(*December 19, 2010*)

Quadratic reciprocity (after Weil)

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

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

Striking is the role of certain quadratic exponential functions, as tempered distributions. The archimedean prototype is

$$S_x(z) \;=\; e^{\pi i x|z|^2} \qquad\qquad (x \in \mathbb{R}^\times \text{ and } z \in \mathbb{C})$$

This argument is suggested by, and essential to, a careful 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. We are concerned not with L^2 Fourier inversion, but rather with a Schwartz-Bruhat Fourier inversion, which is easier.

Let k be a global field of characteristic not 2. On each completion k_v of k fix a non-trivial additive unitary character ψ_v. For global applications, make these choices so that, for all but finitely-many v,

$$\psi_v(xy) \;=\; 1 \text{ for all } y \in \mathfrak{o}_v \;\Leftrightarrow\; x \in \mathfrak{o}_v \qquad\qquad (\mathfrak{o}_v \text{ the local ring of integers})$$

Further, choose the family of characters so that the global character

$$\psi \;=\; \bigotimes_v \psi_v$$

is *trivial* on $k \subset k_{\mathbb{A}}$. For a character and (additive) Haar measure on k_v there is a local Fourier transform

$$Ff(x) \;=\; \hat{f}(x) \;=\; \int_{k_v} f(y)\,\overline{\psi}_v(xy)\,dy$$

Take the Haar measure so that Fourier inversion holds:

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

The aggregate of local measures should make 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 $k \times k$. 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

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

Extend this k_v-linearly to a k_v-valued k_v-bilinear form $\langle , \rangle$ on

$$K_v \;=\; K \otimes_k k_v$$

Give the spaces K_v additive compatible Haar measures, such that Fourier Inversion holds locally everywhere, with respect to the pairing

$$a \times b \;\longrightarrow\; \psi\langle a, b\rangle$$

Locally and globally the convolution on Schwartz-Bruhat functions is

$$(f * \varphi)(a) \;=\; \int f(a-b)\,\varphi(b)\,db$$

The groups are abelian, so convolution is commutative:

$$f * \varphi \;=\; \varphi * f$$

For a Schwartz-Bruhat function f on $K_{\mathbb{A}}$, Poisson summation is

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

Poisson summation 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 supported on K and annihilated by multiplication by all the functions

$$x \;\longrightarrow\; \psi\langle \xi, x\rangle \qquad\qquad (\text{for } \xi \in K)$$

Fourier transform exchanges these conditions, from which follows the Poisson formula up to a constant. Our normalization of measure makes the constant be 1.

[1.0.1] Lemma: *(p-adic version)* For Schwartz-Bruhat f on K_v and smooth φ on K_v,

$$F(\varphi f) \;=\; F\varphi * Ff$$

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

[1.0.2] Note: In the lemma, *smooth* means *locally constant*. The analogue of the lemma in the archimedean case is more delicate, since in that case Schwartz-Bruhat and test functions differ, and the notion of *moderate growth* is needed in addition to smoothness.

Proof: (p-adic case) The proof is a reduction to the corresponding property for Schwartz-Bruhat functions.

Let L_b be the (left regular representation) operator on Schwartz-Bruhat functions by

$$L_b f(a) \;=\; f(a-b)$$

For a function h on K_v, let

$$\theta h(x) \;=\; h(-x)$$

The convolution of a distribution u and a test function f is[1]

$$(u * f)(a) \;=\; u(L_a \theta f)$$

When the distribution u is integration against a *function* S, convolution is the usual convolution of functions.

WIth ch_X be the characteristic function of a (large) compact open subgroup X of K_v

$$\mathrm{ch}_X \varphi \;\longrightarrow\; \varphi \qquad \text{(in the topology of tempered distributions)}$$

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

$$\int_X \varphi(a)\, f(a)\, da \;=\; \int_{K_v} \varphi(a)\, f(a)\, da$$

since in the p-adic case f has compact support. Likewise, since the Fourier transform is a topological automorphism of Schwartz-Bruhat functions,

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

Thus,

$$(F\varphi * Ff)(a) \;=\; (F\varphi)(L_a \theta F f) \;=\; \lim_X (F(\mathrm{ch}_X \varphi))(L_a \theta F f)$$

$$=\; \lim_X (F(\mathrm{ch}_X \varphi) * Ff)(a) \;=\; \lim_X F(\mathrm{ch}_X \varphi f)(a) \;=\; F(\varphi f)(a)$$

using the identity

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

for Schwartz-Bruhat functions. ///

---

2. *Weil's quadratic exponential distributions*

Weil's quadratic exponential functions are introduced, as tempered distributions. The first two lemmas contain the germ of the reciprocity law.

For $x \in k_v^\times$ define

$$S_x(a) \;=\; \psi_v(\frac{x}{2}\langle a, a\rangle)$$

View this as a tempered distribution, as usual, by identifying it with the integration-against functional

$$f \;\longrightarrow\; \int_{K_v} S_x(a)\, f(a)\, da$$

[2.0.1] Lemma: *(p-adic case)*

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

where

$$\gamma(x) \;=\; \lim_X \int_X \psi_v(\frac{x}{2}\langle a, a\rangle)\, da$$

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

[1] Expression of convolution in terms of left and right regular representations proceeds similarly on any unimodular topological group, by changing variables in the integrals, using the invariance of the measure. For that matter, the precise relationship is often less significant than the fact that there *is* a relationship.

[2.0.2] Lemma: Let f be a Schwartz-Bruhat function on K_v. For $x \in k_v^\times$ and $a \in K_v$

$$(S_x * f)(a) \;=\; S_x(a)\, F(S_x f)(xa)$$

Proof: (of first lemma) In the course of the proof, we show that the limit exists in the stronger sense indicated. By the usual definition of Fourier transform of a tempered distribution,

$$FS_x(f) \;=\; S_x(Ff) \;=\; \int_{K_v} S_x(a)\, Ff(a)\, da$$

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

$$FS_x(f) \;=\; \int_{K_v} S_x(a)\, \mathrm{ch}_X(a)\, Ff(a)\, da$$

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

$$\int_{K_v} f_1(a)\, Ff_2(a)\, da \;=\; \int_{K_v} Ff_1(a)\, f_2(a)\, da$$

Thus,

$$FS_x(f) \;=\; \int_{K_v} F(S_x \mathrm{ch}_X)(a)\, f(a)\, da$$

Since generally

$$\psi_v\langle a, b\rangle \;=\; \psi_v(\langle a, b\rangle^\sigma) \;=\; \psi_v\langle b, a\rangle$$

given $a \in K_v$,

$$F(S_x \mathrm{ch}_X)(a) \;=\; \int_X S_x(b)\, \overline{\psi}_v\langle a, b\rangle\, db \;=\; \int_X \psi_v(\frac{x}{2}\langle b, b\rangle - \langle a, b\rangle)\, db$$

$$= \int_X \psi_v(\frac{x}{2}\langle b, b\rangle - \tfrac{1}{2}\langle a, b\rangle - \tfrac{1}{2}\langle b, a\rangle)\, db \;=\; \int_X \psi_v(\frac{x}{2}\langle b - x^{-1}a, b - x^{-1}a\rangle - x^{-1}\langle a, a\rangle)\, db$$

For X large enough (depending upon a), replace b by $b + x^{-1}a$ to obtain

$$F(S_x \mathrm{ch}_X)(a) \;=\; S_{-x^{-1}}\langle a, a\rangle \int_X \psi_v(\frac{x}{2}\langle b, b\rangle)\, db$$

Thus,

$$FS_x \;=\; S_{-x^{-1}} \lim_X \int_X \psi_v(\frac{x}{2}\langle b, b\rangle)\, db$$

as claimed. ///

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

$$\psi\langle a, b\rangle \;=\; \psi\langle b, a\rangle$$

we have

$$(f * S_x)(a) \;=\; (S_x * f)(a) \;=\; \int_K S_x(a - b)\, f(b)\, db \;=\; \int_K \psi\big(\frac{x}{2}\langle a, a\rangle - \frac{x}{2}\langle a, b\rangle - \frac{x}{2}\langle b, a\rangle + \frac{x}{2}\langle b, b\rangle\big)\, f(b)\, db$$

$$= \int_K S_x(a)\, \overline{\psi}\langle xa, b\rangle\, S_x(b)\, f(b)\, db \;=\; S_x(a) \int_K \overline{\psi}\langle xa, b\rangle\, S_x(b)\, f(b)\, db \;=\; S_x(a)\, F(S_x f)(xa)$$

This is all we want here. ///

3. Quadratic norm residue symbols and local integrals

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

$$\nu_v : k_v^\times \longrightarrow \{\pm 1\}$$

attached to the 'separable quadratic extension' K_v/k_v as follows. If $K_v = K \otimes_k k_v$ is not a field, then just put $\nu_v(x) = 1$ for all $x \in k_v^\times$. If K_v is a field, put $\nu_v(x) = 1$ if x is a norm from K_v, otherwise $\nu_v(x) = -1$.

It is standard but non-trivial that *the norms from K_v are of index two in $k_v^\times$ for K_v a separable quadratic field extension of $k_v^\times$*. We invoke this know that ν_v is a group homomorphism.

As in the previous section, let

$$\gamma(x) \;=\; \gamma_v(x) \;=\; \lim_X \int_X S_x(a)\, da$$

where X ranges over larger and larger compact open subgroups of K_v, and $x \in k_v^\times$.

[3.0.1] Lemma: *(p-adic case)*

$$\gamma_v(x) \;=\; \nu_v(x)|x|_{k_v}^{-1}\, \gamma_v(1) \qquad\qquad (\text{for } x \in k_v^\times)$$

Proof: From the definition,

$$\gamma(x) \;=\; \lim_X \int_X \psi(xaa^\sigma)\, da$$

and *the limit is reached for sufficiently large X*. For $x \in k_v^\times$ of the form $x = bb^\sigma$, replacing a by ab^{-1} in the integral gives

$$\gamma(x) \;=\; |b|_{K_v}^{-1} \lim_X \int_{bX} \psi(aa^\sigma)\, da$$

We are using the local norms making the product formula hold, so

$$|x|_{k_v} \;=\; |bb^\sigma|_{k_v} \;=\; |b|_{K_v}$$

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

When x is not a local norm, then it must be that K_v is a field, otherwise the local norm map is onto. Let Θ be the subgroup of $K_v^\times$ of elements of norm 1; it is *compact*. Letting X vary over Θ-*stable* compact open subgroups,

$$\gamma(x) \;=\; \lim_X \int_X \psi(xaa^\sigma)\, da \;=\; \lim_X \int_{\Theta\backslash X} \int_\Theta \psi(xa\theta\theta^\sigma a^\sigma)\, d\theta\, da \;=\; \lim_X \int_{\Theta\backslash X} \psi(xaa^\sigma)\, da$$

where we give Θ total measure 1. Taking the quotient of $K_v^\times$ by the kernel Θ of the norm,

$$\varphi \;:\; \Theta\backslash K_v^\times \longrightarrow k_v^\times \qquad\qquad (\text{by } \alpha \to \alpha\alpha^\sigma)$$

is an isomorphism to its image. Note that

$$d^\times\alpha \;=\; |\alpha|_{K_v}^{-1} d\alpha \qquad\qquad d^\times y \;=\; |y|_{k_v}^{-1} dy$$

are multiplicative Haar measures on $K_v^\times$ and $k_v^\times$, respectively. The (topological) isomorphism just above yields an identity

$$\gamma(x) \;=\; \lim_X \int_{\Theta\backslash X} \psi(xaa^\sigma)\, da \;=\; \lim_{X'} \int_{\Theta\backslash X'} \psi(x\alpha\alpha^\sigma)\, |\alpha|_{K_v}\, d^\times\alpha \;=\; \lim_Y \int_Y \psi(xy)\, |y|_{k_v}\, d^\times y$$

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*.)

Since in this quadratic field extension the norms are of index 2,

$$\lim_Y \int_Y \psi(xy)\, d^\times y \;=\; \lim_Z \int_Z \psi(xy)\, \frac{1}{2}(1 + \mathrm{ord}_v(y))\, |y|_{k_v}\, d^\times y$$

where Z runs over larger and larger compact open additive subgroups of k_v (ignoring the point $0 \in k_v^\times$). A typical elementary cancellation argument shows

$$\lim_Z \int_Z \psi(xy)\, |y|_{k_v}\, d^\times y \;=\; 0 \qquad\qquad (\text{for } x \neq 0)$$

Then

$$\gamma(x) \;=\; \lim_Z \int_Z \psi(xy)\, \frac{1}{2}\mathrm{ord}_v(y)\, |y|_{k_v}\, d^\times y$$

Replace y by yx^{-1} to obtain the desired identity. ///

---

4. *Reciprocity law for quadratic norm residue symbols*

The first reciprocity law is that (quadratic) **global norm residue symbols**

$$x \;\longrightarrow\; \nu_{K/k}(x) \;=\; \Pi_v\, \nu_v(x) \qquad\qquad (\text{with } x \text{ an idele of } k)$$

are *Hecke characters*, that is, are *trivial on* $k^\times$. Continuity is clear.

Proof: This *global* assertion needs a global *source*: Poisson summation. For f an *adelic* Schwartz-Bruhat function, $x \in k^\times$, and an adele $a = \{a_v\}$, write

$$S_x(a) \;=\; \Pi_v\, S_x^v(a_v)$$

where now

$$S_x^v(a) \;=\; \psi_v(\frac{x}{2} a_v a_v^\sigma)$$

Since S_x is 1 on K,

$$\sum_{a\in K} f(a) \;=\; \sum_{a\in K} S_x(a)\, f(a)$$

By Poisson summation,

$$\sum_{a\in K} F(S_x f)(a) \;=\; \sum_{a\in K} (FS_x * Ff)(a) \;=\; \gamma(x) \sum_{a\in K} (S_{-x^{-1}} * Ff)(a)$$

by the first lemma, which computed the Fourier transform of S_x as tempered distribution. By the second lemma, which computed $S_x * f$, this is

$$\gamma(x) \sum_{a\in K} S_{-x^{-1}}(a)\, F(S_{-x^{-1}} Ff)(xa) \;=\; \gamma(x) \sum_{a\in K} F(S_{-x^{-1}} Ff)(xa)$$

since $S_{-x^{-1}} = 1$ on K. Change variables in the sum, replacing a by ax^{-1}, to obtain (so far)

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

the latter by Poisson summation, and this is

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

since $S_{-x^{-1}}(a) = 1$, and again applying Poisson summation. Taking any f so that

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

necessarily

$$\gamma(x) = 1 \qquad \text{(for all } x \in k^\times)$$

Then

$$1 = \gamma(x) = \Pi_v \gamma_v(x) = \Pi_v |x|_{k_v}^{-1} \nu_v(x)\gamma_v(x) = \Pi_v \nu_v(x)\gamma_v(1) = \nu(x)\gamma(1)$$

from the product formula and from the earlier result that

$$\gamma_v(x) = \nu_v(x)\gamma_v(1)$$

Thus, ν is a Hecke character. ///

---

5. *Quadratic Hilbert-symbol reciprocity*

Recall the definition of quadratic Hilbert symbols, and obtain the their reciprocity law from the fact that the norm residue symbol is a Hecke character.

For $a, b \in k_v$ the (quadratic) **Hilbert symbol** is

$$(a,b)_v = \begin{cases} 1 & \text{(when } ax^2 + by^2 = z^2 \text{ has non-trivial solution in } k_v) \\ -1 & \text{(otherwise)} \end{cases}$$

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

$$\Pi_v (a,b)_v = 1$$

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

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

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

has a solution over the global field k, with $x = 0$. Then there is a solution over k_v for all v, so all the Hilbert symbols are all 1. Thus, the reciprocity assertion holds in this case.

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

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

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

At a prime v of k *split* in K, the local extension $K \otimes_k k_v$ is not a field, and the norm is a surjection, so $\nu_v \equiv 1$ in that case.

At a prime v of k *not* split in K, the local extension $K \otimes_k k_v$ *is* a field, so

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

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

In summary, the values $(a,b)_v$ of the Hilbert symbol coincide with the values of the local norm residue symbol $\nu_v(a)$ 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. ///

In the proof, we proved a local statement stronger than that required to obtain the reciprocity law: we showed that *the quadratic Hilbert symbol $(a,b)_v$ is the quadratic local norm residue symbol $\nu_v(a)$ attached to the local extension $k_v(\sqrt{b})$, for any non-zero $a, b \in k_v$.* When b is a square in k we must interpret this extension as

$$k_v[X] \bmod X^2 - b$$

---

6. *Quadratic reciprocity*

Now we obtain the most traditional quadratic reciprocity law from the reciprocity law for the quadratic Hilbert symbol. We only derive what is often called the *main 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 $\mathfrak{o}$ 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 v of $\mathfrak{o}$, and for $x \in \mathfrak{o}$ define the quadratic symbol

$$\left(\frac{x}{v}\right)_2 \;=\; \begin{cases} 1 & (\text{for} x \text{ a non-zero square mod } v) \\ 0 & (\text{for } x = 0 \bmod v) \\ -1 & (\text{for } x \text{ a non-square mod } v) \end{cases}$$

For $\pi \in \mathfrak{o}$ generating a prime ideal v, also write

$$\left(\frac{x}{\pi}\right)_2 \;=\; \left(\frac{x}{v}\right)_2$$

A prime v is **odd** when the cardinality of its residue class field is odd. In the number field case, a prime is **infinite** when 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

$$\infty : P \;\longrightarrow\; q^{\deg P}$$

A prime (i.e., valuation) v 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 $\mathfrak{o}$ generating distinct odd prime ideals. Then

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 \;=\; \Pi_v \, (\pi, \varpi)_v$$

where v runs over all *even or infinite* primes, and $(\,,\,)_v$ is the (quadratic) Hilbert symbol.

Quadratic Reciprocity ('supplementary part'): Let $\pi \in \mathfrak{o}$ generate an odd prime ideal. For any other element α of $\mathfrak{o}$ which is a $\pi\mathfrak{o}$-unit,

$$\left(\frac{\alpha}{\pi}\right)_2 \;=\; \Pi_v\,(\pi,\alpha)_v$$

where v 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 $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$ are odd primes,

$$(\pi,\varpi)_v \;=\; \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & \text{for } v = \pi\mathfrak{o} \\ \left(\frac{\pi}{\varpi}\right)_2 & \text{for } v = \varpi\mathfrak{o} \\ 1 & \text{for } v \text{ odd and } v \neq \pi\mathfrak{o}, \varpi\mathfrak{o} \end{cases}$$

Let $v = \pi\mathfrak{o}$. Suppose that there is a solution x, y, z in k_v to

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

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

On the other hand, if ϖ is a square modulo v, then we can use Hensel's lemma to infer that ϖ is a square in k_v. Then

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

certainly has a non-trivial solution.

Further, for v is an odd prime distinct from both $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$, then both π and ϖ are v-units. If ϖ is a square in k_v, then

$$\varpi \;=\; z^2$$

certainly has a solution, so the Hilbert symbol is 1. Suppose ϖ is not a square in k_v. Then, $k_v(\sqrt{\varpi})$ is an unramified field extension of k_v, since v is odd. Thus, the norm map is surjective to units in k_v. Thus, there are $y, z \in k_v$ 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 quadratic reciprocity for two (positive) odd prime numbers p, q in $\mathbb{Z}$. We wish to recover the assertion

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

We have proven so far that

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

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

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

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, only the 2-adic Hilbert symbol contributes to the right-hand side of Gauss' formula: so far

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

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 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)

$$P \;\longrightarrow\; q^{\deg P}$$

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 $k = \mathbb{Q}$). ///