QUADRATIC RECIPROCITY, AFTER WEIL

The character associated to a quadratic extension field K of $\mathbb{Q}$,

$$\chi : \mathbb{Z}^+ \longrightarrow \mathbb{C}, \quad \chi(n) = (\mathrm{disc}(K)/n) \quad \text{(Jacobi symbol)},$$

is in fact a Dirichlet character; specifically its conductor is $|\mathrm{disc}(K)|$. This fact encodes basic quadratic reciprocity from elementary number theory, phrasing it in terms that presage class field theory.

This writeup discusses Hilbert quadratic reciprocity in the same spirit. Let k be a number field, and let K be a quadratic extension field of k. We show that a global quadratic norm residue character,

$$\nu_{K/k} : \mathbb{A}_k^\times \longrightarrow \{\pm 1\},$$

is a *Hecke character*, i.e., it is trivial on $k^\times$. This fact encodes the Hilbert quadratic reciprocity rule, i.e., the product formula for quadratic Hilbert symbols. The reciprocity rule in turn encodes elementary quadratic reciprocity statements, including basic quadratic reciprocity.

The ideas here work in the geometric (function field) case as well, but for simplicity we discuss only number fields.

This writeup is modeled on a writeup by Paul Garrett,

`http://www.math.umn.edu/~garrett/m/v/quad_rec_02.pdf` .

The Weil representation appears in

> A. Weil, *Sur certaines d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211,

and Hilbert quadratic reciprocity in

> D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresber. Deutsch. Math. Verein. **4** (1897), 175–546.

Contents

1. The additive character of the rational adeles

For each finite rational prime p define a corresponding local character,

$$\mathbf{e}_p : \mathbb{Q}_p \longrightarrow \mathbb{T}, \quad \mathbf{e}_p(x) = \exp(2\pi i x).$$

The defining formula is meaningful on the dense subset $\mathbb{Z}[1/p]$ of $\mathbb{Q}_p$, from which it extends continuously to all of $\mathbb{Q}_p$. Also define an Archimedean character,

$$\mathbf{e}_\infty : \mathbb{R} \longrightarrow \mathbb{T}, \quad \mathbf{e}_\infty(x) = \exp(-2\pi i x).$$

The resulting rational adele character is

$$\mathbf{e}_\mathbb{A} : \mathbb{A} \longrightarrow \mathbb{T}, \quad \mathbf{e}_\mathbb{A} = \bigotimes_{p \in \mathbf{f} \cup \infty} \mathbf{e}_p.$$

The adele character is trivial on $\mathbb{Q}$ (diagonally embedded in $\mathbb{A}$). Indeed, "partial fractions" says that

$$\mathbb{Q} = \sum_{p \in \mathbf{f}} \mathbb{Z}[1/p] \quad \text{(indirect sum)},$$

and on each summand $\mathbf{e}_\mathbb{A} = \mathbf{e}_p \otimes \mathbf{e}_\infty$ is trivial.

2. The additive character of the k-adeles

Let k be a number field. For each place v of k, divisible by a unique rational place p (possibly $p = \infty$), define

$$\psi_v : k_v \longrightarrow \mathbb{T}, \quad \psi_v = \mathbf{e}_p \circ \mathrm{Tr}_{k_v/\mathbb{Q}_p}.$$

If v is non-Archimedean then the kernel of ψ_v is the local inverse-different $\delta^{-1}_{k_v/\mathbb{Q}_p}$. The resulting k-adele character is

$$\psi : \mathbb{A}_k \longrightarrow \mathbb{T}, \quad \psi = \mathrm{e}_\mathbb{A} \circ \mathrm{Tr}_{\mathbb{A}_k/\mathbb{A}} = \bigotimes_v \psi_v.$$

Since $\mathrm{Tr}_{\mathbb{A}_k/\mathbb{A}}$ takes k to $\mathbb{Q}$, it follows that ψ is trivial on k. Here we tacitly use the fact that the global trace is the sum of the local traces, i.e., the following diagram commutes:

$$\begin{tikzcd} k \arrow[r] \arrow[d, "\mathrm{Tr}_{k/\mathbb{Q}}"'] & \mathbb{A}_k \arrow[d, "\mathrm{Tr}_{\mathbb{A}_k/\mathbb{A}}"] \\ \mathbb{Q} \arrow[r] & \mathbb{A} \end{tikzcd}$$

(Note: ψ can be constructed more conceptually by noting that a certain representation is one-dimensional. See Paul Garrett's pieces on dualities, linked from my page of number theory materials.)

3. The quadratic extension and desiderata

Let K be a quadratic extension of k. Let σ be the nontrivial automorphism of K over k. The trace from K to k,

$$\mathrm{Tr}_{K/k} : K \longrightarrow k, \quad \mathrm{Tr}_{K/k}(x) = x + x^\sigma,$$

defines a sequilinear symmetric pairing,

$$\langle\ ,\ \rangle : K \times K \longrightarrow k, \quad \langle x, y \rangle = \mathrm{Tr}_{K/k}(xy^\sigma).$$

Note that in particular,

$$\langle x, x\rangle = \mathrm{Tr}_{K/k}(\mathrm{N}_{K/k}(x)) = 2\mathrm{N}_{K/k}(x).$$

For each place v of k, define

$$K_v = K \otimes_k k_v.$$

Since $K = k(\sqrt{\alpha}) \approx k[X]/\langle X^2 - \alpha\rangle$, it follows that

$$K_v \approx k_v[X]/\langle X^2-\alpha\rangle = \begin{cases} k_v(\sqrt{\alpha}) & \text{if } \alpha \text{ is not a square in } k_v, \\ k_v \times k_v & \text{if it is,} \end{cases}$$

and σ extends to a nontrivial automorphism of K_v over k_v in either case. The local pairing is

$$\langle\ ,\ \rangle_v : K_v \times K_v \longrightarrow k_v, \quad \langle x, y\rangle_v = \mathrm{Tr}_{K_v/k_v}(xy^\sigma),$$

and again

$$\langle x, x\rangle_v = 2\mathrm{N}_{K_v/k_v}(x).$$

(In the case $K_v = k_v \times k_v$, the smaller field k_v embeds diagonally, so that $\mathrm{Tr}(xy^\sigma) = \mathrm{Tr}((x_1, x_2)(y_2, y_1)) = \mathrm{Tr}((x_1y_2, x_2y_1)) = x_1y_2 + x_2y_1$ and $\mathrm{N}(x) = (x_1, x_2)(x_2, x_1) = x_1x_2$ under the identification of k_v with its embedded image.)

The local Fourier transform is

$$\mathcal{F}f(y) = \int_{K_v} \overline{\psi}_v(\langle x, y\rangle_v)f(x)\,dx,$$

with the Haar measure normalized so that $\mathcal{F}\mathcal{F}f(x) = f(-x)$.

Lemma 1. *Let v be non-Archimedean. Then for any Schwartz–Bruhat function f on K_v and any smooth function ϕ on K_v,*

$$\mathcal{F}(\phi f) = \mathcal{F}\phi * \mathcal{F}f.$$

Granting convergence, the fact that the Fourier transform of the product is the convolution of the Fourier transforms is purely formal, so the point of interest is that ϕ need only be smooth. If ϕ were Schwartz–Bruhat then the lemma would merely state a standard result.

Proof. Let 1_X denote the characteristic function of any subset X of K_v. The assertion

$$\phi = \lim_X (1_X\phi) \quad \text{(limit of tempered distributions)}$$

refers to a limit over increasing balls X, and the limit is taken in the weak dual topology. That is, for any Schwartz–Bruhat function g,

$$\phi(g) = \lim_X (1_X\phi)(g) \quad \text{(limit of complex numbers).}$$

Indeed, the limit is attained as soon as X contains the support of g. Also, the Fourier transform is a topological automorphism of the space of tempered distributions. Introduce two operators on Schwartz–Bruhat functions,

$$(mg)(y) = g(-y) \qquad \text{and} \qquad (T_xg)(y) = g(y + x).$$

Then the convolution of a tempered distribution and a Schwartz–Bruhat function is by definition

$$(u * g)(x) = u(T_{-x}mg), \quad x \in K_v.$$

This gives $u(mT_xg) = \int u(y)g(x-y)\,dy$ as desired if u itself is a smooth function. To avoid the variable, the formula is

$$u * g = u(T_{-\bullet}mg).$$

Now we can prove the lemma. Since the desired formula does hold when both functions are Schwartz–Bruhat, we have the third equality in

$$\mathcal{F}(\phi f) = \mathcal{F}(\lim_X 1_X\phi f) = \lim_X \mathcal{F}(1_X\phi f) = \lim_X(\mathcal{F}(1_X\phi) * \mathcal{F}f).$$

Next, by the definition of convolution,

$$\lim_X(\mathcal{F}(1_X\phi) * \mathcal{F}f) = \lim_X(\mathcal{F}(1_X\phi))(T_{-\bullet}m\mathcal{F}f).$$

Push the limit back through everything,

$$\lim_X(\mathcal{F}(1_X\phi))(T_{-\bullet}m\mathcal{F}f) = (\mathcal{F}\lim_X(1_X\phi))(T_{-\bullet}m\mathcal{F}f) = (\mathcal{F}\phi)(T_{-\bullet}mt\mathcal{F}f),$$

and then again by the definition of convolution,

$$(\mathcal{F}\phi)(T_{-\bullet}m\mathcal{F}f) = \mathcal{F}\phi * \mathcal{F}f.$$

The previous four displays combine to give the result. □

4. Weil's quadratic exponential distributions

Fix a place v of k. For any $t \in k_v^\times$ define a sort of t-dilated oscillation in the square of the variable,

$$\boxed{S_{t,v} : K_v \longrightarrow \mathbb{T}, \quad S_{t,v}(x) = \psi_v(\tfrac{1}{2}t\langle x, x\rangle_v) = \psi_v(t\,\mathrm{N}_{K_v/k_v}(x)).}$$

We also view $S_{t,v}$ as a tempered distribution,

$$S_{t,v}(f) = \int_{K_v} S_{t,v}(x)f(x)\,dx.$$

Before continuing, we argue that for non-Archimedean v, the integral

$$\int_{K_v} S_{t,v} = \lim_X \int_X S_{t,v} \quad \text{(limit over increasing balls)}$$

is in fact attained by all large enough X. Since K_v is a semisimple, 2-dimensional algebra over k_v and we are not in characteristic 2, the nondegenerate quadratic form N_{K_v/k_v} is diagonalizable over k_v,

$$\mathrm{N}_{K_v/k_v}(x) = a_1x_1^2 + a_2x_2^2.$$

Thus $S_{t,v}(x) = \psi_v(t\,\mathrm{N}_{K_v/k_v}(x)) = \psi_v(ta_1x_1^2)\psi_v(ta_2x_2^2)$ and consequently

$$\int_{K_v} S_{t,v}(x)\,dx = \int_{k_v} \psi_v(ta_1x_1^2)\,dx_1 \int_{k_v} \psi_v(ta_2x_2^2)\,dx_2,$$

and so, absorbing constants into t, it suffices to show that the integral

$$\int_{k_v} \psi_v(tx^2)\,dx$$

stabilizes over large enough balls.

Let ϖ_v be a uniformizer of $\mathcal{O}_v$. Let m and ℓ be large positive integers. Introduce a large shell of k_v and a small subgroup of $\mathcal{O}_v^\times$,

$$X_m = \varpi_v^{-m}\mathcal{O}_v^\times, \quad U_\ell = \exp(\varpi_v^\ell\mathcal{O}_v) = 1 + \varpi_v^\ell\mathcal{O}_v.$$

Thus U_ℓ acts on X_m. Normalize $\mu\mathcal{O}_v$ to 1 and compute

$$\int_{X_m} \psi_v(tx^2)\,dx = \int_{\mathcal{O}_v}\int_{X_m} \psi_v(tx^2)\,dx\,dz = \int_{\mathcal{O}_v}\int_{\exp(\varpi_v^\ell z)X_m} \psi_v(tx^2)\,dx\,dz$$
$$= \int_{\mathcal{O}_v}\int_{X_m} \psi_v(t\,\exp(\varpi_v^\ell z)^2 x^2)\,dx\,dz,$$

noting that $d(\exp(\varpi_v^\ell z)x) = dx$ since $|\exp(\varpi_v^\ell z)| = 1$. The argument of ψ_v in the previous integral is

$$t\,\exp(\varpi_v^\ell z)^2 x^2 = t(1+\varpi_v^\ell z + \mathrm{O}(\varpi_v^{2\ell} z^2))^2 x^2 = t(1+2\varpi_v^\ell z + \mathrm{O}(\varpi_v^{2\ell} z^2))x^2,$$

so that

$$\psi_v(t\,\exp(\varpi_v^\ell z)^2 x^2) = \psi_v(tx^2)\psi_v(2t\varpi_v^\ell z x^2)\psi_v(\mathrm{O}(t\varpi_v^{2\ell} z^2 x^2)).$$

Now, $\ker(\psi_v(t\bullet)) = \varpi_v^n\mathcal{O}_v$ where $n \in \mathbb{Z}$. If $2\ell - 2m \geq n$ then $\psi_v(\mathrm{O}(t\varpi_v^{2\ell} z^2 x^2)) = 1$ for all $x \in X_m$ and $z \in \mathcal{O}_v$, giving

$$\psi_v(t\,\exp(\varpi_v^\ell z)^2 x^2) = \psi_v(tx^2)\psi_v(2t\varpi_v^\ell z x^2),$$

and thus

$$\int_{X_m} \psi_v(tx^2)\,dx = \int_{\mathcal{O}_v}\int_{X_m} \psi_v(tx^2)\psi_v(2t\varpi_v^\ell z x^2)\,dx\,dz$$
$$= \int_{X_m} \psi_v(tx^2)\int_{\mathcal{O}_v} \psi_v(2t\varpi_v^\ell z x^2)\,dz\,dx.$$

If also $\mathrm{ord}_v(2) + \ell - 2m < n$ then for each $x \in X_m$, the character

$$\mathcal{O}_v \longrightarrow \mathbb{T}, \quad z \longmapsto \psi_v(2t\varpi_v^\ell z x^2)$$

is nontrivial, and the inner integral vanishes. Thus, given m, any ℓ such that $n/2 + m \leq \ell < n + 2m - \mathrm{ord}_v(2)$ will make the argument work.

(Note: The additive group structure of $\mathcal{O}_v$ and the multiplicative group structure of U_ℓ are both active in the proof. Because they don't interact directly, one could parametrize $\mathcal{O}_v \longrightarrow U_\ell$ by $z \mapsto 1 + \varpi_v^\ell z$ rather than use the exponential map, even though this parametrization is not a homomorphism. But the resulting argument, superficially a little simpler, is not natural or robust.)

Lemma 2. *Let v be non-Archimedean. Then the Fourier transform of $S_{t,v}$ is*

$$\mathcal{F}S_{t,v} = \int_{K_v} S_{t,v}\ \cdot\ S_{-t^{-1},v}.$$

As just explained, the integral attains its value over large enough balls X.

Proof. Let X be any compact subset of K_v and consider the truncation $1_X S_{t,v}$. Its Fourier transform is

$$\mathcal{F}(1_X S_{t,v})(y) = \int_X \overline{\psi}_v(\langle x,y\rangle_v) S_{t,v}(x)\,dx = \int_X \psi_v(t/2\langle x,x\rangle_v - \langle x,y\rangle_v)\,dx.$$

Complete the square,

$$t/2\langle x,x\rangle_v - \langle x,y\rangle_v = t/2\langle x - t^{-1}y, x - t^{-1}y\rangle_v - t^{-1}/2\langle y,y\rangle_v,$$

and the Fourier transform is now

$$\mathcal{F}(1_X S_{t,v})(y) = \int_X S_{t,v}(x - t^{-1}y)\,dx \cdot S_{-t^{-1},v}(y) = \int_{X - t^{-1}y} S_{t,v}(x)\,dx \cdot S_{-t^{-1},v}(y).$$

Now, $S_{t,v} = \lim_X (1_X S_{t,v})$ in the weak dual topology, and the Fourier transform is continuous, and for any given y we have $X - t^{-1}y = X$ if X is large enough, so altogether,

$$\mathcal{F}S_{t,v}(y) = \lim_X \mathcal{F}(1_X S_{t,v})(y) = \lim_X \int_X S_{t,v}(x)\,dx \cdot S_{-t^{-1},v}(y).$$

□

Lemma 3. *Let v be non-Archimedean or Archimedean. Then for any Schwartz–Bruhat function f on K_v,*

$$(S_{t,v} * f)(x) = S_{t,v}(x)\,\mathcal{F}(S_{t,v}f)(tx).$$

Proof. The readily-verified polarizing identity

$$S_{t,v}(x-y) = S_{t,v}(x)\overline{\psi}_v(\langle tx, y\rangle_v)S_{t,v}(y)$$

gives the result immediately,

$$(S_{t,v} * f)(x) = \int_{K_v} S_{t,v}(x-y)f(y)\,dy = S_{t,v}(x)\int_{K_v} \overline{\psi}_v(\langle tx, y\rangle_v)(S_{t,v}f)(y)\,dy.$$

□

5. The quadratic norm residue symbol

For any place v, non-Archimedean or Archimedean, define

$$\boxed{\nu_v : k_v^\times \longrightarrow \{\pm 1\}, \quad \nu_v(x) = \begin{cases} 1 & \text{if } K_v \text{ is a field and } x \in \mathrm{N}_{K_v/k_v}(K_v^\times), \\ -1 & \text{if } K_v \text{ is a field and } x \notin \mathrm{N}_{K_v/k_v}(K_v^\times), \\ 1 & \text{if } K_v \text{ is not a field.} \end{cases}}$$

We assert without proof that when K_v is a field, the subgroup $\mathrm{N}_{K_v/k_v}(K_v^\times)$ of $k_v^\times$ has index 2. Consequently, ν_v is a homomorphism.

The norm residue symbol captures the reduction of the integral of a dilated quadratic exponential distribution to the normalized case, as follows.

Lemma 4. *For any $t \in k_v^\times$,*

$$\int_{K_v} S_{t,v} = \nu_v(t)|t|_v^{-1}\int_{K_v} S_{1,v}.$$

As earlier, the integrals are taken over increasing balls, so that they stabilize if v is non-Archimedean.

Proof. If t is a norm, i.e., it takes the form $t = \mathrm{N}_{K_v/k_v}(x)$, then

$$\int_{K_v} S_{t,v}(y)\,dy = \int_{K_v} \psi_v(t\mathrm{N}_{K_v/k_v}(y))\,dy = |x|_{K_v}^{-1}\int_{K_v} \psi_v(\mathrm{N}_{K_v/k_v}(xy))\,d(xy).$$

But

$$|x|_{K_v} = |xx^\sigma|_{k_v} = |t|_{k_v},$$

and so the calculation has given the desired result in this case,

$$\int_{K_v} S_{t,v} = |t|_{k_v}^{-1}\int_{K_v} S_{1,v}.$$

If t is not a norm then K_v is a field. Let

$$\Theta = \ker(\mathrm{N}_{K_v/k_v}),$$

so that the norm is constant on orbits Θx in K_v, including the one-point orbit 0 that does not contribute to the integral anyway. Furthermore, the multiplicative group $\Theta\backslash K_v^\times$ (without the one-point orbit) is isomorphic to the index-2 subgroup $\mathrm{N}_{K_v/k_v}(K_v^\times)$ of norms in $k_v^\times$. To find the relation between the Haar measures, compute that for $x \in K_v^\times$ and $u = N_{K_v/k_v}(x) \in k_v^\times$,

$$du = |u|_{k_v}\, d^\times u = |xx^\sigma|_{k_v}\, d^\times(xx^\sigma) = |x|_{K_v} 2d^\times x = 2dx.$$

Thus, giving Θ measure 1 and halving du for convenience,

$$\begin{aligned}\int_{K_v} S_{t,v}(x)\,dx &= \int_{\Theta\backslash K_v}\int_\Theta \psi_v(t\,\mathrm{N}(\theta x))\,d\theta\,d\overline{x} = \int_{\Theta\backslash K_v} \psi_v(t\,\mathrm{N}(\overline{x}))\,d\overline{x} \\ &= \int_{\mathrm{N}(K_v^\times)} \psi_v(tu)\,du = |t|_v^{-1}\int_{t\,\mathrm{N}(K_v^\times)} \psi_v(u)\,du.\end{aligned}$$

Similarly,

$$\int_{K_v} S_{1,v}(x)\,dx = \int_{\mathrm{N}(K_v^\times)} \psi_v(u)\,du,$$

and so it suffices to show that

$$\int_{k_v} \psi_v(u)\,du = 0.$$

Since ψ_v is a nontrivial character on k_v, this is immediate. □

6. Global quadratic norm residue symbol reciprocity law

The global quadratic norm residue symbol is

$$\boxed{\nu_{K/k} : \mathbb{A}_k^\times \longrightarrow \{\pm 1\}, \quad \nu_{K/k} = \bigotimes_v \nu_v.}$$

Theorem 5. *The global quadratic norm residue symbol is a Hecke character.*

Proof. Introduce the global Weil quadratic exponential distribution,

$$\boxed{S_t : \mathbb{A}_K \longrightarrow \mathbb{T}, \quad S_t = \bigotimes_v S_{t,v}.}$$

Specifically,

$$S_t(x) = \prod_v S_{t,v}(x_v) = \prod_v \psi_v(t\,\mathrm{N}_{K_v/k_v}(x_v)) = \psi(t\,\mathrm{N}_{\mathbb{A}_K/\mathbb{A}_k}(x)),$$

so that in particular $S_t = 1$ on K by the usual commutative diagram encoding that the global norm is the product of the local norms,

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{A}_K \\ {\scriptstyle \mathrm{N}_{k/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{\mathbb{A}_K/\mathbb{A}_k}} \\ k & \longrightarrow & \mathbb{A}_k \end{array}$$

and by the fact that ψ is trivial on k.

Take any $t \in k^\times$ and any Schwartz–Bruhat function f on K. Then

$$\begin{aligned}
\sum_{x\in K} f(x) &= \sum_{x\in K} (S_t \cdot f)(x) && \text{since } S_t = 1 \text{ on } K \\
&= \sum_{x\in K} \mathcal{F}(S_t \cdot f)(x) && \text{by Poisson summation} \\
&= \sum_{x\in K} (\mathcal{F}S_t * \mathcal{F}f)(x) && \text{by Lemma 1} \\
&= \int_{\mathbb{A}_K} S_t \cdot \sum_{x\in K} (S_{-t^{-1}} * \mathcal{F}f)(x) && \text{by Lemma 2} \\
&= \int_{\mathbb{A}_K} S_t \cdot \sum_{x\in K} S_{-t^{-1}}(x)(S_{-t^{-1}} \cdot \mathcal{F}f)(tx) && \text{by Lemma 3} \\
&= \int_{\mathbb{A}_K} S_t \cdot \sum_{x\in K} \mathcal{F}f(tx) && \text{since } S_{-t^{-1}} = 1 \text{ on } K \\
&= \int_{\mathbb{A}_K} S_t \cdot \sum_{x\in K} \mathcal{F}f(x) && \text{changing variable} \\
&= \int_{\mathbb{A}_K} S_t \cdot \sum_{x\in K} f(x) && \text{by Poisson summation.}
\end{aligned}$$

By choosing a Schwartz–Bruhat function f so that the sum doesn't vanish we see that

$$\int_{\mathbb{A}_K} S_t = 1.$$

Using Lemma 4 and the idele product formula, compute

$$\int_{\mathbb{A}_K} S_t = \prod_v \int_{K_v} S_{t,v} = \prod_v \nu_v(t)|t|_v^{-1} \int_{K_v} S_{1,v} = \nu_{K/k}(t) \int_{\mathbb{A}_K} S_1,$$

Since both integrals equal 1, we have the result,

$$\nu_{K/k} = 1 \text{ on } k^\times.$$

(Note: The global calculation also uses Archimedean versions of lemmas that were established only for non-Archimedean places.) □

7. Hilbert quadratic reciprocity

Let v be a non-Archimedean or Archimedean place of k. The quadratic Hilbert symbol for any $a, b \in k_v$ is

$$(a,b)_v = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ for some } (x,y,z) \in k_v^3 - \{(0,0,0)\}, \\ -1 & \text{otherwise.} \end{cases}$$

Proposition 6. *Let $a, b \in k^\times$ be nonsquares. Let $K = k(\sqrt{b})$. Then the quadratic Hilbert symbol is the norm residue symbol at all places of k, non-Archimedean or Archimedean,*

$$(a,b)_v = \nu_v(a) \quad \textit{for all } v.$$

Consequently, the product formula for quadratic Hilbert symbols holds,

$$\prod_v (a,b)_v = 1.$$

Proof. We have

$$K_v = K \otimes_k k_v = \begin{cases} k_v(\sqrt{b}) & \text{if } b \text{ is not a square in } k_v, \\ k_v \times k_v & \text{if } b \text{ is a square in } k_v. \end{cases}$$

In the first case, the equation determining the Hilbert symbol has no solution with $x = 0$, so by homogeneity it becomes

$$a = z^2 - by^2 = \mathrm{N}_{K_v/k_v}(z + \sqrt{b}\, y).$$

Thus the Hilbert symbol is 1 exactly when a is a local norm. In the second case, the Hilbert symbol is 1 because b is a local square and the norm residue symbol is 1 because K_v is not a field. With the local equalities established, the product formula restates the fact that $\nu_{K/k}$ is trivial on $k^\times$. □

If either of $a, b \in k^\times$ is a square then $(a, b)_v = 1$ for all v, and the product formula is trivial. Still, in this case we can match the local data as well. Make the interpretations

$$K = k[X]/\langle X^2 - b\rangle \quad \text{and} \quad K_v = K \otimes_k k_v = k_v[X]/\langle X^2 - b\rangle \approx k_v \times k_v.$$

Thus $\nu_v(a) = 1$ for all v and again the quadratic Hilbert symbol agrees with the norm residue symbol everywhere.

8. Quadratic reciprocity

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$. For any $x \in \mathcal{O}_k$, define a quadratic symbol

$$\left(\frac{x}{\mathfrak{p}}\right)_2 = \begin{cases} 1 & \text{if } x + \mathfrak{p} \text{ is a square in } (\mathcal{O}_k/\mathfrak{p})^\times, \\ -1 & \text{if } x + \mathfrak{p} \text{ is a nonsquare in } (\mathcal{O}_k/\mathfrak{p})^\times, \\ 0 & \text{if } x + \mathfrak{p} \text{ is zero in } \mathcal{O}_k/\mathfrak{p}, \end{cases}$$

and define

$$\left(\frac{x}{\pi}\right)_2 = \left(\frac{x}{\mathfrak{p}}\right)_2 \quad \text{for any generator } \pi \text{ of } \mathfrak{p}.$$

A prime ideal of $\mathcal{O}_k$ is *odd* if it does not divide (2).

Theorem 7. (*Main part of quadratic reciprocity*) *Let π and ϖ generate distinct odd prime ideals of $\mathcal{O}_k$. Then*

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \prod_{v \mid 2\cdot\infty} (\pi, \varpi)_v.$$

(*Supplementary part of quadratic reciprocity*) *Let π generate an odd prime ideal of $\mathcal{O}_k$, and let α be coprime to π, i.e., $\alpha + (\pi) \in (\mathcal{O}_k/(\pi))^\times$. Then*

$$\left(\frac{\alpha}{\pi}\right)_2 = \prod_{v \mid 2\alpha\cdot\infty} (\pi, \alpha)_v.$$

Proof. Let $\mathfrak{p} = (\pi)$ and let v be the corresponding place of k. If the Hilbert symbol $(\pi, \varpi)_v$ is 1 then

$$\pi x^2 + \varpi y^2 = z^2, \quad x, y, z \in k_v, \text{ not all } 0.$$

If $x = 0$ then ϖ is a square in $k_v^\times$, hence in $k^\times$, hence in $(\mathcal{O}_k/\mathfrak{p})^\times$ since $(\varpi) \neq (\pi)$, and so certainly the quadratic symbol $(\varpi/\pi)_2$ is 1. Otherwise $\mathrm{ord}_\pi(\pi x^2)$ is odd while $\mathrm{ord}_\pi(\varpi y^2)$ and $\mathrm{ord}_\pi(z^2)$ are even or infinite, so both must be even and hence equal and less than $\mathrm{ord}_\pi(x)$. After canceling powers of π we thus get

$$\pi^{2e+1}\tilde{x}^2 + \varpi\tilde{y}^2 = \tilde{z}^2, \quad \pi \nmid \tilde{x}\tilde{y}\tilde{z}.$$

Take the displayed equality modulo (π) to see that again the quadratic symbol $(\varpi/\pi)_2$ is 1.

Still with $\mathfrak{p} = (\pi)$, suppose now conversely that the quadratic symbol $(\varpi/\pi)_2$ is 1. Thus ϖ is a nonzero square in $(\mathcal{O}_k/\mathfrak{p})^\times$, and so by Hensel's Lemma ϖ is a nonzero square in $k_v^\times$. Consequently the Hilbert symbol $(\pi,\varpi)_v$ is 1. Thus $(\pi,\varpi)_v = (\varpi/\pi)_2$, and similarly $(\varpi,\pi)_w = (\pi/\varpi)_2$ where w is the place of k corresponding to (ϖ).

Next let $\mathfrak{p}$ be an odd prime ideal of $\mathcal{O}_k$ other than (π) and (ϖ), and let v be the corresponding place of k. Let $K_v = k_v(\sqrt{\varpi})$, so that $(\pi,\varpi)_v = \nu_v(\pi)$. If ϖ is a square in k_v then $\nu_v(\pi) = 1$ because $K_v = k_v \times k_v$. If ϖ is not a square in k_v then K_v is unramified over k_v because $\mathfrak{p}$ is odd. Thus the norm surjects to $\mathcal{O}_v^\times$ (because the image has index 2 in $k_v^\times$ and contains only units times even powers of ϖ), giving

$$\pi = \mathrm{N}_{K_v/k_v}(z + y\sqrt{\varpi}) = z^2 - \varpi y^2, \quad y,z \in k_v.$$

So again $(\pi,\varpi)_v = 1$.

Thus by Hilbert quadratic reciprocity,

$$1 = \prod_v (\pi,\varpi)_v = (\pi/\varpi)_2(\varpi/\pi)_2 \prod_{v\mid 2\cdot\infty} (\pi,\varpi)_v,$$

and the main part of quadratic reciprocity follows. The supplementary part is left as an exercise. □

For the simplest case, let p and q be odd rational primes. We have shown that

$$\left(\frac{p}{q}\right)_2 \left(\frac{q}{p}\right)_2 = (p,q)_2(p,q)_\infty.$$

Clearly the equation

$$px^2 + qy^2 = z^2$$

has nonzero real solutions (x,y,z), and so $(p,q)_\infty = 1$. As for whether the equation has nonzero 2-adic solutions, if $p = 1\,(8)$ then Hensel's Lemma lifts the solution $(1,0,1)$ from $\mathbb{Z}/8\mathbb{Z}$ to $\mathbb{Z}_2$, and similarly if $q = 1\,(8)$, while if $p = q = 5\,(8)$ then Hensel's Lemma lifts the solution $(1,2,1)$. Thus $(p,q)_2 = 1$ if either of p,q equals 1 modulo 4. Conversely, if the displayed equation has a nonzero solution in $\mathbb{Z}_2$ then it has a primitive solution and hence has a primitive solution modulo every power of 2; but if p and q both equal 3 modulo 4 then there is no primitive solution modulo 4. Thus $(p,q)_2 = -1$ in this case. The main part of the usual quadratic reciprocity law follows.

9. Ending remarks

Starting from the number field k, our second main datum could be a binary quadratic form Q over k rather than a quadratic field extension of k. Then we would define $K = k[X]/\langle X^2 - \mathrm{disc}(Q)\rangle$, a quadratic field extension of k if Q is anisotropic and a 2-dimensional k-vector space regardless. At a suitable level of equivalence, the norm from K to k is the binary quadratic form Q.

A person might argue that this writeup gets things backwards, that really Hilbert quadratic reciprocity makes ν a Hecke character rather than conversely. But the larger issue is that ν being a Hecke character helps to show that a construction called the Weil representation gives rise to automorphic forms. The Weil representation space is the Schwartz–Bruhat functions on $\mathbb{A}_K$,

$$\mathcal{S}(\mathbb{A}_K),$$

and the group represented is

$$G \times H \quad \text{where} \begin{cases} G = \mathrm{Sp}(1, \mathbb{A}_k) = \mathrm{SL}(2, \mathbb{A}_k), \\ H = \prod_v H_v, \quad H_v = \{k \in K_v : \mathrm{N}_{K_v/k_v}(h) = 1\}. \end{cases}$$

The Weil representation in general pairs metaplectic and orthogonal groups. The situation discussed in this writeup is the simplest case.