# Reciprocity Laws: Artin-Hilbert

Parvati Shastri

## 1. Introduction

In this volume, the early reciprocity laws including the quadratic, the cubic have been presented in Adhikari's article [1]. Also, in that article we have seen an exposition on the Eisenstein reciprocity without the use of class field theory. In the International Congress of Mathematicians, 1900, Hilbert asked for the most general reciprocity law, (Hilbert's problem 9) which would hold in any number field. In order to formulate and prove such a general reciprocity law, Hilbert introduced the *norm residue symbol* known after him as the Hilbert Symbol, in place of the power residue symbol and proved a reciprocity law for this symbol. From this law, one can derive all the earlier power reciprocity laws. Later on, Artin introduced a symbol named after him as the Artin Symbol, and proved a reciprocity law for his symbol. This is the crux of class field theory, today. In this article, we shall assume but recall the relevent theorems from class field theory, and deduce Hilbert's reciprocity law and show how this would imply the power reciprocity laws, that you have seen earlier. Further, we will also explicitly derive the quadratic reciprocity law, without the use of class field theory. We begin with Kummer Theory.

## 2. Kummer Theory

**Theorem 1** *Let $K$ be a field of characteristic 0, and $\mu_n \subset K$, be the group of all $n^{th}$ roots of unity.*[1] *Let $\Delta$ be a subgroup of $K^*$ such that $K^{*n} \subset \Delta \subset K^*$ and $L = K(\sqrt[n]{\Delta})$. Then $L/K$ is a Galois extension (in fact, abelian of exponent $n$) and there exists a canonical isomorphism* [2]

$$\frac{\Delta}{K^{*n}} \longrightarrow Hom\,(G(L/K), \mu_n)\,.$$

**Proof:** (Sketch) Assume $K^*/K^{*n}$ is finite. Let $G = \mathrm{Gal}(L/K)$ and let $a \in \Delta$. Define

$$\chi_a : G \longrightarrow \mu_n$$

[1] This result holds also in characteristic $p > 0$ under the additional hypothesis that, $(charK, n) = 1$.

[2] If $K^*/K^{*n}$ is infinite, then in the case when $\Delta/K^{*n}$ is also infinite, or equivalently, $L/K$ is infinite, one needs to take continuous homomorphisms. However, we need to apply this result in the case when $K^*/K^{*n}$ is finite, and we sketch a proof for this case only.

by

$$\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

We have a homomorphism

$$\theta : \Delta \longrightarrow \mathrm{Hom}(G, \mu_n)$$

defined by

$$\theta(a) = \chi_a.$$

It is clear that $\ker \theta = K^{*n}$. We claim that $\theta$ is surjective. Let $\chi \in \mathrm{Hom}(G, \mu_n)$. Then by Dedekind's theorem on the linear independence of characters, the sum $\sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \neq 0$. Let $\lambda \in L^*$ be such that $b = \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}(\lambda) \neq 0$. For $\tau \in G$, we have,

$$\begin{aligned} \tau(b) &= \tau\left(\textstyle\sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}\right)(\lambda) \\ &= \textstyle\sum_{\sigma \in G} \chi(\sigma)(\tau\sigma^{-1})(\lambda) \\ &= \chi(\tau)\left(\textstyle\sum_{\sigma \in G} \chi(\tau^{-1}\sigma)\tau\sigma^{-1}\right)(\lambda) \\ &= \chi(\tau)b. \end{aligned}$$

Let $a = b^n$. Then $a \in K^n$ and we get $\theta(a) = \chi$. Therefore we get an induced isomorphism,

$$\frac{\Delta}{K^{*n}} \cong \mathrm{Hom}(G, \mu_n).$$

**Remark 1** The above correspondence gives a bijection between subgroups $\Delta$ of $K^*$ with $K^{*n} \subset \Delta \subset K^*$ and abelian extensions of exponent $n$. (For a proof of this statement as well as for generalization to infinite extensions, the reader can refer to [4], Chapter 8, or [3], p.15. See also [2], §4, this volume.)

## 3. Local Reciprocity Law

Let $K$ be a local field of characteristic 0. By this we mean, a finite extension of $\mathbb{Q}_p$. For any local field $K$, we fix the following notations.

| | |
|---|---|
| $\mathcal{O}_K$ | ring of integers of $K$ |
| $m_K$ | the maximal ideal of $K$ |
| $\pi_K$ | a generator for $m_K$ |
| $U_K$ | group of units of $K$ |
| $\kappa(K)$ | the residue class field $\mathcal{O}_K/m\mathcal{O}_K$. |

The following is the main theorem of local class field theory.

**Theorem 2** *Let $L|K$ be a finite abelian extension of local fields with Galois group $G(L|K)$. Let $N_{L|K} : L \longrightarrow K$ denote the norm map. Then there exists a canonical isomorphism*

$$r_{L|K} : G(L|K) \longrightarrow K^*/N_{L|K}L^*$$

We will not prove this theorem, but briefly discuss how the isomorphism is defined. First assume that $L|K$ is unramified. Then $r_{L|K}$ can be described as follows. We know that $K^* = U_K \times (\pi_K)$, where $(\pi_K)$ is the (multiplicative) cyclic group generated by $\pi_K$. Since $L|K$ is unramified, $N_{L|K}$ is surjective on the unit group, that is, $N_{L|K}(U_L) = U_K$. Clearly $N_{L|K}(\pi) = \pi^n$, where $n = [L : K]$. It follows that $K^*/N_{L|K}(L^*) \cong (\pi)/(\pi^n)$, since $K^{*n} \subset N_{L|K}(L^*)$. On the other hand, if $L|K$ is unramified, the Galois group $G(L|K)$ is isomorphic to the Galois group of the residue classfield extension $\kappa(L)|\kappa(K)$. This is a finite extension of a finite field. Recall that a finite extension of a finite field is cyclic and there is a distinguished generator for the Galois group, viz., the Frobenius. So there is a unique generator of $G(L|K)$ which corresponds to the Frobenius. Let us denote this generator by $\phi$.[3] The reciprocity map $r_{L|K}$ is given by,

$$r_{L|K}(\phi) = \pi \bmod N_{L|K}(L^*).$$

In the general case, $r_{L|K}$ is defined, subject to the following two properties:

(i) (Functoriality) If $L|K$ and $L'|K'$ are finite Galois extensions of local fields with $K \subset K', L \subset L'$, then the diagram

$$\begin{array}{lcl} G(L'|K') & \stackrel{r_{L'|K'}}{\longrightarrow} & K'^*/N_{L'|K'}L'^* \\ \text{Res} \downarrow & & \downarrow N_{K'|K} \\ G(L|K) & \stackrel{r_{L|K}}{\longrightarrow} & K^*/N_{L|K}L^* \end{array}$$

is commutative, where Res denotes the restriction map $\text{Res}(\sigma) = \sigma|L \ \forall \sigma \in G(L'|K')$.
(ii) If $L|K$ is a finite unramified extension, then $r_{L|K}$ is simply the map $r_{L|K}(\phi_{L|K}) = [\pi]$, where $[\pi]$ is the class of $\pi$ mod $N_{L|K}(L^*)$.

Let $L|K$ be a totally ramified cyclic extension and $\sigma$ be a generator for $G(L|K)$. Then one can show that there exists a finite abelian extension $\Sigma$

[3] $\phi$ is characterized by the property,

$$\phi(x) \equiv x^q \bmod \pi \ \forall \ x \in \mathcal{O}_K,$$

where $q$ is the cardinality of $\kappa(K)$.

of $K$ such that $L\Sigma|\Sigma$ is unramified and the restriction of the Frobenius of $L\Sigma|\Sigma$ to $L$ is $\sigma$. Then $r_{L|K}(\sigma) = N_{\Sigma|K}(\pi_\Sigma)$. The general case is reduced to the cyclic case. Also this map is surjective and the kernel of this map is precisely the commutator subgroup $[G, G]$.

Thus, there is a canonical (i.e., satisfying (i) and (ii) above) isomorphism

$$r_{L|K} : G(L|K)^{\text{ab}} \longrightarrow K^*/N_{L|K}(L^*).$$

In particular, for finite *abelian extensions*, the Galois group $G(L|K)$ is isomorphic to the norm residue group $K^*/N_{L|K}(L^*)$.

## 4. Local Artin Symbol

Let the notation be as in section 2. Let $(*, L|K)$ be the inverse of the reciprocity map. By composing it with the natural map $K^* \longrightarrow N_{L|K}(L^*)$, we get for every $a \in K^*$, a symbol which we still denote by $(a, L|K)$ taking values in $G(L|K)$. This is called the Artin symbol; i.e., the local Artin symbol is induced by the inverse of the local reciprocity map.

Observe that we have the following simple description of the Artin symbol in the special cases $a = \pi,\ u$ where $\pi$ is a parameter and $u$ is a unit in $K$, viz.,

$$(\pi, L|K) \text{ is } \quad \text{the } \ \text{Frobenius} \in G(L|K)$$

and

$$(u, L|K) = 1.$$

## 5. Hilbert Symbol

We now define the Hilbert Symbol. Let $\mu_n$ be the group of $n^{\text{th}}$ roots of unity. Assume that $K$ is a local field containing $\mu_n$. We have, by Kummer Theory,

$$K^*/K^{*n} \cong \text{Hom}\,(G(L|K), \mu_n)\,,$$

where $L = K(\sqrt[n]{K^*})$. (Note that $K^*/K^{*n}$ is finite, since $K$ is a local field.) On the other hand, local reciprocity law gives an isomorphism,

$$K^*/N_{L|K}(L^*) \cong G(L|K).$$

Since, $K^{*n} \subset N_{L|K}(L^*) \subset K^*$, it follows that $K^{*n} = N_{L|K}L^*$. Hence we get a pairing,

$$\langle\ ,\ \rangle_n : K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n$$

given by

$$\langle a, b\rangle_n = \chi_b\left((a, L|K)\right),$$

where $\chi_b$ is the character associated to $b$ by Kummer Theory, and $(a, L|K)$ is the local Artin symbol. By the properties of the Artin symbol, it follows that

$$\langle a, b\rangle_n = \chi_b\left((a, L|K)\right) = \frac{(a, L|K)\,(\sqrt[n]{b})}{\sqrt[n]{b}} = \frac{\left(a, K(\sqrt[n]{b})|K\right)\,(\sqrt[n]{b})}{\sqrt[n]{b}} \in \mu_n.$$

By composing it with the natural map $K^* \to K^*/K^{*n}$, we get a pairing

$$\langle\ ,\ \rangle_n : K^* \times K^* \longrightarrow \mu_n.$$

This is called the *Hilbert symbol* of degree $n$. In what follows, we will fix an $n$, and drop the suffix $n$.

**Remark 2** It follows easily by the definition that the Hilbert symbol is non degenerate in the sense that,

$$\langle a, b\rangle = 1\ \forall\ b \in K^* \Rightarrow a \in K^{*n}$$

and

$$\langle a, b\rangle = 1\ \forall\ a \in K^* \Rightarrow b \in K^{*n}.$$

We now recall a few basic properties of the Hilbert symbol, which are needed in the sequel.

**Lemma 1** The Hilbert symbol has the following properties:

(i) (Bimultiplicativity)
$\langle aa', b\rangle = \langle a, b\rangle.\langle a', b\rangle,\ \langle a, bb'\rangle = \langle a, b\rangle.\langle a, b'\rangle\ \forall\ a, b \in K^*.$

(ii) $\langle 1-a, a\rangle = 1 = \langle a, 1-a\rangle\ \forall\ a \in K^*.$

(iii) $\langle a, b^{-1}\rangle = \langle a, b\rangle^{-1} = \langle a, -a\rangle = 1 = \langle a, 1\rangle.$

(iv) (Skew symmetry) $\langle a, b\rangle = \langle b, a\rangle^{-1}.$

**Proof:** Part (i) follows by definition (easy to check). For proving Parts (ii), (iii) and (iv), observe that, for $a, b \in K^*$, $\langle a, b\rangle = 1$ if and only if $a$ is a norm from $K(\sqrt[n]{b})$.
We have,

$$1 - a = \prod_{i=1}^{n}\left(1 - \zeta^i\,\sqrt[n]{a}\right),$$

where $\zeta$ is a primitive $n^{\text{th}}$ root of unity, i.e., $1-a$ is a norm from $K(\sqrt[n]{a})$. So (ii) follows.

Next, by (i) we have, $\langle a,1\rangle.\langle a,1\rangle = \langle a,1\rangle$. Hence $\langle a,1\rangle = 1$. Similarly, $\langle a,b\rangle.\langle a,b^{-1}\rangle = \langle a,bb^{-1}\rangle = \langle a,1\rangle = 1$ Now, observe that $-a = \frac{1-a}{1-a^{-1}}$. Therefore, if we take $b = -a$, we get $\langle a,-a\rangle = 1$. This completes the proof of Part (iii).

(iv) By (iii) we have, $\langle ab,-ab\rangle = 1$. Now use bimultiplicativity and simplify using (iii) to get (iv).

## 6. Power Residue Symbol

We now assume that $(n,p) = 1$ where $p$ is the characteristic of the residue class field and compute the Hilbert symbols $\langle u,v\rangle$ and $\langle \pi,u\rangle$, where $u,v$ are units and $\pi$ is a parameter of $K$. It follows from standard facts of local theory, that $K(\sqrt[n]{v})$ is unramified, and that the norm function is surjective on the unit group. Therefore $\langle u,v\rangle = 1\ \forall$ units $u,v \in K$. Also, by the discussions in Section 4, we know that the parameter corresponds to the Frobenius under the reciprocity map. Thus

$$\left(\pi, K(\sqrt[n]{u})|K\right)(x) \equiv x^q \bmod \pi\ \forall\ x \in \mathcal{O}_L,$$

where $L = K(\sqrt[n]{u})$. In particular, $(\pi, K(\sqrt[n]{u})|K)\,(\sqrt[n]{u}) \equiv \sqrt[n]{u}^q \bmod \pi$ $\equiv u^{\frac{q-1}{n}}.\sqrt[n]{u} \bmod \pi$. So $\langle \pi,u\rangle \equiv u^{\frac{q-1}{n}} \bmod \pi$. We define the $n^{\text{th}}$ *power residue symbol*, by

$$\left(\frac{u}{\pi}\right) = \langle \pi,u\rangle.$$

Note that $\langle \pi,u\rangle$ is a root of unity in $K$ and is independent of the parameter chosen.

## 7. Artin's Reciprocity Law

Let $K$ be a number field. Let $V_K$ be the set of all valuations of $K$ including the archimedian ones. Let $L|K$ be a finite abelian extension of $K$. For every valuation $v \in V_K$, fix a valuation $w$ of $L$, which extends $v$. Note that the archimedian completions of $K_v$ are isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. Therfore either $L_w \cong K_v \cong \mathbb{R}$ or $\mathbb{C}$ or $L_w \cong \mathbb{C}$ is a quadratic extension of $K_v \cong \mathbb{R}$, with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In order to state Artin's reciprocity law, we need to define Artin's symbol at the archimedian completions also. If $L_w|K_v$ is quadratic, let $\sigma$ be the nontrivial automorphism of $L_w|K_v$. We define $(a, L_w|K_v) = 1$, if $a > 0$, $(a, L_w|K_v) = \sigma$ if $a < 0$. If $L_w \cong K_v$ we define $(a, L_w|K_v) = 1$. With this notation, we have,

**Theorem 3** *For any $a \in K^*$,*

$$\prod_{v \in V_K} (a, L_w|K_v)) = 1.^4$$

## 8. Hilbert's Reciprocity Law

As in the case of Artin symbol, we also need to extend Hilbert's symbol at the archimedian completions, in an obvious manner. For $a, b \in \mathbb{R}$, define

$$\langle a, b\rangle := (-1)^{\frac{\operatorname{sgn} a - 1}{2} \cdot \frac{\operatorname{sgn} b - 1}{2}}.$$

With this definition, we have

**Theorem 4** *Let $K$ be a number field, $\mu_n \subset K$, and $V_K$ be as in the previous section. Let $a, b \in K^*$. Then*

$$\prod_{v \in V_K} \langle a, b\rangle_v = 1,$$

*where $\langle a, b\rangle_v$ is the $n^{th}$ Hilbert symbol at the completion $K_v$.*

**Proof:** This is immediate from Artin's reciprocity law. In fact, we have,

$$\begin{aligned} \textstyle\prod_{v \in V_K} \langle a, b\rangle_v &= \textstyle\prod_v \chi_b \left(a, K_v(\sqrt[n]{b})\right) \\ &= \frac{(\prod_v (a, K_v(\sqrt[n]{b})))(\sqrt[n]{b})}{\sqrt[n]{b}} \\ &= \frac{\mathrm{Id}(\sqrt[n]{b})}{\sqrt[n]{b}} \\ &= 1. \end{aligned}$$

(The last but one equality is by Artin's reciprocity law.)

## 9. Power Reciprocity Law

We need to define global power residue symbol, in terms of the local symbols. Let $K$ be a number field containing $\mu_n$, as in the previous section. Let $a, b \in K$. Let $(b) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_i}$ be the factorization of the principal ideal $(b)$. Let $v_{\mathfrak{p}}$ be the valuation on $K$ corresponding to the prime ideal $\mathfrak{p}$. We define the power residue symbol $\left(\frac{a}{b}\right)$ to be the product of the local power residue symbols; i.e.,

$$\left(\frac{a}{b}\right) = \prod_{\mathfrak{p}} \left(\frac{a}{b}\right)_{v_{\mathfrak{p}}}.$$

[4] Note that this would also mean that all but finitely many terms in this product are equal to 1.

This is well defined, since the local power residue symbol is independent of the parameter chosen.

**Theorem 5** *Let $K$ be a number field, $\mu_n \subset K$, $a, b \in K^*$. Let $(a), (b), (n)$ be relatively prime and let*

$$V_{n\infty} = \{v_{\mathfrak{p}} : \mathfrak{p}|(n)\} \cup \{v : v \text{ is archimedian}\}.$$

*Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in V_{n\infty}} \langle a, b\rangle_v.$$

**Proof:** Let us look at Hilbert's reciprocity law,

$$\prod_{v \in V_K} \langle a, b\rangle_v = 1.$$

Let $V_0 = \{v \in V_K : v|abn\infty\}$ and $V_1 = V_K - V_0$. The left hand side can be written as

$$\prod_{v|b} \langle a, b\rangle_v \prod_{v|b} \langle a, b\rangle_v \prod_{v|n\infty} \langle a, b\rangle_v \prod_{v \in V_1} \langle a, b\rangle_v.$$

Now, observe that

$$\prod_{v \in V_1} \langle a, b\rangle_v = 1,$$

since each of the symbols is trivial. Also,

$$\langle a, b\rangle_v = \left(\frac{b}{a}\right)_v \text{ if } v|a$$

and

$$\langle a, b\rangle_v = \langle b, a\rangle_v^{-1} = \left(\frac{a}{b}\right)_v^{-1} \text{ if } v|b.$$

Hence the theorem follows.

## 10. Quadratic Reciprocity Law

In order to derive the quadratic reciprocity law, we need to compute the Hilbert symbols in the special case, $n = 2, K = \mathbb{Q}$. First assume $a, b$ are odd positive integers. Then we have,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \langle a, b\rangle_2 \langle a, b\rangle_\infty.$$

Here $\langle a, b\rangle_2$ denotes the Hilbert symbol at the dyadic completion $\mathbb{Q}_2$. Since $a, b$ are positive, $\langle a, b\rangle_\infty = 1$. So, we only need to compute $\langle a, b\rangle_2$. Let $U_{\mathbb{Q}_2}$

be the unit group of $\mathbb{Q}_2$. Note that $U_{\mathbb{Q}_2}/U^2_{\mathbb{Q}_2}$ is generated by $\{5,-1\}$.[5] By the bimultiplicative and skew symmetric properties of the Hilbert symbol, it is enough to compute $\langle 5,-1\rangle_2$, $\langle 5,-5\rangle_2$, $\langle -1,-1\rangle_2$. We have, $\langle 5,-1\rangle_2 = \langle 5,5\rangle_2 = 1$ and $\langle -1,-1\rangle_2 = -1$. From this it follows that

$$\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}}(-1)^{\frac{b-1}{2}},$$

for $a, b \in \{5,-1\}$. For arbitrary odd integers, the result follows from the multiplicativity of these symbols and the fact that for an odd integer $a$, $a^2 \equiv 1 \bmod 4$.

## REFERENCES

1. S.D.Adhikari, *The Early Reciprocity Laws: From Gauss to Eisenstein*, This volume.

2. M. J. Narlikar, *Abelian Kummer Theory*, This volume.

3. J.Neukirch, Class Field Theory, Springer-Verlag, 1986.

4. V. Suresh, Chapter 8 in *Introduction to Class Field Theory*, (Lecture Notes of the Instructional School on Algebraic Number Theory, held in the Department of Mathematics, University of Mumbai, December 1994-January 1995).

5. J. Tate, Problem 9: The General Reciprocity Law, Proceedings of Symp. in Pure Math. Vol. 28, 1976, pp. 311-322.

Parvati Shastri
Department of Mathematics
University of Mumbai
Mumbai 400 098
*e-mail:* parvati@math.mu.ac.in

[5] This is a consequence of Hensel's lemma.