,dxdy = \gamma(f_v)|\rho|^{-1/2}\int_{X_v}\Phi(x)\,dx \tag{3.2}$$

for every $\Phi \in \mathcal{S}(X_v)$. Our presentation follows Weil's original paper [6].

It's useful to prove the following two lemmas, to considerably reduce the computational effort needed to prove this.

Lemma 3.3. *Write $X_v = X_1 \oplus X_2$ for X_1, X_2 two smaller-dimensional vector spaces over k_v. Then if $f_v(x_1, x_2) = f_1(x_1) + f_2(x_2)$, we have $\gamma(\chi_v \circ f_v) = \gamma(\chi_v \circ f_1)\gamma(\chi_v \circ f_2)$.*

Proof. Set $F_v = \chi_v \circ f_v$ and $F_1 = \chi_v \circ f_1, F_2 = \chi_v \circ f_2$. Then $F_v = F_1F_2$. From this and Fubini's theorem by decomposing $\int_X = \int_{X_1}\int_{X_2}$, the identity follows immediately from (3.2). ☐

Lemma 3.4. *If f_v, g_v are two nondegenerate equivalent quadratic forms over X_v, then $\gamma(f_v) = \gamma(g_v)$.*

Proof. Write $f_v = g_v \circ B$ for some $B \in \mathrm{Aut}(X_v)$. Let ρ_f, ρ_g be the associated isomorphisms. Then $\rho_f = B^* \circ \rho_g \circ B$. As $|B| = |B^*|$, when changing g_v to f_v in (3.2), the right hand side will change by a factor of $\gamma(f_v)/\gamma(g_v) \cdot |B|^{-2/2}$, and the left hand side will change by a factor of $|B|^{-1}$. Because the resulting equation is still true, we find that $\gamma(f_v) = \gamma(g_v)$ since the left and right hand sides must have changed by the same factor. ☐

With this two lemmas, we start computing γ factors. We will explicitly do the work for nonarchimedean places, but since the computations for $\mathbb{R}, \mathbb{C}$ are just calculus, we omit them and refer a curious reader to [6].

3.1.1. *Nonarchimedean places.*

These are the most interesting. Take $f : X \to k_v$ a quadratic form with associated isomorphism $\rho : X \to X^*$.

The main difference in geometry between these and the archimedean places is that, since χ_v's kernel is some open subgroup of k_v, on all sufficiently small lattices[2] L of X, we find that $\chi_v(f_v(x)) = 1$ for $x \in L$. In particular, if $x, y \in L$ then

$$1 = \chi_v(f_v(x+y)) = \chi_v(f_v(x)f_v(y)(y\rho_v)(x)) = \chi_v(f_v(x))\chi_v(f(y)) \cdot \chi_v(\rho_V(y)(x)) = \chi_v(\rho_v(y)(x)).$$

Hence, $\rho_v(L) \subseteq L_*$ for L_* the dual lattice. Set $L' = \rho_v^{-1}(L_*)$, noting that $L' \supseteq L$.

[2] By a lattice, we mean a compact subgroup which is an $\mathcal{O}_v$ module for $\mathcal{O}_v$ the ring of integers

Then

$$(\mathbb{1}_L * (\chi_v \circ f_v))(x) = \int_L \chi_v(f_v(x-y))\,dy = \chi_v(f_v(x)) \int_L \chi_v(\rho_v(x)(-y))\,dy.$$

If $\rho_v(x) \in L_*$, then the above expression is just $\chi_v(f_v(x))m(L)$ for $m(L) = \int_L dy$ the measure of L. If $\rho_v(x) \notin L_*$, then since $y \mapsto -y$ is an involution of L we find that the integral is 0. In other words,

$$(\mathbb{1}_L * (\chi_v \circ f_v))(x) = \chi_v(f_v(x))m(L)\mathbb{1}_{L_*}(x\rho_v) = \chi_v(f_v(x))m(L)\mathbb{1}_{L'}(x).$$

Setting $\Phi = \mathbb{1}_L$ in (3.2) then tells us that

$$\int_{L'} \chi_v(f_v(x))\,dx = \gamma(f_v)|\rho_v|^{-1/2}.$$

In particular, $\gamma(f_v)$ is the sign of $\int_{L'} \chi_v \circ f_v$. We can make this more explicit as follows. Since for $x \in L$ we have

$$\chi_v(f_v(x)) = \chi_v(\langle x, 2^{-1}\rho_v x\rangle) = 1,$$

so that $\chi_v \circ f_v(y)$ depends only on y mod L, we may write

$$\int_{L'} \chi_v \circ f_v = m(L) \sum_{x \in L'/L} \chi_v(f_v(x)).$$

We denote this quantity by $g(f_v)$, and so $\gamma(f_v) = g(f_v)/|g(f_v)|$.

Remark 3.5. As the notation suggests, this is a slight generalization of a Gauss sum. When proving quadratic reciprocity, we make this connection more explicit.

3.1.2. *Archimedean places.* We will omit the calculations for archimedean places since they are just certain integral computations that can be found in [6], section 26.

All quadratic forms over $\mathbb{R}$ are equivalent to a form $x_1^2 + \cdots + x_p^2 - y_1^2 - \cdots - y_q^2$. If we take $\chi_v(\xi) = e^{-2\pi i \xi}$, then we can compute that

$$\gamma(x_1^2 + \cdots + x_p^2 - y_1^2 - \cdots - y_q^2) = (e^{-\pi i/4})^{p-q}.$$

Over $\mathbb{C}$, all quadratic forms are equivalent to the form $x_1^2 + \cdots + x_n^2$. And we find that $\gamma(x_1^2 + \cdots + x_n^2) = 1$.

3.2. **The adelic case.** Fix X a finite-dimensional vector space over k. Define $X_v = X \otimes k_v$ and $X_A = X \otimes \mathbf{A}_k$.

Pick $\chi = \otimes_v \chi_v$ a character which has value 1 on k.

Theorem 3.6. *Let f be a nondegenerate quadratic form on X. Then*

$$\gamma(\chi \circ f) = \prod_v \gamma(\chi_v \circ f) = 1.$$

The above notation is a little abusive, since in $\gamma(\chi \circ f)$ we really mean the canonical extension of $f : X_k \to k$ to $f : X_A \to \mathbf{A}(K)$, and likewise for the $\gamma(\chi_v \circ f)$ factors.

Proof. That $\gamma(\chi \circ f) = 1$ follows from Theorem 2.10. Specifically, set $G = X_A$ and let $\Gamma = X_k$, noting that Γ is discrete since k is discrete in $\mathbf{A}_k$. $\chi \circ f$ is trivial on Γ because χ is trivial on k and $f(X_k) \subseteq k$.

The last thing to check is that the associated isomorphism ρ to f carries X_k to Γ_*. For this, just identify $\mathbf{A}(K)$ with its dual using χ, and note then that $\Gamma_* = X_k$ as well after making that identification since the dual of k is k.

Hence, $\gamma(\chi \circ f) = 1$. The product formula

$$\gamma(\chi \circ f) = \prod_v \gamma(\chi_v \circ f)$$

follows from Fubini's theorem applied to (3.2). Thus the theorem is proven. $\square$

Theorem 3.6 is our fundamental relationship between Gauss sums, and it will play the role that Proposition 1.3 did in our proof of quadratic reciprocity over $\mathbb{Q}$ at the start.

3.3. **Gamma factors for a monomial.** Let $\mathfrak{d}$ denote the different of $k/\mathbb{Q}$. We will need to take the duals of lattices when computing the gamma factors at nonarchimedean places, which is why the different is relevant.

We work out the gamma factors explicitly for the form $f(x) = \omega x^2$, where $\omega \in k$ is some number so that the fractional ideal $\omega\mathfrak{d}$ can be written in the form $\mathfrak{b}/\mathfrak{a}$ for $\mathfrak{a}, \mathfrak{b}$ ideals of $\mathcal{O}_k$ which are both coprime and odd (i.e., coprime to (2)).

Let $\sigma_1, ..., \sigma_r$ denote the real embeddings of k. Then set

$$\operatorname{sgn} \omega = \sum_{i=1}^{r} \operatorname{sgn} \sigma_i(\omega),$$

where for $t \in \mathbb{R}$, we say that $\operatorname{sgn} t = 1$ if $t > 0$, $\operatorname{sgn} t = 0$ if $t = 0$, and $\operatorname{sgn} t = -1$ otherwise. Then, since the gamma factors are all 1 at the complex places, the archimedean gamma factors have total contribution $e^{-\pi i (\operatorname{sgn} \omega)/4}$ to the product.

Now, the nonarchimedean gamma factors. Take v a place corresponding to a prime ideal $\mathfrak{p}$. We will handle separately the cases of $\mathfrak{p} \mid \mathfrak{a}, \mathfrak{p} \mid 2\mathfrak{b}$, and then all other primes. These cases are mutually exclusive by the postulated coprimalities.

First when $\mathfrak{p} \mid \mathfrak{a}$. We use the notation of Section 3.1.1 in making this computation. Set e the highest exponent for which $\mathfrak{p}^e \mid \mathfrak{a}$, and let $L = \pi^e \mathcal{O}_v$ for π a generator of $\mathcal{O}_v$'s maximal ideal.

Then $\chi_v(f(x)) = 1$ on L, which we see as follows. We know that $\chi_v(f(x)) = 1$ whenever $f(x) = \omega x^2 \in \pi^{-e'}\mathcal{O}_v$, where e' is the largest exponent so that $\mathfrak{p}^{e'} \mid \mathfrak{d}$. If $x \in L$, then $\omega x^2 \pi^{e'}$ has valuation at least

$$\nu_{\mathfrak{p}}(\omega) + 2e + e'.$$

Since $\omega\mathfrak{d} = \mathfrak{b}/\mathfrak{a}$, the valuation of ω is just $-e - e'$, and hence $\omega x^2 \pi^{e'}$ has valuation at least $e > 0$. Thus $\chi_v(f(x)) = 1$ on L, as χ_v is trivial on elements of strictly positive valuation.

Then $L_* = \pi^{-e-e'}\mathcal{O}_v$, and $\rho_v(y)(x) = \chi_v(2\omega xy)$. Thus $L' = \rho_v^{-1}(L_*)$ consists of those $y \in k_v$ for which $2\omega y \in \pi^{-e-e'}\mathcal{O}_v$. By a similar valuation computation to the above, this is equivalent to demanding $y \in \mathcal{O}_v$. Hence $L' = \mathcal{O}_v$.

Thus, we have $\gamma_v(f) = g_v(f)/|g_v(f)|$ for

$$g_v(f) = \sum_{x \in \mathcal{O}_v/\pi^e\mathcal{O}_v} \chi_v(\omega x^2) = \sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\omega x^2).$$

Define

$$C(\omega) = \prod_{\mathfrak{p} \mid \mathfrak{a}} \sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\omega x^2).$$

This quantity collects all the gamma factors at the places dividing $\mathfrak{a}$.

Remark 3.7. Since each gamma factor has absolute value one, it follows that $C(\omega) \neq 0$. This nonzero-ness is thus obvious from our perspective, but in Hecke's perspective it requires a tedious algebraic argument.

Now, the primes $\mathfrak{p} \mid 2\mathfrak{b}$. A similar computation goes through, but here we may take $L = \mathcal{O}_v$. Then if we take e' the maximal exponent of the $\mathfrak{p}$ in $\mathfrak{d}$, and e the maximal exponent of $\mathfrak{p}$ in $2\mathfrak{b}$, we find that $L_* = \pi^{-e'}\mathcal{O}_v$ and $L' = \pi^{-e}\mathcal{O}_v$. Then $\gamma_v(f) = g_v(f)/|g_v(f)|$ for

$$g_v(f) = \sum_{x \in \pi^{-e}\mathcal{O}_v/\mathcal{O}_v} \chi_v(\omega x^2) = \sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\omega(x/\pi^e)^2).$$

Let

$$D(\omega) = \prod_{\mathfrak{p} \mid 2\mathfrak{b}} \sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\omega(x/\pi^e)^2).$$

One can similarly compute that all other nonarchimedean places have gamma factors equal to 1. Theorem 3.6 therefore gives us

$$1 = e^{-\pi i(\operatorname{sgn}\omega)/4} \frac{C(\omega)}{|C(\omega)|} \frac{D(\omega)}{|D(\omega)|},$$

or alternatively

$$\frac{C(\omega)}{|C(\omega)|} = e^{\pi i(\operatorname{sgn}\omega)/4} \frac{|D(\omega)|}{D(\omega)}. \tag{3.8}$$

We use this relation to derive a version of quadratic reciprocity in $\mathcal{O}_k$.

Remark 3.9. At this point, we are essentially following Hecke's proof [3] of quadratic reciprocity. Thus, our arguments here closely mirror chapter VIII of [3].

First, we need a little bit of algebraic insight about these $C(\omega)$.

Proposition 3.10. *Suppose $\alpha, \beta \in \mathcal{O}_k$ are both* odd *(i.e. $\alpha\mathcal{O}_k$ is coprime to $2\mathcal{O}_k$), coprime to each other and both coprime to some integral ideal $\mathfrak{b}$. Suppose $\omega \in k$ is so that $\omega\mathfrak{d} = \mathfrak{b}$. Then*

$$C\left(\frac{\omega}{\alpha\beta}\right) = C\left(\frac{\omega\alpha}{\beta}\right) C\left(\frac{\beta\omega}{\alpha}\right).$$

Remark 3.11. The point of this lemma is that it gives us an easier way to compute $C(\omega/(\alpha\beta))$ by reducing the size of the denominator we're over. A similar statement is true with α, β replaced by ideals, but we won't need that for our work.

Proof. Suppose v is a place corresponding to a prime dividing β. Then α is a unit in $\mathcal{O}_v$, and so by doing a change of variables in the sum it's easy to see $g_v(\omega x^2\alpha^{-1}\beta^{-1}) = g_v(\omega x^2\alpha\beta^{-1})$ by sending x to αx. An analogous statement holds for the primes dividing α.

By the coprimality, we then find

$$\begin{aligned} C\left(\frac{\omega}{\alpha\beta}\right) &= \prod_{\mathfrak{p}\mid\alpha} g_v(\omega x^2\alpha^{-1}\beta^{-1}) \prod_{\mathfrak{p}\mid\beta} g_v(\omega x^2\alpha^{-1}\beta^{-1}) \\ &= \prod_{\mathfrak{p}\mid\alpha} g_v(\omega x^2\alpha^{-1}\beta^{1}) \prod_{\mathfrak{p}\mid\beta} g_v(\omega x^2\alpha^{1}\beta^{-1}) \\ &= C\left(\frac{\omega\beta}{\alpha}\right) C\left(\frac{\omega\alpha}{\beta}\right), \end{aligned}$$

as desired. ∎

If we're going to state quadratic reciprocity, we'll need a Legendre symbol that works in general number fields. So we define $\left(\frac{\alpha}{\beta}\right)$ for $\alpha, \beta \in \mathcal{O}_k$ coprime (i.e., the principal ideals they generate are coprime) as follows. If $\beta\mathcal{O}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_l$, for (not necc. distinct) primes $\mathfrak{p}_i$, then set

$$\left(\frac{\alpha}{\beta}\right) = \prod_{i=1}^{l} \left(\frac{\alpha}{\mathfrak{p}_i}\right) = \prod_{i=1}^{l} \begin{cases} 1 & \alpha \equiv x^2 \pmod{\mathfrak{p}_i}, \\ -1 & \text{otherwise.} \end{cases}$$

Note that this definition even makes sense whenever β is any ideal of $\mathcal{O}_k$.

Proposition 3.12. *If $\alpha \in \mathcal{O}_k$ is coprime to $\mathfrak{a}$, and $\omega\mathfrak{d} = \mathfrak{b}/\mathfrak{a}$ in lowest terms, then*

$$C(\alpha\omega) = \left(\frac{\alpha}{\mathfrak{a}}\right) C(\omega).$$

Proof. Similarly to Proposition 3.10, this reduces to showing that at each place v corresponding to a prime $\mathfrak{p} \mid \mathfrak{a}$, with e the maximal exponent dividing $\mathfrak{a}$,

$$\sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\alpha\omega x^2) = \left(\frac{\alpha}{\mathfrak{p}^e}\right) \sum_{x \in \mathcal{O}_k/\mathfrak{p}^e} \chi_v(\omega x^2).$$

This identity is proven similarly to the corresponding classical Gauss sum identity; see [3], Theorem 155. □

With these preliminaries, we can finally prove quadratic reciprocity.

Theorem 3.13. *Suppose that $\alpha, \beta \in \mathcal{O}_k$ are odd (i.e. the principal ideals they generate are coprime to (2)) and coprime to each other. Further suppose that α is primary, i.e. congruent to a square modulo $4\mathcal{O}_k$. Then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = (-1)^{\sum_{i=1}^{r} \frac{\operatorname{sgn}\sigma_i\alpha - 1}{2} \cdot \frac{\operatorname{sgn}\sigma_i\beta - 1}{2}},$$

where $\sigma_1, \ldots, \sigma_r$ are the real embeddings of k.

Remark 3.14. Hecke in sections 59-62 of [3] derives supplementary theorems for dealing with the case where you drop the oddness assumption or the primary assumption. These are analogous to the expressions for $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$ in the classical case. We will not prove these supplementary theorems.

Proof. Analogously to Dirichlet's theorem, one can prove that there are infinitely many prime ideals in the same ideal class as $\mathfrak{d}$, by taking characters on the ideal class group. In particular, since of course only finitely many primes divide $\alpha\beta$, there must some integral ideal $\mathfrak{b}$ so that $\mathfrak{b}/\mathfrak{d} = (\omega)$ is principal (with $\omega \in k$), and $(\mathfrak{b}, \alpha\beta) = \mathcal{O}_k$.

Notice that, by Proposition 3.10 and Proposition 3.12,

$$C\left(\frac{\omega}{\alpha\beta}\right) = C\left(\frac{\alpha\omega}{\beta}\right) C\left(\frac{\beta\omega}{\alpha}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) C(\omega/\alpha)C(\omega/\beta). \tag{3.15}$$

Since Legendre symbols have modulus 1, we can replace every expression in the above equation by its sign, telling us

$$\frac{C(\omega\alpha^{-1}\beta^{-1})}{|C(\omega\alpha^{-1}\beta^{-1})|} = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) \frac{C(\omega/\alpha)C(\omega/\beta)}{|C(\omega/\alpha)C(\omega/\beta)|}.$$

Applying (3.8), we get

$$v(\omega,\alpha,\beta)\frac{D(\omega\alpha^{-1})D(\omega\beta^{-1})}{|D(\omega\alpha^{-1})D(\omega\beta^{-1})|}=\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)\frac{D(\omega\alpha^{-1}\beta^{-1})}{|D(\omega\alpha^{-1}\beta^{-1})|}\tag{3.16}$$

for

$$v(\omega,\alpha,\beta)=e^{\pi i(\operatorname{sgn}(\omega\alpha^{-1}\beta^{-1})-\operatorname{sgn}(\omega\alpha^{-1})-\operatorname{sgn}(\omega\beta^{-1}))/4}.$$

Note that if x,y,z are all real, then

$$\operatorname{sgn}(xy^{-1}z^{-1})-\operatorname{sgn}(xy^{1})-\operatorname{sgn}(xz^{-1})+\operatorname{sgn}(x)=\operatorname{sgn}(x)(\operatorname{sgn}y-1)(\operatorname{sgn}z-1),$$

and that the quantity $(\operatorname{sgn}y-1)(\operatorname{sgn}z-1)$ is a multiple of 4, since $\operatorname{sgn}y,\operatorname{sgn}z$ are both odd. Thus, applying this identity in each real embedding of k, we derive

$$v(\omega,\alpha,\beta)e^{\pi i\operatorname{sgn}(\omega)/4}=(-1)^{\sum_{i=1}^{r}\frac{\operatorname{sgn}\sigma_i\alpha-1}{2}\frac{\operatorname{sgn}\sigma_i\beta-1}{2}}.\tag{3.17}$$

We are allowed to drop $\operatorname{sgn}(\omega)$ on the right hand side since $e^{-\pi i}=e^{+\pi i}$.

Now we use the assumption that α is primary. Because of that, if $\mathfrak{p}^f\mid 2$, then $\alpha\equiv a^2 \pmod{\mathfrak{p}^{2f}}$ where $a\notin\mathfrak{p}$, so that

$$\begin{aligned}g_{\mathfrak{p}}(\omega x^2/\alpha)&=\sum_{x\in\mathcal{O}_k/\mathfrak{p}^f}\chi_v(\omega x^2\alpha^{-1}/\pi^{2f})\\&=\sum_{x\in\mathcal{O}_k/\mathfrak{p}^f}\chi_v(\omega(xa^{-1})^2/\pi^{2f})\\&=\sum_{x\in\mathcal{O}_k/\mathfrak{p}^f}\chi_v(\omega x^2/\pi^{2f})\\&=g_{\mathfrak{p}}(\omega x^2).\end{aligned}$$

A similar argument applies to $\omega x^2/(\alpha\beta)$, so that

$$\prod_{\mathfrak{p}|2}g_{\mathfrak{p}}(\omega\alpha^{-1}x^2)g_{\mathfrak{p}}(\omega\beta^{-1}x^2)=\prod_{\mathfrak{p}|2}g_{\mathfrak{p}}(\omega x^2)g_{\mathfrak{p}}(\omega\alpha^{-1}\beta^{-1}x^2).$$

The equation above is *almost* saying that $D(\omega\alpha^{-1})D(\omega\beta^{-1})=D(\omega)D(\omega\alpha^{-1}\beta^{-1})$, but we're missing the primes dividing $\mathfrak{b}$. Fortunately, these work out simply, so we find

$$\begin{aligned}D(\omega\alpha^{-1})D(\omega\beta^{-1})&=\prod_{\mathfrak{p}|2}\left[g_{\mathfrak{p}}(\omega\alpha^{-1}x^2)g_{\mathfrak{p}}(\omega\beta^{-1}x^2)\right]\prod_{\mathfrak{p}|\mathfrak{b}}\left[g_{\mathfrak{p}}(\omega\alpha^{-1}x^2)g_{\mathfrak{p}}(\omega\beta^{-1}x^2)\right]\\&=\prod_{\mathfrak{p}|2}\left[g_{\mathfrak{p}}(\omega x^2)g_{\mathfrak{p}}(\omega\alpha^{-1}\beta^{-1}x^2)\right]\prod_{\mathfrak{p}|\mathfrak{b}}\left(\frac{\alpha^{-1}}{\mathfrak{p}^{\nu(\mathfrak{b})}}\right)^2\left[g_{\mathfrak{p}}(\omega x^2)g_{\mathfrak{p}}(\omega\alpha^{-1}\beta^{-1}x^2)\right]\\&=D(\omega)D(\omega\alpha^{-1}\beta^{-1}).\end{aligned}$$

Substituting this and (3.17) into (3.16) gives

$$e^{-\pi i\operatorname{sgn}(\omega)/4}\frac{D(\omega)}{|D(\omega)|}=(-1)^{\sum_{i=1}^{r}\frac{\operatorname{sgn}\sigma_i\alpha-1}{2}\frac{\operatorname{sgn}\sigma_i\beta-1}{2}}\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right).$$

Applying (3.8), the left hand side is just $|C(\omega)|/C(\omega)$. Hence we need to prove that $C(\omega)$ is a positive real, and then we will have quadratic reciprocity. But fortunately, (3.15) still holds when $\alpha=\beta=1$, and so from it we find $C(\omega)=C(\omega)^2$, implying that $|C(\omega)|/C(\omega)=1$. Quadratic reciprocity follows. □

4. Heisenberg Groups and The Fourier Transform Theorem

Now, we prove Theorem 2.2. The idea of the proof will be to turn a certain identity at the level of the Heisenberg group into the Fourier transform identity. We start by introducing some more notation. This sections follows the presentation of Weil's paper [6], and also the first chapter of [4].

4.1. The group $\mathrm{Sp}(G)$.

We define a bicharacter $F : (G \times G^*) \times (G \times G^*) \to \mathbb{T}$ by the formula

$$F((x_1, x_1^*), (x_2, x_2^*)) = x_2^*(x_1).$$

An automorphism $\sigma : G \times G^* \to G \times G^*$ is said to be *symplectic* if σ preserves the bicharacter $F(z_1, z_2)F(z_2, z_1)^{-1}$. We write $\mathrm{Sp}(G)$ for the group of all symplectic automorphisms.

We can write a matrix for σ as

$$\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\alpha : G \to G, \beta : G \to G^*, \gamma : G^* \to G$, and $\delta : G^* \to G^*$ are morphisms making

$$(x, x^*)\sigma = (x, x^*) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (x\alpha + x^*\gamma, x\beta + x^*\delta)$$

true.

4.2. Heisenberg groups.

Heisenberg groups arise in trying to find representations of G and related groups.

It's easy to get a representation of G on $L^2(G)$: just define

$$R(g)\Phi(x) = \Phi(x + g),$$

and then you have a unitary representation. We can also define a unitary representation of G^* on $L^2(G)$, as

$$S(g^*)\Phi(x) = g^*(x)\Phi(x).$$

Here, the representation is unitary because $|g^*(x)| = 1$ for all $x \in X$.

It would be nice to put these together to get a representation of $G \times G^*$ in $L^2(G)$, but alas $R(g), S(g^*)$ don't commute; in fact we have the easily derived relation

$$R(g)S(g^*) = g^*(g)S(g^*)R(g). \tag{4.1}$$

This relation allows us to get a representation of a group closely related to $G \times G^*$. Namely, let $A(G) = G \times G^* \times \mathbb{T}$ be endowed with the product topology, and the group law

$$(g, g^*, t)(h, h^*, s) = (g + h, g^* + h^*, h^*(g)ts).$$

$A(G)$ is said to be a *Heisenberg group*, and has a natural unitary representation $U : A(G) \to \mathrm{Aut}(L^2(G))$ coming from (4.1) given by

$$U(g, g^*, t) = tS(g^*)R(g).$$

For brevity, we will write $U(g, g^*) = S(g^*)R(g)$.

We denote by $\mathbf{A}(G)$ for the image of U in $\mathrm{Aut}(L^2(G))$. We note U gives an isomorphism $\mathbf{A}(G) \cong A(G)$, with the isomorphism holding in the category of topological groups if we endow $\mathrm{Aut}(L^2(G))$ with the strong operator topology.

4.3. **Automorphisms of $A(G)$.** Set $B(G) = \mathrm{Aut}(A(G))$. Theorem 2.2 will come from a certain relationship between automorphisms of $A(G)$, which is why $B(G)$ is useful for us to consider.

An automorphism $s \in B(G)$ induces an automorphism on the center of $A(G)$, which is just the factor $\mathbb{T}$, and hence s also induces an automorphism of $A(G)/\mathbb{T} = G \times G^*$.

We will focus on the subgroup $B_0(G)$ of automorphisms s which are trivial on the center.

If $s \in B_0(G)$, then

$$(w,t)s = [(w,1)(0,t)]s = (w,1)s \cdot (0,t)s = (w\sigma, f(w)t)$$

for σ the induced automorphism of $G \times G^*$, and $f : G \times G^* \to \mathbb{T}$ some continuous map. We can thus identify an element $s \in B_0(G)$ by the pair (σ, f).

We have, for F the operator defined in Section 4.1,

$$\begin{aligned}((w_1+w_2)\sigma, f(w_1+w_2)) &= (w_1+w_2, 1)s \\ &= [(w_1,1)(w_2, F(w_1,w_2)^{-1})]s \\ &= (w_1\sigma, f(w_1)) \cdot (w_2\sigma, F(w_1,w_2)^{-1} f(w_2)) \\ &= ((w_1+w_2)\sigma, F(w_1\sigma, w_2\sigma)F(w_1,w_2)^{-1} f(w_1) f(w_2))\end{aligned}$$

and so we get the law

$$f(w_1+w_2) = F(w_1\sigma, w_2\sigma)F(w_1,w_2)^{-1} f(w_1) f(w_2). \tag{4.2}$$

In particular, by swapping w_1, w_2 we derive

$$F(w_1\sigma, w_2\sigma)F(w_1,w_2)^{-1} = F(w_2\sigma, w_1\sigma)F(w_2,w_1)^{-1}$$

so that σ is symplectic.

Thus, by sending $s = (\sigma, f) \in B_0(G)$ to $\sigma \in \mathrm{Sp}(G)$, we get a map $B_0(G) \to \mathrm{Sp}(G)$. It's easy to check that this is a morphism of groups, since in terms of pairs (σ, f), the group law on $B_0(G)$ can be written as

$$(\sigma_1, f_1) \cdot (\sigma_2, f_2) = (\sigma_2 \circ \sigma_1, f_1 \cdot (f_2 \circ \sigma_1)),$$

where this group law follows from expanding

$$(w,t)(\sigma_1, f_1)(\sigma_2, f_2) = (w\sigma_1, f_1(w)t)(\sigma_2, f_2) = (w\sigma_1\sigma_2, f_2(w\sigma_1)f_1(w)t).$$

4.4. **Matrix decompositions in $B_0(G)$.** We study more closely the structure of the $s \in B_0(G)$. Write $s = (\sigma, f)$ and expand σ as a matrix

$$\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

as we did in Section 4.1.

If $\gamma : G^* \to G$ is an isomorphism, then

$$d_0'(\gamma) = \left(\begin{pmatrix} 0 & -\gamma^{*-1} \\ \gamma & 0 \end{pmatrix}, (u, u^*) \mapsto \overline{u^*(u)} \right)$$

belongs to $B_0(G)$.

If f is a bicharacter and $\rho : G \to G^*$ is the symmetric morphism associated to f, then

$$t_0(f) = \left(\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}, f \right)$$

also lies in $B_0(G)$.

Now, suppose that you have a character of degree two $f : G \to \mathbb{T}$ whose associated morphism $\rho : G \to G^*$ is an isomorphism. Define

$$f'(x^*) = f(\rho^{-1}(x^*)).$$

Remark 4.3. The expression f' appears in Theorem 2.2. Our goal is to relate $\widehat{f}$ and f'.

Consider the pair

$$s = \left(\begin{pmatrix} 1 & 0 \\ \rho^{-1} & 1 \end{pmatrix}, (u, u^*) \mapsto f'(u^*) \right).$$

The compatibility constraint (4.2) is satisfied, as for $w_1 = (u_1, u_1^*), w_2 = (u_2, u_2^*)$ we have

$$\begin{aligned} F\left(w_1 \begin{pmatrix} 1 & 0 \\ \rho^{-1} & 1 \end{pmatrix}, w_2 \begin{pmatrix} 1 & 0 \\ \rho^{-1} & 1 \end{pmatrix} \right) F(w_1, w_2)^{-1} f'(u_1^*) f'(u_2^*) &= u_2^*(u_1 - u_1^*\rho^{-1}) u_2^*(-u_1) f'(u_1^*) f'(u_2^*) \\ &= u_2^*(-u_1^*\rho^{-1}) f(-u_1^*\rho^{-1}) f(-u_2^*\rho^{-1}) \\ &= u_2^*(-u_1^*\rho^{-1}) \cdot f(-u_1^*\rho^{-1} - u_2^*\rho^{-1}) \cdot \rho(u_2^*\rho^{-1})(u_1^*\rho^{-1}) \\ &= f'(u_1^* + u_2^*) \cdot u_2^*(-u_1^*\rho^{-1}) \cdot u_2^*(u_1^*\rho^{-1}) \\ &= f'(u_1^* + u_2^*). \end{aligned}$$

Hence $s \in B_0(G)$. We will write s in two different ways, which will be key to our proof of Theorem 2.2. First, we get the decomposition

$$s = t_0(f) d_0'(\rho^{-1}) t_0(f),$$

since, using that $\rho^* = \rho$ (after identifying G with its double dual in the canonical way)

$$\begin{aligned} t_0(f) d_0'(\rho^{-1}) t_0(f^-) &= t_0(f) \left(\begin{pmatrix} 0 & -\rho^* \\ \rho^{-1} & 0 \end{pmatrix}, (u, u^*) \mapsto u^*(-u) \right) \left(\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}, f \right) \\ &= \left(\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}, f \right) \left(\begin{pmatrix} 1 & -\rho \\ \rho^{-1} & 0 \end{pmatrix}, (u, u^*) \mapsto u^*(-u) f(u^*\rho^{-1}) \right) \\ &= \left(\begin{pmatrix} 1 & 0 \\ \rho^{-1} & 1 \end{pmatrix}, (u, u^*) \mapsto f(u) \cdot (u\rho + u^*)(-u) \cdot f(u + u^*\rho^{-1}) \right). \end{aligned}$$

Thus, the verification boils down to showing

$$f(u) \cdot (u\rho + u^*)(-u) \cdot f(u + u^*\rho^{-1}) = f'(u^*).$$

Weil gives a proof of this in general, but a quick algebraic proof can be given assuming that G admits a map $\frac{1}{2} : G \to G$ which has $\frac{1}{2} \circ \frac{1}{2} = 1$, for 1 the identity. This is true in our above use case (since number fields do not have characteristic 2), and with this assumption we may write

$f(x) = \rho(u)(\frac{1}{2}u)$ so that

$$\begin{aligned}
f(u)\cdot(u\rho+u^*)(-u)\cdot f(u+u^*\rho^{-1}) &= \rho(u)\left(\frac{1}{2}u\right)\cdot(u\rho)(-u)\cdot u^*(-u)\cdot(u\rho+u^*)\left(\frac{1}{2}u+\frac{1}{2}u^*\rho^{-1}\right)\\
&= \rho(u)\left(-\frac{1}{2}u\right)\cdot u^*(-u)\cdot\rho(u)\left(\frac{1}{2}u\right)\cdot u^*\left(\frac{1}{2}u\right)\cdot u^*\left(\frac{1}{2}u\right)\cdot u^*\left(\frac{1}{2}u^*\rho^{-1}\right)\\
&= u^*\left(\frac{1}{2}u^*\rho^{-1}\right)\\
&= \rho(u^*\rho^{-1})\left(\frac{1}{2}u^*\rho^{-1}\right)\\
&= f(u^*\rho^{-1})\\
&= f'(u).
\end{aligned}$$

A similarly gruesome computation shows

$$s = d_0'(\rho^{-1})t_0(f^{-1})d_0'(-\rho^{-1}),$$

for $f^{-1}(x) = f(x)^{-1}$, i.e. the reciprocal and not the literal inverse function.

Therefore we have the relation

$$t_0(f)d_0'(\rho^{-1})t_0(f^-) = d_0'(\rho^{-1})t_0(f^{-1})d_0'(-\rho^{-1}).$$

Noting that $d_0'(-\rho^{-1})d_0'(\rho^{-1})$ is the identity, we find

$$d_0'(-\rho^{-1})t_0(f)d_0'(\rho^{-1})t_0(f) = t_0(f^{-1})d_0'(-\rho^{-1}). \tag{4.4}$$

This relation will ultimately turn into our Fourier transform equation. But at the moment, this relationship is true at the level of $B(G)$, which is an automorphism of $A(G)$. In order for it to say something about the Fourier transform, we need to lift this relation to be about operators on $L^2(G)$. As a consequence, we need to somehow interpret $B_0(G)$ as a subgroup of $\mathrm{Aut}(L^2(G))$.

Because $A(G) \cong \mathbf{A}(G) \leq \mathrm{Aut}(L^2(G))$, the way to view $B_0(G)$ as a subgroup of $\mathrm{Aut}(L^2(G))$ will be for us to identify $B_0(G)$ will *inner* automorphisms of $L^2(G)$.

4.5. **Inner Automorphisms of $L^2(G)$.** Define $\mathbf{B}_0(G)$ to be the normalizer of $\mathbf{A}(G)$ in $L^2(G)$. If $\mathbf{s} \in \mathbf{B}_0(X)$, then define $\pi_0(\mathbf{s})$ to be the conjugation by $\mathbf{s}$ automorphism on $\mathbf{A}(G) \cong A(G)$. Thus, $\pi_0 : \mathbf{B}_0(G) \to \mathrm{Aut}(A(G)) \cong B(G)$. In fact, the image of π_0 is contained in $B_0(G)$ because the operators $U(0,t)$ are all just scalar multiplications, and hence commute with $\mathbf{s}$, so conjugation by $\mathbf{s}$ must leave them in tact.

In general there's no section of π_0. However, we can define sections of d_0, t_0, and d_0'. These allow us to lift (4.4), even if we cannot lift a generic relation.

Specifically, $d_0 : \mathrm{Aut}(G) \to B_0(G)$ has a section $\mathbf{d}_0 : \mathrm{Aut}(G) \to \mathbf{B}_0(G)$ given by

$$\mathbf{d}_0(\alpha)\Phi(x) = |\alpha|^{1/2}\Phi(x\alpha).$$

This formula is not hard to divine: the point is that $d_0(\alpha)$ should "apply α" to the G component of something in $A(G)$, and this is just the lift of that to $L^2(G)$; the factor of $|\alpha|^{1/2}$ is only present so our operator is unitary.

To check that this is a section of d_0, note that $\mathbf{d}_0(\alpha)$ conjugates a general element $U(u, u^*, t) \in \mathbf{A}(G)$ as

$$\begin{aligned}\mathbf{d}_0(\alpha)^{-1}U(u,u^*,t)\mathbf{d}_0(\alpha)\Phi &= |\alpha|^{1/2}\cdot \mathbf{d}_0(\alpha^{-1})U(u,u^*,t)(x\mapsto \Phi(x\alpha))\\ &= t|\alpha|^{1/2}\cdot \mathbf{d}_0(\alpha^{-1})(x\mapsto \Phi(u+x\alpha)u^*(x\alpha))\\ &= x\mapsto t\Phi(u\alpha^{-1}+x)u^*(x)\\ &= U(u\alpha^{-1},u^*,t)\Phi,\end{aligned}$$

and so indeed $\pi_0\mathbf{d}_0 = d_0$.

In a similar vein, one can construct sections

$$\mathbf{t}_0(f)\Phi(x) = \Phi(x)f(x),$$

$$\mathbf{d}'_0(\gamma)\Phi(x) = |\gamma|^{-1/2}\widehat{\Phi}(-x\gamma^{*-1}),$$

where f is a character of G of second degree and $\gamma : G^* \to G$ is an isomorphism.

Define

$$\mathbf{s} = \mathbf{d}'_0(-\rho^{-1})\mathbf{t}_0(f)\mathbf{d}'_0(\rho^{-1})\mathbf{t}_0(f^-),$$

$$\mathbf{s}' = \mathbf{t}_0(f^{-1})\mathbf{d}'_0(-\rho^{-1}).$$

We know from (4.4) that $\pi_0(\mathbf{s}) = \pi_0(\mathbf{s}')$. Thus, we need to do two things: understand $\ker \pi_0$, and understand what $\mathbf{s}$ and $\mathbf{s}'$ do.

We start by seeing what these operators do. The complicated formulas can, fortunately, be greatly simplified. For $\mathbf{s}'$, write

$$\begin{aligned}\mathbf{s}'\Phi &= \mathbf{t}_0(f^{-1})\mathbf{d}'_0(-\rho^{-1})\Phi\\ &= |\rho|^{1/2}\mathbf{t}_0(f^{-1})[x\mapsto \widehat{\Phi}(x\rho)]\\ &= x\mapsto |\rho|^{1/2}f^{-1}(x)\widehat{\Phi}(x\rho).\end{aligned}$$

Simplifying $\mathbf{s}$ is a bit of a longer task. First observe

$$\begin{aligned}\mathbf{s}\Phi &= \mathbf{d}'_0(-\rho^{-1})\mathbf{t}_0(f)\mathbf{d}'_0(\rho^{-1})\mathbf{t}_0(f^-)\Phi\\ &= \mathbf{d}'_0(-\rho^{-1})\mathbf{t}_0(f)\mathbf{d}'_0(\rho^{-1})(f^-\Phi)\\ &= |\rho|^{1/2}\mathbf{d}'_0(-\rho^{-1})\mathbf{t}_0(f)(x\mapsto \widehat{f^-\Phi}(-x\rho)).\end{aligned}$$

Set $\Psi(x) = \widehat{f^-\Phi}(-x\rho)$, so that

$$\begin{aligned}\mathbf{s}\Phi &= |\rho|^{1/2}\mathbf{d}'_0(-\rho^{-1})\mathbf{t}_0(f)\Psi\\ &= |\rho|^{1/2}\mathbf{d}'_0(-\rho^{-1})(x\mapsto f(x)\Psi(x))\\ &= x\mapsto |\rho|\widehat{f\Psi}(x\rho).\end{aligned}$$

Now, we may compute

$$\begin{aligned}
\widehat{f\Psi}(x\rho) &= \int_G f(g)\Psi(g)\cdot(x\rho)(g)\,dg \\
&= \int_G\int_G f(g)f(-h)\Phi(h)\cdot(-g\rho)(h)\cdot(x\rho)(g)\,dhdg \\
&= \int_G\int_G f(g-h)\Phi(h)\cdot(x\rho)(g)\,dhdg \\
&= \int_G [f*\Phi](g)\cdot(x\rho)(g)\,dg \\
&= \widehat{f*\Phi}(x\rho).
\end{aligned}$$

Therefore

$$\mathbf{s}\Phi(x) = |\rho|\widehat{f*\Phi}(x\rho). \tag{4.5}$$

So now we know that $\pi_0\mathbf{s} = \pi_0\mathbf{s}'$, and we have explicit expressions for $\mathbf{s}, \mathbf{s}'$. To relate these expressions, we thus just need to compute $\ker\pi_0$.

Theorem 4.6. $\ker\pi_0 \cong \mathbb{T}$, *and more specifically* $\ker\pi_0$ *consists of all the unitary operators of the form* $\Phi \mapsto t\Phi$ *for* $t \in \mathbb{T}$ *a scalar.*

Proof. $\ker\pi_0$ is precisely the centralizer of $\mathbf{A}(G)$ in $\mathrm{Aut}(L^2(G))$. It's clear that constants belong to the centralizer, and so we just show that they make up all of the centralizer. Suppose then that $\mathbf{s}$ lies in the centralizer of $\mathbf{A}(G)$.

It's a general theorem of harmonic analysis that representations of a group like $A(G)$ correspond bijectively to representations of its algebra $C_c(A(G))$ of compactly supported continuous functions under convolution. We will use the idea of that theorem, though we won't need the theorem itself.

Namely, take $\phi \in C_c(A(G))$. Then we may define $U(\phi) : L^2(G) \to L^2(G)$ as

$$U(\phi)\Phi(x) = \int_{A(G)} U(z)\Phi(x)\cdot\phi(z)\,dz.$$

Define $k_\phi : G\times G \to \mathbb{C}$ as

$$k_\phi(x, x+u) = \int_{\mathbb{T}}\int_{G^*} \phi(u, u^*, t)\cdot tu^*(x)\,du^*dt.$$

We may write $U(\phi)$ as the integral operator

$$U(\phi)\Phi(x) = \int_G k_\phi(x,y)\Phi(y)\,dy.$$

By Plancherel's theorem we can check that the mapping $\phi \mapsto k_\phi$ is an isometry, and hence extends from $C_c(A(G))$ to $L^2(A(G))$. Using Fourier inversion, we can construct an inverse mapping.

Since $\mathbf{s}$ lies in the centralizer of $\mathbf{A}(G)$, $\mathbf{s}$ commutes with every $U(z)$, and hence commutes with every operator $U(\phi)$. Therefore, by the above noticed fact that the operators $U(\phi)$ are dense in the space of integral transform operators on $L^2(G)$, we find that for any kernel $K \in L^2(G\times G)$, the integral operator

$$I_K\Phi(x) = \int_G K(x,y)\Phi(y)\,dy$$

commutes with $\mathbf{s}$.

Now we have our problem: there are a lot of integral operators. In particular, let $K(x,y) = P(x)\overline{Q(y)}$ be separable for $P, Q \in L^2(G)$. Then

$$I_K\Phi(x) = \int_G P(x)\overline{Q(y)}\Phi(y)\,dy = P(x)\langle \Phi, Q\rangle .$$

As $\mathbf{s}$ and I_K commute, we thus find that the function

$$x \mapsto P(x)\langle \mathbf{s}\Phi, Q\rangle = \langle P(x)\mathbf{s}\Phi, Q\rangle$$

is the same as the function

$$x \mapsto \langle \Phi, Q\rangle \cdot (\mathbf{s}P)(x) = \langle (\mathbf{s}P)(x)\Phi, Q\rangle .$$

As this holds for every choice of P, Q, $\mathbf{s}$ must be multiplication by a constant. Since the operator is unitary, that constant must belong to $\mathbb{T}$, and so the theorem follows. $\square$

Since $\pi_0\mathbf{s} = \pi_0\mathbf{s}'$, and the kernel of π_0 is $\mathbb{T}$, the operators $\mathbf{s}, \mathbf{s}'$ differ by multiplication by some factor $\gamma(f) \in \mathbb{T}$. In particular,

$$|\rho|\widehat{f * \Phi}(x\rho) = \gamma(f)|\rho|^{1/2} f^{-1}(x)\widehat{\Phi}(x\rho) \tag{4.7}$$

for every Φ. But this is exactly the second equation in Theorem 2.2. To get the first part, a transformation for $\widehat{f\Phi}$, is not so difficult from here, which we show as follows. Pick Φ_1 Schwartz, so that

$$[\widehat{f * \Phi_1}]\Phi = \widehat{f * \Phi_1} * \widehat{\Phi}.$$

Since, for $F(x^*) = f(x^*\rho^{-1})^{-1}$ we have

$$\widehat{f * \Phi_1}(x^*) = \gamma(f)|\rho|^{-1/2}F(x^*)\widehat{\Phi_1}(x^*),$$

by our above derivation, if we let Φ_1 vary over an approximate identity (that is, a net acting like an identity element of $C_c(G)$ under convolution; an LCA group always admits such a net) then

$$[\widehat{f * \Phi_1}]\Phi = \widehat{f * \Phi_1} * \widehat{\Phi} = \gamma(f)|\rho|^{-1/2}[F\widehat{\Phi_1} * \widehat{\Phi}$$

becomes

$$\widehat{f\Phi} = \gamma(f)|\rho|^{1/2}[F * \widehat{\Phi}],$$

concluding our verification of Theorem 2.2.

5. Acknowledgements

The MathOverflow thread https://mathoverflow.net/questions/120067 was the inspiration for this paper; Paul Garret's answer on that thread in particular shaped our presentation of the Poisson summation of Weil's Θ functions, as mentioned in more detail in Remark 2.6.

Michael Berg's book [1], mentioned in the MathOverflow thread, was very helpful for compiling sources related to Weil and Hecke's proofs of quadratic reciprocity.

Last but certainly not least, thanks to Matthew Emerton who helped me learn enough number theory for Weil's writing to make sense and, perhaps more importantly, helped me to not be scared of reading old papers.

References

[1] Michael C. Berg. *The Fourier Analytic Proof of Quadratic Reciprocity*. Wiley-Interscience, 2000.

[2] Paul Garrett. *Quadratic reciprocity (after Weil)*. 2010. URL: https://www-users.cse.umn.edu/~garrett/m/v/quad_rec.pdf.

[3] Erich Hecke. *Lectures on the Theory of Algebraic Numbers*. Trans. by George U. Brauer and Jay R. Goldman. Springer-Verlang, 1981.

[4] Jun-ichi Igusa. *Theta Functions*. Springer-Verlang, 1972.

[5] Anders Karlsson. "Applications of heat kernels on abelian groups". In: *Number Theory, Analysis and Geometry: In Memory of Serge Lang* (2012), pp. 307–320.

[6] André Weil. "Sur certains groupes d'opérateurs unitaires". In: *Acta Mathematica* 111 (1964), pp. 143–211. DOI: https://doi.org/10.1007/BF02391012.