(*September 17, 2010*)

Quadratic reciprocity (after Weil)

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

I show that over global fields (characteristic not 2) the *quadratic norm residue symbol* is a *Hecke character*, i.e., is a $k^\times$-invariant continuous character on the ideles of k. From this *reciprocity law* follows directly the traditional reciprocity laws for quadratic Hilbert symbols, and for quadratic symbols.

A striking point in the proof is the role played by quadratic exponential functions, treated as tempered distributions. The archimedean prototype is the function

$$S_x(z) \;=\; e^{\pi i x|z|^2}$$

for $x \in \mathbb{R}^\times$ and $z \in \mathbb{C}$.

This argument is suggested by and is essential to a treatment of Weil representations, and proof that *theta series are automorphic forms.*

---

1. *Standard set-up and Poisson summation*

This section reviews standard items (measures, convolutions, characters, bilinear forms). Note that we are concerned not with an L^2 Fourier inversion, but rather with a Schwartz-Bruhat Fourier inversion, which is easier to treat.

Let k be a global field of characteristic not 2. On each completion $k_{\mathbf{p}}$ of k we fix a non-trivial additive unitary character $\psi_{\mathbf{p}}$. For global applications, we are constrained to make these choices so that, for all but finitely-many $\mathbf{p}$,

$$\psi_{\mathbf{p}}(xy) = 1 \;\forall y \in \mathbf{o}_{\mathbf{p}} \Leftrightarrow x \in \mathbf{o}_{\mathbf{p}}$$

where $\mathbf{o}_{\mathbf{p}}$ is the local ring of integers for non-archimedean primes. Further, we are constrained to choose the family of characters so that the global character

$$\psi = \bigotimes_{\mathbf{p}} \psi_{\mathbf{p}}$$

is trivial on $k \subset k_{\mathbb{A}}$.

For an additive Haar measure $\mu^o_{\mathbf{p}}$ on $k_{\mathbf{p}}$ we have a local Fourier transform

$$\mathbb{F}f(x) = \hat{f}(x) = \int_{k_{\mathbf{p}}} f(y)\,\overline{\psi}_{\mathbf{p}}(xy)\,d\mu^o_{\mathbf{p}}(y)$$

We take the Haar measure so that Fourier inversion

$$f\,\hat{}\,\hat{}\,(x) = f(-x)$$

holds. The total measure of the quotient $\mathbb{A}_k/k$ be 1.

Let K be either a quadratic field extension of k or isomorphic to $k \times k$, and in either case let σ be the non-trivial k-algebra automorphism of K. Define a k-valued k-bilinear form $\langle , \rangle$ on K by

$$\langle \alpha, \beta \rangle = \mathrm{tr}_{K/k}(\alpha\beta^\sigma)$$

where

$$\mathrm{tr}_{K/k}(\alpha) = \alpha + \alpha^\sigma$$

We can extend this $k_{\mathbf{p}}$-linearly to a $k_{\mathbf{p}}$-valued $k_{\mathbf{p}}$-bilinear form $\langle , \rangle_{\mathbf{p}}$ on

$$K_{\mathbf{p}} = K \otimes_k k_{\mathbf{p}}$$

Give the spaces $K_{\mathbf{p}}$ additive Haar measures in a compatible way, such that Fourier Inversion holds locally everywhere, with respect to the pairing

$$v \times w \to \psi(\langle v, w \rangle)$$

Both locally and globally there is the convolution on Schwartz-Bruhat functions

$$(f * \phi)(v) = \int f(v - w)\, \phi(w)\, dw$$

Since the groups involved are abelian, convolution is commutative:

$$f * \phi = \phi * f$$

For a Schwartz-Bruhat function f on $K_{\mathbb{A}}$, we have Poisson Summation

$$\sum_{x \in K} f(x) = \sum_{x \in K} \hat{f}(x)$$

This assertion is equivalent to the assertion that the tempered distribution u defined by

$$u(f) = \sum_{x \in K} f(x)$$

is its own Fourier transform. This may be proven by proving the one-dimensionality of the space of distributions v which are (first) supported on K and (second) annihilated by multiplication by the functions

$$x \to \psi(\langle \xi, x \rangle)$$

for all $\xi \in K$. The Fourier transform simply exchanges these conditions, from which follows the Poisson formula up to a constant. Our normalization of measure makes the constant be 1.

---

2. *Weil's quadratic exponential distributions*

We introduce Weil's quadratic exponential functions, which we consider as tempered distributions. The first two lemmas below, while straightforward, contain the germ of the reciprocity law. The third lemma is a recollection of a more general fact as manifest here.

For $x \in k_{\mathbf{p}}^\times$ define

$$S_x(v) = \psi_{\mathbf{p}}(\frac{x}{2}\langle v, v \rangle)$$

We may view this as a tempered distribution (as usual), by identifying it with the integration-against functional

$$f \to \int_{K_{\mathbf{p}}} S_x(v)\, f(v)\, dv$$

Lemma (p-adic case):

$$FS_x = \gamma(x)\, S_{-x^{-1}}$$

where

$$\gamma(x) = \lim_X \int_X \psi_{\mathbf{p}}(\frac{1}{2}x\langle w, w\rangle)\, dw$$

as X ranges over larger and larger compact open subgroups of $K_{\mathbf{p}}$. (In fact, there is a large-enough compact open subgroup Y of K so that the limit is reached for any $X \supset Y$).

Lemma: Let f be a Schwartz-Bruhat function on $K_{\mathbf{p}}$. For $x \in k^\times$ and $v \in K_{\mathbf{p}}$ we have

$$(S_x * f)(v) = S_x(v)\, F(S_x f)(xv)$$

Lemma (p-adic version): Let f be a Schwartz-Bruhat function on $K_{\mathbf{p}}$ and let ϕ be a smooth function on $K_{\mathbf{p}}$. For $x \in k^\times$, $v \in K_{\mathbf{p}}$, we have

$$F(\phi f) = F\phi * Ff$$

where $F\phi$ is the Fourier transform of the tempered distribution ϕ.

Note: In the last lemma, the 'smoothness' means locally constant. The analogue of the third lemma in the archimedean case requires a more delicate statement, since there Schwartz-Bruhat and test functions differ, and the notion of *'moderate growth'* is needed in addition to smoothness.

Proof: (of first lemma) In the course of the proof, we do indeed show that the limit exists, even in the stronger sense indicated.

By the usual definition of Fourier transform of a tempered distribution,

$$FS_x(f) = S_x(Ff) = \int_{K_{\mathbf{p}}} S_x(v)\, Ff(v)\, dv$$

Since Ff is also a Schwartz-Bruhat function, we can insert the characteristic function ch_X of any sufficiently large compact open set X into the integral without affecting its value. Thus,

$$FS_x(f) = \int_{K_{\mathbf{p}}} S_x(v)\mathrm{ch}_X(v)\, Ff(v)\, dv$$

Then $S_x\mathrm{ch}_X$ is itself a Schwartz-Bruhat function, so we can apply the identity

$$\int_{K_{\mathbf{p}}} f_1(v)Ff_2(v)\, dv = \int_{K_{\mathbf{p}}} Ff_1(v)f_2(v)\, dv$$

Thus, we have

$$FS_x(f) = \int_{K_{\mathbf{p}}} F(S_x\mathrm{ch}_X)(v)\, f(v)\, dv$$

Given $v \in K_{\mathbf{p}}$, we have

$$F(S_x\mathrm{ch}_X)(v) = \int_X S_x(w)\bar{\psi}_{\mathbf{p}}(\langle v, w\rangle)\, dw =$$

$$= \int_X \psi_{\mathbf{p}}(\frac{1}{2}x\langle w, w\rangle - \langle v, w\rangle)\, dw =$$

$$= \int_X \psi_{\mathbf{p}}(\frac{1}{2}x\langle w - x^{-1}v, w - x^{-1}v\rangle - x^{-1}\langle v, v\rangle)\, dw$$

since generally

$$\psi_{\mathbf{p}}(\langle v, w\rangle) = \psi_{\mathbf{p}}(\langle v, w\rangle^\sigma) = \psi_{\mathbf{p}}(\langle w, v\rangle)$$

For X large enough (depending upon v), we can replace w by $w + x^{-1}v$ to obtain

$$F(S_x \mathrm{ch}_X)(v) = S_{-x^{-1}}(\langle v, v\rangle) \int_X \psi_{\mathbf{p}}(\frac{1}{2}x\langle w, w\rangle)\, dw$$

Thus,

$$FS_x = S_{-x^{-1}} \lim_X \int_X \psi_{\mathbf{p}}(\frac{1}{2}x\langle w, w\rangle)\, dw$$

as claimed. ///

Proof: (of second lemma) From the definitions, and from

$$\psi(\langle v, w\rangle) = \psi(\langle w, v\rangle)$$

we have

$$(f * S_x)(v) = (S_x * f)(v) = \int_K S_x(v - w) f(w)\, dw =$$

$$= \int_K S_x(v)\bar{\psi}(\langle xv, w\rangle) S_x(w) f(w)\, dw =$$

$$= S_x(v)\, F(S_x f)(xv)$$

This is all we want here. ///

Proof: (of third lemma, p-adic case) Let T_w be the (regular representation) operator on Schwartz-Bruhat functions by

$$T_w f(v) = f(v + w)$$

The convolution of a distribution u and a test function f is defined as

$$(u * f)(v) = u(T_{-v} f)$$

It is easy to see that if the distribution u is integration against a function S, then this convolution is the usual convolution of functions.

Let ch_X be the characteristic function of a (large) compact open subgroup X of $K_{\mathbf{p}}$. Then, in the topology of (tempered) distributions,

$$\mathrm{ch}_X \phi \to \phi$$

Indeed, for large enough X depending upon the Schwartz-Bruhat function f,

$$\int_X \phi(v)\, f(v)\, dv = \int_{K_{\mathbf{p}}} \phi(v)\, f(v)\, dv$$

since in the p-adic case f has compact support. Likewise, since the Fourier transform is an isomorphism (topological) of Schwartz-Bruhat functions, also

$$\lim_X F(\mathrm{ch}_X u) = Fu$$

Thus,

$$(F\phi * Ff)(v) = (F\phi)(T_{-v}Ff) = \lim_X (F(\mathrm{ch}_X\phi))(T_{-v}Ff) =$$
$$= \lim_X (F(\mathrm{ch}_X\phi) * Ff)(v) = \lim_X F(\mathrm{ch}_X\phi f)(v) =$$
$$= F(\phi f)(v)$$

where we invoke the usual identity

$$F(\alpha * \beta) = F\alpha * F\beta$$

only for Schwartz-Bruhat functions. ///

---

3. *Quadratic norm residue symbols and local integrals*

One more bit of preparation is required. We define the **local norm residue symbol**

$$\nu_{\mathbf{p}} : k_{\mathbf{p}}^\times \to \{\pm 1\}$$

attached to the 'separable quadratic extension' $K_{\mathbf{p}}/k_{\mathbf{p}}$ as follows. If $K_{\mathbf{p}} = K \otimes_k k_{\mathbf{p}}$ is not a field, then just put $\nu_{\mathbf{p}}(x) = 1$ for all $x \in k_{\mathbf{p}}^\times$. If $K_{\mathbf{p}}$ is a field, put $\nu_{\mathbf{p}}(x) = 1$ if x is a norm from $K_{\mathbf{p}}$, otherwise $\nu_{\mathbf{p}}(x) = -1$.

It is a 'standard but non-trivial fact' that *the norms from $K_{\mathbf{p}}$ are of index two in $k_{\mathbf{p}}^\times$ if $K_{\mathbf{p}}$ is a separable quadratic field extension of $k_{\mathbf{p}}^\times$*. We invoke this in order to be confident that $\nu_{\mathbf{p}}$ is a group homomorphism.

As in the previous section, let

$$\gamma(x) = \gamma_{\mathbf{p}}(x) = \lim_X \int_X S_x(v)\, dv$$

where X ranges over larger and larger compact open subgroups of $K_{\mathbf{p}}$, and $x \in k_{\mathbf{p}}^\times$.

Lemma (p-adic case): For $x \in k_{\mathbf{p}}^\times$ we have

$$\gamma_{\mathbf{p}}(x) = \nu_{\mathbf{p}}(x)|x|_{k_{\mathbf{p}}}^{-1}\, \gamma_{\mathbf{p}}(1)$$

Proof: From the definition,

$$\gamma(x) = \lim_X \int_X \psi(xvv^\sigma)\, dv$$

and *the limit is actually reached for sufficiently large X*. If $x \in k_{\mathbf{p}}^\times$ is of the form ww^σ, then replacing v by vw^{-1} in the integral gives

$$\gamma(x) = |w|_{K_{\mathbf{p}}}^{-1} \lim_X \int_{wX} \psi(vv^\sigma)\, dv$$

We are taking the local norms which make the product formula hold, so

$$|x|_{k_{\mathbf{p}}} = |ww^\sigma|_{k_{\mathbf{p}}} = |w|_{K_{\mathbf{p}}}$$

Thus, we have the desired formula in case x is a local norm.

If x is not a local norm, then it must be that $K_{\mathbf{p}}$ is a field, since otherwise the local norm map is onto. Let Θ be the subgroup of $K_{\mathbf{p}}^\times$ of elements of norm 1; it is *compact*. Then, letting X vary over Θ-*stable* compact open subgroups,

$$\gamma(x) = \lim_X \int_X \psi(xvv^\sigma)\, dv =$$
$$= \lim_X \int_{\Theta\backslash X} \int_\Theta \psi(xv\theta\theta^\sigma v^\sigma)\, d\theta\, dv =$$

$$= \lim_X \int_{\Theta\backslash X} \psi(xvv^\sigma)\, dv$$

where we give Θ total measure 1.

Now

$$\Theta\backslash K_{\mathbf{p}}^\times \xrightarrow{\phi} k_{\mathbf{p}}^\times$$

by

$$\alpha \to \alpha\alpha^\sigma$$

is an isomorphism. Note that

$$d^\times\alpha = |\alpha|_{K_{\mathbf{p}}}^{-1} d\alpha$$

$$d^\times y = |y|_{k_{\mathbf{p}}}^{-1} dy$$

are multiplicative Haar measures on $K_{\mathbf{p}}^\times$ and $k_{\mathbf{p}}^\times$, respectively. Then the (topological) isomorphism just above yields an identity

$$\gamma(x) = \lim_X \int_{\Theta\backslash X} \psi(xvv^\sigma)\, dv =$$

$$= \lim_{X'} \int_{\Theta\backslash X'} \psi(x\alpha\alpha^\sigma)\, |\alpha|_{K_{\mathbf{p}}}\, d^\times\alpha =$$

$$= \lim_Y \int_Y \psi(xy)\, |y|_{k_{\mathbf{p}}}\, d^\times y =$$

where $y = \alpha\alpha^\sigma$, $X' = X - 0$, and Y is the image of X' under the norm map. (Here we choose *some* compatible normalizations of the measures: it doesn't matter *which* compatible normalization we choose).

Then, again using the fact that in this quadratic field extension the norms are of index 2,

$$\lim_Y \int_Y \psi(xy)\, d^\times y = \lim_Z \int_Z \psi(xy)\, \frac{1}{2}(1 + \nu_{\mathbf{p}}(y))\, |y|_{k_{\mathbf{p}}}\, d^\times y$$

where Z runs over larger and larger compact open additive subgroups of $k_{\mathbf{p}}$ (ignoring the point $0 \in k_{\mathbf{p}}^\times$).

An elementary (and typical) cancellation argument shows that for $x \neq 0$

$$\lim_Z \int_Z \psi(xy)\, |y|_{k_{\mathbf{p}}}\, d^\times y = 0$$

Then

$$\gamma(x) = \lim_Z \int_Z \psi(xy)\, \frac{1}{2}\nu_{\mathbf{p}}(y)\, |y|_{k_{\mathbf{p}}}\, d^\times y$$

At this point, replace y by yx^{-1} to obtain the desired identity. ///

---

4. *Reciprocity law for quadratic norm residue symbols*

The reciprocity law here is the assertion that (quadratic) **global norm residue symbols**

$$\nu_{K/k}(x) = \Pi_{\mathbf{p}}\, \nu_{\mathbf{p}}(x)$$

(with x an idele of k) are *Hecke characters*, i.e., are *trivial on* $k^\times$. (The continuity is clear).

Proof: This *global* assertion needs a global 'source': Poisson summation. Let f be any *adelic* Schwartz-Bruhat function. Fix $x \in k^\times$. For an adele $v = (v_{\mathbf{p}})_{\mathbf{p}}$ write

$$S_x(v) = \Pi_{\mathbf{p}}\, S_x^{\mathbf{p}}(v_{\mathbf{p}})$$

where now

$$S_x^{\mathbf{p}}(v) = \psi_{\mathbf{p}}(\frac{1}{2} x v_{\mathbf{p}} v_{\mathbf{p}}^{\sigma})$$

Then

$$\sum_{v\in K} f(v) = \sum_{v\in K} S_x(v) f(v)$$

since S_x is 1 on K. Then by Poisson summation this is

$$\sum_{v\in K} F(S_x f)(v) = \sum_{v\in K} (FS_x * Ff)(v) =$$

$$= \gamma(x) \sum_{v\in K} (S_{-x^{-1}} * Ff)(v) =$$

by the first lemma concerning S_x which computed its Fourier transform as tempered distribution. Then, by the second lemma on S_x (computing $S_x * f$), this is equal to

$$\gamma(x) \sum_{v\in K} S_{-x^{-1}}(v)\, F(S_{-x^{-1}} Ff)(xv) =$$

$$= \gamma(x) \sum_{v\in K} F(S_{-x^{-1}} Ff)(xv)$$

since $S_{-x^{-1}} = 1$ on K. We may change variables in the sum, replacing v by vx^{-1}, to obtain (so far)

$$\sum_{v\in K} f(v) = \gamma(x) \sum_{v\in K} F(S_{-x^{-1}} Ff)(v) =$$

$$= \gamma(x) \sum_{v\in K} S_{-x^{-1}}(v)\, Ff(v)$$

(the latter by Poisson summation)

$$= \gamma(x) \sum_{v\in K} Ff(v) = \gamma(x) \sum_{v\in K} f(v)$$

since $S_{-x^{-1}}(v) = 1$, and again applying Poisson summation.

Thus, taking any f so that

$$\sum_{v\in K} f(v) \neq 0$$

we conclude that necessarily

$$\gamma(x) = 1$$

for all $x \in k^\times$. Then

$$1 = \gamma(x) = \Pi_{\mathbf{p}}\, \gamma_{\mathbf{p}}(x) = \Pi_{\mathbf{p}}\, |x|_{k_{\mathbf{p}}} \nu_{\mathbf{p}}(x) \gamma_{\mathbf{p}}(x)$$

$$= \Pi_{\mathbf{p}}\, \nu_{\mathbf{p}}(x) \gamma_{\mathbf{p}}(1) = \nu(x)\gamma(1)$$

from the product formula and from the earlier result that

$$\gamma_{\mathbf{p}}(x) = \nu_{\mathbf{p}}(x) \gamma_{\mathbf{p}}(1)$$

Thus, we have proven that ν is a Hecke character. ///

5. *Quadratic Hilbert-symbol reciprocity*

We now 'recall' the definition of Hilbert symbols (in the quadratic case), and obtain the reciprocity law for these from the fact that the norm residue symbol is a Hecke character.

For $a, b \in k_{\mathbf{p}}$ define the (quadratic) **Hilbert symbol**

$$(a, b)_{\mathbf{p}} = \pm 1$$

by taking it to be 1 if the equation

$$ax^2 + by^2 = z^2$$

has a solution x, y, z with $x, y, z \in k_{\mathbf{p}}$ not all 0, and if there is no solution then we define the value of this symbol to be -1.

Certainly much can be said about this Hilbert symbol, but we content ourselves with the reciprocity law:

[5.0.1] Theorem: For $a, b \in k^\times$

$$\Pi_{\mathbf{p}}\ (a, b)_{\mathbf{p}} = 1$$

Proof: We prove this from the fact that the quadratic norm residue symbol is a Hecke character.

If b (or a) is a square in $k^\times$, then the equation

$$ax^2 + by^2 = z^2$$

certainly has a solution over the global field k, with $x = 0$. Then there is certainly a solution over $k_{\mathbf{p}}$ for all $\mathbf{p}$, so all the Hilbert symbols are all 1. Thus, the reciprocity assertion certainly holds in this case.

Suppose that b is not a square in $k^\times$. Then rewrite the equation as

$$ax^2 = z^2 - by^2 = \mathrm{Norm}_{K/k}(z + y\sqrt{b})$$

where $K = k(\sqrt{b})$ is now a quadratic field extension of k.

At a prime $\mathbf{p}$ of k which *splits* in K, the local extension $K \otimes_k k_{\mathbf{p}}$ is not a field, and the 'norm' map is a surjection, so $\nu_{\mathbf{p}} \equiv 1$ in that case.

At a prime $\mathbf{p}$ of k which does *not* split in K, the local extension $K \otimes_k k_{\mathbf{p}}$ *is* a field, so

$$ax^2 = z^2 - by^2$$

can have no (non-trivial) solution x, y, z even in $k_{\mathbf{p}}$ unless $x \neq 0$. In that case, we can divide by x and find that a is a norm if and only if this equation has a solution.

In summary, the values $(a, b)_{\mathbf{p}}$ of the Hilbert symbol coincide with the values of the local norm residue symbol $\nu_{\mathbf{p}}(a)$ attached to the local field extension $k(\sqrt{b})/k$. Thus, the 'reciprocity law' for the norm residue symbol gives the corresponding result for the Hilbert symbol. ///

Observe that, in the course of the proof, we essentially proved a local statement stronger than that required to obtain the reciprocity law: we showed that *the quadratic Hilbert symbol* $(a, b)_{\mathbf{p}}$ *is equal to the quadratic local norm residue symbol* $\nu_{\mathbf{p}}(a)$ *attached to the 'local extension'* $k_{\mathbf{p}}(\sqrt{b})$*, for any non-zero* $a, b \in k_{\mathbf{p}}$. Here if b is a square in k then we must interpret this 'extension' as being

$$k_{\mathbf{p}}[X] \bmod X^2 - b$$

6. *Quadratic reciprocity*

Now we obtain the most traditional sort of quadratic reciprocity law from the reciprocity law for the quadratic Hilbert symbol. We only derive what is often called the 'main part', i.e., the part refering to non-archimedean odd primes. Inspection of the relation (indicated in the proof) of the quadratic symbols to Hilbert symbols will make clear how to obtain the 'auxiliary' parts of quadratic reciprocity.

Fix a 'ring of integers' $\mathbf{o}$ inside k: for number fields k take the integral closure of $\mathbb{Z}$ in k, and for a function field which is a separable extension of $\mathbb{F}_q(X)$ take the integral closure of $\mathbb{F}_q[X]$ in k.

For a (non-archimedean) prime $\mathbf{p}$ of $\mathbf{o}$, and for $x \in \mathbf{o}$ define the quadratic symbol

$$\left(\frac{x}{\mathbf{p}}\right)_2$$

to be 1 if x is a non-zero square mod $\mathbf{p}$, 0 if x is 0 mod $\mathbf{p}$, and -1 if x is a non-square mod $\mathbf{p}$. If $\pi \in \mathbf{o}$ generates a prime ideal $\mathbf{p}$, then also write

$$\left(\frac{x}{\pi}\right)_2 = \left(\frac{x}{\mathbf{p}}\right)_2$$

Recall that a prime $\mathbf{p}$ is **odd** if the cardinality of its residue class field is odd. Concommitantly, in the number field case, a prime is **infinite** if it lies over the real prime of $\mathbb{Q}$. In the function field case, the 'prime at infinity' in $\mathbb{F}_q(T)$ is given by the valuation

$$\infty : P \to q^{\deg P}$$

A prime (i.e., valuation) $\mathbf{p}$ of a finite separable extension k of $\mathbb{F}_q(T)$, lying over ∞, is an **'infinite prime of k'**.

The reciprocity law here is:

Quadratic Reciprocity ('main part'): Let π and ϖ be two elements of $\mathbf{o}$ generating distinct odd prime ideals. Then

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = \Pi_{\mathbf{q}} \, (\pi, \varpi)_{\mathbf{q}}$$

where $\mathbf{q}$ runs over all *even or infinite* primes, and $(,)_{\mathbf{q}}$ is the (quadratic) Hilbert symbol.

Quadratic Reciprocity ('supplementary part'): Let π and be two elements of $\mathbf{o}$ generating an odd prime ideal. For any other element α of $\mathbf{o}$ which is a $\pi\mathbf{o}$-unit,

$$\left(\frac{\alpha}{\pi}\right)_2 = \Pi_{\mathbf{q}} \, (\pi, \alpha)_{\mathbf{q}}$$

where $\mathbf{q}$ runs over all *even or infinite* primes and over all primes at which α is not a local unit.

The proof of the 'main part' illustrates well-enough the connection, so we omit explicit proof of the 'supplementary part'.

Proof: (of main part) We claim that, since $\pi\mathbf{o}$ and $\varpi\mathbf{o}$ are odd primes,

$$\begin{aligned} (\pi, \varpi)_{\mathbf{q}} &= \left(\tfrac{\varpi}{\pi}\right)_2 \text{ for } \mathbf{q} = \pi\mathbf{o} \\ &= \left(\tfrac{\pi}{\varpi}\right)_2 \text{ for } \mathbf{q} = \varpi\mathbf{o} \\ &= 1 \text{ for } \mathbf{q} \text{ odd and } \mathbf{q} \neq \pi\mathbf{o}, \varpi\mathbf{o} \end{aligned}$$

Let $\mathbf{p} = \pi\mathbf{o}$. Suppose that there is a solution x, y, z in $k_{\mathbf{p}}$ to

$$\pi x^2 + \varpi y^2 = z^2$$

Then (via the ultrametric property) $\mathrm{ord}_{\mathbf{p}} y$ and $\mathrm{ord}_{\mathbf{p}} z$ must be identical, and less than $\mathrm{ord}_{\mathbf{p}} x$, since ϖ is a $\mathbf{p}$-unit and $\mathrm{ord}_{\mathbf{p}} \pi x^2$ is *odd*. Then multiply through by π^{2n} so that $\pi^n y$ and $\pi^n z$ are $\mathbf{p}$-units. Then we see that ϖ must be a square modulo $\mathbf{p}$.

On the other hand, if ϖ is a square modulo $\mathbf{p}$, then we can use Hensel's lemma to infer that ϖ is a square in $k_{\mathbf{p}}$. Then

$$\varpi y^2 = z^2$$

certainly has a non-trivial solution.

Further, if $\mathbf{q}$ is an odd prime distinct from both $\pi\mathbf{o}$ and $\varpi\mathbf{o}$, then both π and ϖ are $\mathbf{q}$-units. If ϖ is a square in $k_{\mathbf{q}}$, then

$$\varpi = z^2$$

certainly has a solution, so the Hilbert symbol is 1. Suppose ϖ is not a square in $k_{\mathbf{q}}$. Then, $k_{\mathbf{q}}(\sqrt{\varpi})$ is an unramified field extension of $k_{\mathbf{q}}$, since $\mathbf{q}$ is odd. Thus, the norm map is surjective to units in $k_{\mathbf{q}}$. Thus, there are $y, z \in k_{\mathbf{q}}$ so that

$$\pi = \mathrm{Norm}(z + y\sqrt{\varpi}) = z^2 - \varpi y^2$$

Thus, all but the even prime and infinite prime quadratic Hilbert symbols have interpretations in terms of quadratic symbols. ///

---

7. *The simplest examples*

First, let's recover the statement of quadratic reciprocity for two (positive) odd prime numbers p, q in $\mathbb{Z}$. We wish to recover the assertion

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4}$$

What we have in fact proven, so far, is that by the result of the previous section

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

where $(p, q)_2$ is the 2-adic Hilbert symbol and $(p, q)_\infty$ is the $\mathbb{Q}_\infty \approx \mathbb{R}$ Hilbert symbol.

Since both p, q are positive, the equation

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

certainly has non-trivial real solutions x, y, z. That is, the 'real' Hilbert symbol $(p, q)_\infty$ for the archimedean completion of $\mathbb{Q}$ has the value 1. Therefore, it is only the 2-adic Hilbert symbol which must contribute to the right-hand side of Gauss' formula: so far we have

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

A modest exercise using Hensel's lemma shows that the solvability of the equation above (for p, q both 2-adic units) depends only upon their residue classes mod 8. The usual formula is but one way of interpolating the 2-adic Hilbert symbol by more elementary-looking formulas. ///

For contrast, let us derive the analogue for $\mathbb{F}_q[T]$ with q odd: for distinct *monic* irreducible polynomials π, ϖ in $\mathbb{F}_q[T]$, we have

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = \left(\frac{-1}{\mathbb{F}_q}\right)_2^{(\deg \pi)(\deg \varpi)}$$

where $\left(\frac{-1}{\mathbb{F}_q}\right)_2$ is $\pm$ depending upon whether -1 is a square in $\mathbb{F}_q$ or not.

So far, from the general assertion of the previous section,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = (\pi, \varpi)_\infty$$

where ∞ is the prime (valuation)

$$P \to q^{\deg P}$$

This valuation has valuation ring consisting of all rational functions in T which can be written as power series in the local parameter $t_\infty = T^{-1}$. Then

$$\pi = t_\infty^{-\deg \pi}(1 + t_\infty(\ldots))$$

where $(1 + t_\infty(\ldots))$ is some power series in t_∞. A similar assertion holds for ϖ. Thus, if either degree is *even*, then one of π, ϖ is a local square, so the Hilbert symbol is $+1$.

If $t_\infty^{-\deg \pi}(1 + t_\infty(\ldots))$ is a non-square, then $\deg \pi$ is odd. Nevertheless, *any* expression of the form

$$1 + t_\infty(\ldots)$$

is a local square (by Hensel's lemma). Thus, without loss of generality for local purposes, we are contemplating the equation

$$t_\infty(x^2 + y^2) = z^2$$

The t_∞-order of the right-hand side is even. If there is no $\sqrt{-1}$ in $\mathbb{F}_q$, then the left-hand side is t_∞-times a norm from the unramified extension

$$\mathbb{F}_q(\sqrt{-1}(T) = \mathbb{F}_q(T)(\sqrt{-1}$$

so has odd order. This is impossible. On the other hand if there is a $\sqrt{-1}$ in $\mathbb{F}_q$ then the equation has non-trivial solutions.

Thus, if neither π nor ϖ is a local square (i.e., both are of odd degree), then the Hilbert symbol is 1 if and only if there is a $\sqrt{-1}$ in $\mathbb{F}_q$. The formula given above is an elementary interpolation of this assertion (much as was done for the case $k = \mathbb{Q}$). ///