

RATIONAL RECIPROCITY LAWS

MARK BUDDEN ¹

10/7/05

The purpose of this note is to provide an overview of Rational Reciprocity (and in particular, of Scholz's reciprocity law) for the non-number theorist. In the first part, we will describe the background in number theory that will be necessary for a complete understanding of the material to be discussed in the second part. The second part focuses on a proof of Scholz's reciprocity law using the splitting of minimal polynomials and considers ways in which this law can be extended.

1. Algebraic Number Fields

Here, we focus on the necessary aspects of number theory that will be used throughout the remainder of this note. By an algebraic number field K , we mean a finite dimensional extension of \mathbb{Q} . If K and L are two algebraic number fields satisfying $K \subseteq L$, then L can be viewed as a K -vector space and we denote its dimension by $[L : K]$. By the Primitive Element Theorem, there exists $a \in L$ such that $L = K(a)$. The element a is algebraic over K (it is the root of a nonzero polynomial in $K[x]$ - see Theorem 4.1 of Jacobson [J]). There exists a unique monic irreducible polynomial in $K[x]$ with a as a root. This polynomial is referred to as the minimal polynomial of a over K and its degree is equal to the dimension of L over K . The Galois group $\text{Gal}(L/K)$ is defined to be the group of all automorphisms of L that fix K .

Now we define an important subring of an algebraic number field. Such a subring will mimic the role that \mathbb{Z} plays as a subring of \mathbb{Q} . An element $b \in K$ is called an algebraic integer if it is the root of a monic polynomial in $\mathbb{Z}[x]$. The set of all algebraic integers in K form a ring, called the ring of integers in K , that is denoted by \mathcal{O}_K . If L/K is an extension of algebraic number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$.

1.1. Quadratic Fields. Consider the quadratic field $\mathbb{Q}(\sqrt{d})$ where $d \neq 0$ is a square-free integer. It is a simple exercise (see Proposition 13.1.1 of [IR]) to show that

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z} \left[\frac{-1+\sqrt{d}}{2} \right] & \text{if } d \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

Furthermore, the units of $\mathbb{Q}(\sqrt{d})$ are given by

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}^\times = \begin{cases} \{\pm 1\} & \text{if } d < -3 \text{ or } d = -2 \\ \{\pm 1, \pm i\} & \text{if } d = -1 \\ \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\} & \text{if } d = -3 \\ \{\pm \varepsilon_d^m \mid m \in \mathbb{Z}, \text{ some unit } \varepsilon_d > 1\} & \text{if } d > 0 \end{cases}$$

(see Propositions 13.1.5 and 13.1.6 of [IR]). In the last case, where $\mathbb{Q}(\sqrt{d})$ is a "real" number field, the group of units has infinite order and ε_d is called the fundamental unit of $\mathbb{Q}(\sqrt{d})$.

¹Research partially supported by AASU Internal Grant #727188.

1.2. Ramification Theory. Ramification theory was introduced by David Hilbert (see [H], [Ja], and [N]) and was utilized in his work to find the “most general reciprocity law in an arbitrary algebraic number field” (see [T]). For the purposes of this note, we will only consider ramification theory as it pertains to algebraic number fields. Let L/K be an extension of algebraic number fields (assume all extensions are Galois, as this is the case we will need) and let \mathcal{O}_L and \mathcal{O}_K be the respective rings of integers. Then if \mathfrak{p} is a nonzero prime ideal of \mathcal{O}_K , the ideal $\mathfrak{p}\mathcal{O}_L$ has the factorization (see Theorem 6.8 of [Ja], Chapter 1, Section 6)

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^e$$

for distinct prime ideals \mathfrak{P}_i of \mathcal{O}_L and there is a constant

$$f = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

that is independent of i . Furthermore,

$$efg = [L : K]$$

and the action of $\text{Gal}(L/K)$ permutes the ideals \mathfrak{P}_i of \mathcal{O}_L containing \mathfrak{p} . Here, e is called the ramification degree of \mathfrak{P}_i over \mathfrak{p} and f is called the residue degree of \mathfrak{P}_i over \mathfrak{p} . Now if \mathfrak{P} is a nonzero prime ideal of \mathcal{O}_L and $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$, then we say that \mathfrak{P} is ramified over \mathcal{O}_K (or \mathfrak{p} ramifies in \mathcal{O}_L) if $e > 1$. If $e = 1$, then \mathfrak{P} is called unramified.

Example 1. Consider the quadratic field $\mathbb{Q}(i)$. In lifting a prime $p \in \mathbb{Z}$ to the ring of integers $\mathbb{Z}[i] \subset \mathbb{Q}(i)$, one of three things can occur. It is possible that the ideal $p\mathbb{Z}[i]$ is a prime ideal in $\mathbb{Z}[i]$. This is the inert case. It is also possible that $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{q}$ where \mathfrak{p} and \mathfrak{q} are distinct prime ideals in $\mathbb{Z}[i]$. Here, we say that p splits in $\mathbb{Z}[i]$. Finally, p may ramify: $p\mathbb{Z}[i] = \mathfrak{p}^2$. The only prime that ramifies in $\mathbb{Z}[i]$ is 2 since $2\mathbb{Z}[i] = ((i+1)\mathbb{Z}[i])^2$. We leave it as an exercise to prove that p splits if $p \equiv 1 \pmod{4}$ and is inert if $p \equiv 3 \pmod{4}$. This result should be compared to the supplementary law to the law of quadratic reciprocity (the Legendre symbol is defined below):

$$(1) \quad \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Thus, $\left(\frac{-1}{p}\right) = 1$ if and only if p splits in $\mathbb{Q}(\sqrt{-1})$.

In general, a similar result holds in $\mathbb{Q}(\sqrt{a})$ for the Legendre symbol: if $a \in \mathbb{Z}$ and p is a rational prime such that $(a, p) = 1$, then

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise.} \end{cases}$$

The following theorem follows from Proposition 2.1 of [Le2].

Theorem 2.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \text{ splits in } \mathbb{Q}(\sqrt{a}) \\ -1 & \text{if } p \text{ is inert in } \mathbb{Q}(\sqrt{a}). \end{cases}$$

In an extension of algebraic number fields L/K , it is known that there are only finitely-many primes that ramify. This result is obtained by considering the discriminant of a number field and is beyond the scope of this note. The final result that we will state in this section is due to Kummer (cf. Theorem 7.4, [Ja], Chapter 1, Section 7).

Kummer's Theorem Let \mathfrak{p} be a prime ideal in \mathcal{O}_K and assume that there is an element $\theta \in L$ such that $\mathcal{O}_L = \mathcal{O}_K[\theta]$. Let $f(x)$ be the minimal polynomial of θ over K and let $\bar{f}(x)$ be the polynomial obtained by reducing the coefficients of $f(x)$ modulo \mathfrak{p} . If

$$\bar{f}(x) = \bar{g}_1(x)^{a_1} \bar{g}_2(x)^{a_2} \cdots \bar{g}_t(x)^{a_t}$$

is the factorization of $\bar{f}(x)$ into a product of distinct irreducible polynomials over $\mathcal{O}_K/\mathfrak{p}$, then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{a_1} \mathfrak{P}_2^{a_2} \cdots \mathfrak{P}_t^{a_t}$$

for certain prime ideals \mathfrak{P}_i of \mathcal{O}_L corresponding one-to-one with the irreducible factors $\bar{g}_i(x)$. Moreover, the residue degree f of \mathfrak{P}_i corresponds to the degree of $\bar{g}_i(x)$.

1.3. Cyclotomic Fields. A cyclotomic field is a field of the form $\mathbb{Q}(\zeta_n)$ (we assume $n \geq 3$), where

$$\zeta_n = \cos(2\pi/n) + i \sin(2\pi/n)$$

is a primitive n^{th} root of unity. We begin with the special case where $n = p$ is prime. The minimal polynomial of ζ_p over \mathbb{Q} is

$$(2) \quad \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

which is irreducible in $\mathbb{Z}[x]$ (Theorem 1 from [IR], Chapter 13, Section 2). Since the roots of $\Phi_p(x)$ are the primitive p^{th} roots of unity ζ_p^j where $j \in \{1, 2, \dots, p-1\}$, we can write

$$(3) \quad \Phi_p(x) = \prod_{j=1}^{p-1} (x - \zeta_p^j) \in \mathbb{Q}(\zeta_p)[x].$$

The cyclotomic polynomial $\Phi_n(x)$ is defined recursively (Proposition 13.2.2 of [IR]) by the equation

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

and is the minimal polynomial of ζ_n over \mathbb{Q} .

In general, the ring of integers of an algebraic number field $\mathbb{Q}(\alpha)$ will not be $\mathbb{Z}[\alpha]$. However, in the special case of $\mathbb{Q}(\zeta_n)$, we do have that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ (Theorem 2.6 of [W]). Regarding the ramification of primes in $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} , we have the following theorem (Proposition 2.3 of [W]).

Theorem 3. p ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p|n$.

The Galois group of the extension $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} (the group of automorphisms of $\mathbb{Q}(\zeta_n)$ that fix \mathbb{Q}) is given by

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \{ \sigma_k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times \},$$

where $\sigma_k(\zeta_n) = \zeta_n^k$ ([IR], Proposition 13.2.1 and the corollaries of Theorem 1 in Chapter 13, Section 2). Under the Fundamental Theorem of Galois Theory, there is correspondence between subgroups $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and intermediate fields of the extension ([J], Section 4.5). In the special case $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the Galois group is cyclic and hence has a unique subgroup of any order that divides

$$|\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1.$$

Assuming that $p \geq 3$, we see that $2|(p-1)$, and hence, there is a unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. Plugging $x = 1$ into (2) and (3), we see that

$$\begin{aligned} p &= (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}) \\ &= ((1 - \zeta^2)(1 - \zeta^{-2}))((1 - \zeta^4)(1 - \zeta^{-4})) \cdots ((1 - \zeta^{p-1})(1 - \zeta^{-(p-1)})) \\ &= (2 - \zeta^2 - \zeta^{-2})(2 - \zeta^4 - \zeta^{-4}) \cdots (2 - \zeta^{p-1} - \zeta^{-(p-1)}) \\ &= (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (\zeta^j - \zeta^{-j})^2. \end{aligned}$$

Thus, it follows that if $p^* = (-1)^{(p-1)/2}p$, then $\mathbb{Q}(\sqrt{p^*})$ is contained in $\mathbb{Q}(\zeta_p)$ and $p = p^*$ if and only if $p \equiv 1 \pmod{4}$.

2. Reciprocity

Looking back at the development of algebraic number theory over the last few centuries, reciprocity has influenced the subject more than any other single topic. First observed independently by Euler and Legendre, the Law of Quadratic Reciprocity demanded a generalization that was sought by number theorists until the 1930s. The Law of Quadratic Reciprocity itself has been proved by more than 300 methods and many of the techniques used have provided the discipline with new tools and at times, completely new theories. To begin, we state the Law of Quadratic Reciprocity.

Law of Quadratic Reciprocity *If p and q are distinct rational primes, then*

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

The law of quadratic reciprocity saw generalizations by individuals such as Eisenstein, Hasse, Hilbert, Takagi, Artin, and Tate. These laws are not the focus of this brief survey and the interested reader is referred to the comprehensive text [Le2], as well as its upcoming volumes 2 and 3 (part of the draft of volume 2 is currently available on Lemmermeyer's webpage <http://www.rzuser.uni-heidelberg.de/~hb3/>). The emphasis here will be on a certain class of reciprocity laws known as rational reciprocity laws.

2.1. Rational Reciprocity. The main difference between a reciprocity law and a rational reciprocity law is that rational reciprocity refers to residue symbols that are defined on integers and only take on the values ± 1 . To begin, we define the rational power residue symbol $\left(\frac{a}{p}\right)_n$, where $(a, p) = 1$, to be 1 if a is an n^{th} power residue of p and -1 otherwise. In particular, if an integer a such that $(a, p) = 1$ satisfies

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$$

for a rational prime p and a nonnegative integer n , then define the rational symbol

$$\left(\frac{a}{p}\right)_{2n} \equiv a^{\frac{p-1}{2n}} \pmod{p}.$$

This symbol takes on the same value as $\left(\frac{a}{\mathfrak{p}}\right)_{\mathbb{Q}(\zeta_{2n})}$, the $2n^{\text{th}}$ power residue symbol where \mathfrak{p} is any prime above p in $\mathbb{Q}(\zeta_{2n})$. It should be noted that the Legendre symbol is equivalent to the rational power residue symbol when $n = 1$.

In 1934, Scholz [S] proved a rational quartic reciprocity law via class field theory. While the law still bears Scholz's name, it was recently noted by Lemmermeyer (see the notes at the end of Chapter 5 in [Le2]) that it had been proved much earlier in 1839 by Schönemann [Sc]. Since then, Scholz's reciprocity law has been proved by many different methods (see [EP], [L1], [Wi], and [WHF]). The unfamiliar reader is referred to Emma Lehmer's expository article [L2] for a complete description of rational reciprocity laws and [WHF] or [Le1] for a proof of an all-encompassing rational quartic reciprocity law.

Scholz's Reciprocity Law *If $p \equiv q \equiv 1 \pmod{4}$ are distinct primes such that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$, then*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_p}{q}\right) = \left(\frac{\varepsilon_q}{p}\right).$$

Before we prove Scholz's reciprocity law, we begin with a description of the unique quadratic and quartic subfields of $\mathbb{Q}(\zeta_p)$ when $p \equiv 1 \pmod{4}$. We saw in Section 1.3 that the quadratic subfield is given by $K = \mathbb{Q}(\sqrt{p})$. Perhaps less well-known, the quartic subfield is given by

$$L = \mathbb{Q}\left(\sqrt{\varepsilon_p(-1)^{(p-1)/4}\sqrt{p}}\right) = K\left(\sqrt{\varepsilon_p(-1)^{(p-1)/4}\sqrt{p}}\right)$$

(see Proposition 5.9, [Le2]). Now we give the proof of Scholz's reciprocity law that will be generalized in [BEK].

Proof. We proceed in a manner similar to the proof of quadratic reciprocity that was given by Lemmermeyer [Le2] after Proposition 3.4 on page 83. One can easily check that if $\sigma_k \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (where $\sigma_k(\zeta_p) = \zeta_p^k$), then

$$\sigma_k(\sqrt{p}) = \left(\frac{k}{p}\right) \sqrt{p},$$

implying that

$$\text{Gal}(\mathbb{Q}(\zeta_p)/K) \cong \left\{ \sigma_k \mid \left(\frac{k}{p}\right) = 1 \right\}.$$

Similarly, it can also be shown that

$$\text{Gal}(\mathbb{Q}(\zeta_p)/L) \cong \left\{ \sigma_k \mid \left(\frac{k}{p}\right)_4 = 1 \right\}.$$

Thus, the Galois group $\text{Gal}(L/K)$ consists of the identity automorphism and an automorphism $\alpha = \sigma_k|_L$ where k is a quadratic residue of p that is not a quartic residue.

From these Galois groups, one sees that the cyclotomic polynomial $\Phi_p(x)$ splits over K as

$$\Phi_p(x) = \varphi_p(x) \tilde{\varphi}_p(x)$$

where

$$\varphi_p(x) = \prod_{\left(\frac{j}{p}\right)=1} (x - \zeta_p^j) \quad \text{and} \quad \tilde{\varphi}_p(x) = \prod_{\left(\frac{k}{p}\right)=-1} (x - \zeta_p^k).$$

Since $\Phi_p(x)$ splits into linear factors in $\mathbb{Z}[\zeta_p][x]$, it follows that

$$\varphi_p(x), \tilde{\varphi}_p(x) \in \mathbb{Z}[\zeta_p][x] \cap K[x] = \mathcal{O}_K[x] = \mathbb{Z}\left[\frac{-1 + \sqrt{p}}{2}\right][x].$$

The polynomial $\varphi_p(x)$ can then be factored over L :

$$\varphi_p(x) = \psi_p(x) \tilde{\psi}_p(x) \in \mathcal{O}_L[x]$$

where

$$\psi_p(x) = \prod_{\left(\frac{m}{p}\right)_4=1} (x - \zeta_p^m) \quad \text{and} \quad \tilde{\psi}_p(x) = \prod_{\left(\frac{n}{p}\right)_4=-1} (x - \zeta_p^n).$$

To simplify notation in what follows, we will denote

$$\pi_p = \varepsilon_p(-1)^{(p-1)/4} \sqrt{p}$$

so that $L = \mathbb{Q}(\sqrt{\pi_p})$ (and hence, $L = K(\sqrt{\pi_p})$) and α sends

$$(4) \quad \sqrt{\pi_p} \mapsto -\sqrt{\pi_p}.$$

Considering the action of α on the polynomial $\varphi_p(x) = \psi_p(x)\tilde{\psi}_p(x)$, we see that α interchanges $\psi_p(x)$ and $\tilde{\psi}_p(x)$.

Define the polynomial $\vartheta_p(x) = \psi_p(x) - \tilde{\psi}_p(x)$ and note that

$$\alpha(\vartheta_p(x)) = -\vartheta_p(x).$$

Using (4), it follows that

$$\alpha(\sqrt{\pi_p} \vartheta_p(x)) = \sqrt{\pi_p} \vartheta_p(x),$$

proving that

$$(5) \quad \vartheta_p(x) \in \sqrt{\pi_p} \mathbb{Z} \left[\frac{-1 + \sqrt{p}}{2} \right] [x].$$

We will write $\vartheta_p(x) = \sqrt{\pi_p} \phi_p(x)$ with $\phi_p(x) \in \mathbb{Z} \left[\frac{-1 + \sqrt{p}}{2} \right] [x]$.

Since $\left(\frac{p}{q}\right) = 1$, q splits in K . In other words, we can write $q = \lambda \cdot \beta(\lambda)$, where β is the nontrivial automorphism in $\text{Gal}(K/\mathbb{Q})$ given by $\sqrt{p} \mapsto -\sqrt{p}$. The residue field $\mathcal{O}_K/\lambda\mathcal{O}_K \cong \mathbb{Z}/q\mathbb{Z}$. Now we raise $\vartheta_p(x)$ to the power q and reduce modulo $\lambda\mathcal{O}_K$. Since we are also assuming that $\left(\frac{q}{p}\right) = 1$, we can use the fact that $\left(\frac{q}{p}\right)_4 = \pm 1$.

$$(6) \quad \begin{aligned} (\vartheta_p(x))^q &\equiv (\psi_p(x) - \tilde{\psi}_p(x))^q \\ &\equiv \prod_{\left(\frac{m}{p}\right)_4=1} (x^q - \zeta_p^{mq}) - \prod_{\left(\frac{n}{p}\right)_4=-1} (x^q - \zeta_p^{nq}) \\ &\equiv \left(\frac{q}{p}\right)_4 (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \pmod{\lambda\mathcal{O}_K}. \end{aligned}$$

The automorphism $\sigma_q \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is in $\text{Gal}(\mathbb{Q}(\zeta_p)/K)$ and its restriction to $\text{Gal}(L/K)$ is α if and only if $\left(\frac{q}{p}\right)_4 = -1$. On the other hand, we can apply (5) to find

$$\begin{aligned} (\vartheta_p(x))^q &\equiv \sqrt{\pi_p}^q (\phi_p(x))^q \\ &\equiv (\varepsilon_p^2 p)^{\frac{q-1}{4}} (\sqrt{\pi_p}) (\phi_p(x))^q \pmod{\lambda\mathcal{O}_K}. \end{aligned}$$

Applying an analog of Fermat's Little Theorem (Proposition 9.3.1 of [IR]) to the coefficients of $(\phi_p(x))^q \pmod{\lambda\mathcal{O}_K}$, it follows that

$$\begin{aligned}
 (\vartheta_p(x))^q &\equiv (\varepsilon_p^2)^{\frac{q-1}{4}} (\sqrt{\pi_p}) \phi_p(x^q) \\
 &\equiv \left(\frac{\varepsilon_p^2 p}{q}\right)_4 \vartheta_p(x^q) \\
 (7) \qquad &\equiv \left(\frac{\varepsilon_p^2 p}{q}\right)_4 (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \pmod{\lambda\mathcal{O}_K}.
 \end{aligned}$$

Next, we show that

$$\psi_p(X) \not\equiv \tilde{\psi}_p(X) \pmod{\lambda\mathcal{O}_K}.$$

By Kummer's Theorem ([Ja], Theorem 7.4), the ideal generated by q in $\mathbb{Z}[\zeta_p]$ (which is unramified since p is the only ramified prime) decomposes in exactly the same way as $\Phi_p(X)$ decomposes in $(\mathbb{Z}/q\mathbb{Z})[X]$. If

$$\varphi_p(X) \equiv (\psi_p(X))^2 \pmod{\lambda\mathcal{O}_K},$$

then we can pick $\{0, 1, \dots, q-1\}$ as coset representatives of $\mathcal{O}_K/\lambda\mathcal{O}_K \cong \mathbb{Z}/q\mathbb{Z}$ to obtain a square factor of $\Phi_p(X)$ in $(\mathbb{Z}/q\mathbb{Z})[X]$, contradicting the observation that q does not ramify in $\mathbb{Z}[\zeta_p]$.

Finally, comparing (6) and (7) we obtain

$$\left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_p^2}{q}\right)_4 \left(\frac{p}{q}\right)_4 = \left(\frac{\varepsilon_p}{q}\right)_4 \left(\frac{p}{q}\right)_4.$$

By symmetry, the statement of Scholz's reciprocity law follows. \square

2.2. Generalizing Scholz's Law. In [BW1], Buell and Williams conjectured, and in [BW2] they proved, an octic reciprocity law of Scholz type which we refer to below as Scholz's octic reciprocity law. While this law does not receive as much attention as Scholz's original law, it does provide insight into the potential formulation of a general rational reciprocity law of this type.

Scholz's Octic Reciprocity Law *Let $p \equiv 1 \pmod{8}$ and $q \equiv 1 \pmod{8}$ be distinct rational primes such that $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. Then*

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \begin{cases} \left(\frac{\varepsilon_p}{q}\right)_4 \left(\frac{\varepsilon_q}{p}\right)_4 & \text{if } N(\varepsilon_{pq}) = -1 \\ (-1)^{h(pq)/4} \left(\frac{\varepsilon_p}{q}\right)_4 \left(\frac{\varepsilon_q}{p}\right)_4 & \text{if } N(\varepsilon_{pq}) = 1. \end{cases}$$

Buell and Williams' law provides a beautiful rational octic reciprocity law involving the fundamental units of quadratic fields, but it loses some of the simplicity of the statement of Scholz's law. It seems more natural to use units from the unique quartic subfield of $\mathbb{Q}(\zeta_p)$ when constructing such an octic law. This was our motivation in the formulation of the following rational reciprocity law similar to that of Scholz (upcoming in [BEK]).

Theorem 4. *Let $p \equiv 1 \pmod{2^t}$ and q be distinct odd rational primes such that*

$$\left(\frac{p}{q}\right)_{2^{t-1}} = \left(\frac{q}{p}\right)_{2^{t-1}} = \left(\frac{2}{p}\right)_{2^{t-2}} = 1,$$

and set

$$A_t = \left\{ 1 \leq a \leq \frac{p-1}{2} \mid \left(\frac{a}{p} \right)_{2^{t-1}} = 1 \right\} \quad \text{and} \quad B_t = \left\{ 1 \leq b \leq \frac{p-1}{2} \mid \left(\frac{b}{p} \right)_{2^{t-1}} = -1 \right\}.$$

Then

$$\left(\frac{p}{q} \right)_{2^t} \left(\frac{q}{p} \right)_{2^t} = \left(\frac{\beta_{2^t}}{q} \right)_{2^{t-1}}$$

where

$$\beta_{2^t} = \prod_{k=2}^t \eta_{2^k}^{2^{t-2}} \quad \text{and} \quad \eta_{2^t} := \frac{\prod_{b \in A_{t-1} \cap B_t} (\zeta_{2^p}^b - \zeta_{2^p}^{-b})}{\prod_{a \in A_t} (\zeta_{2^p}^a - \zeta_{2^p}^{-a})} \in \mathcal{O}_{K_{2^t-1}}^\times.$$

The proof of Theorem 4 is similar to the proof of Scholz's reciprocity law that was given up above. However, one needs to consider the intermediate subfields of degrees 2^{t-1} and 2^t (K_{2^t-1} and K_{2^t} , respectively) of $\mathbb{Q}(\zeta_p)$ over \mathbb{Q} . It can be shown that η_{2^t} is a unit in the ring of integers of K_{2^t-1} , similar to Scholz's law where ε_p was a unit in the quadratic extension. It is not immediately clear that Theorem 4 contains Scholz's reciprocity law as a corollary (when $t = 2$). This realization follows from Proposition 3.24 of [Le2] where it is shown that $\eta_4 = \varepsilon_p^h$ for an odd integer h (the class number of $\mathbb{Q}(\sqrt{p})$). Hence, we have that

$$\left(\frac{\eta_4}{q} \right) = \left(\frac{\varepsilon_p^h}{q} \right) = \left(\frac{\varepsilon_p}{q} \right),$$

resulting in the statement of Scholz's law. Finally, it should be noted that the octic version ($t = 3$) of Theorem 4 is different from that of Buell and Williams and we leave it to the reader to compare the two laws.

REFERENCES

- [BEK] M. Budden, J. Eisenmenger, and J. Kish, *A Generalization of Scholz's Reciprocity Law*, in preparation
- [BW1] D. Buell and K. Williams, *Is There an Octic Reciprocity Law of Scholz Type?*, Amer. Math. Monthly **85** (1978), 483-484.
- [BW2] D. Buell and K. Williams, *An Octic Reciprocity Law of Scholz Type*, Proc. Amer. Math. Soc. **77** (1979), 315-318.
- [EP] D. Estes and G. Pall, *Spinor Genera of Binary Quadratic Forms*, J. Number Theory **5** (1973), 421-432.
- [FT] A. Fröhlich and M. Taylor, "Algebraic Number Theory," Cambridge University Press, 1991.
- [H] D. Hilbert, "The Theory of Algebraic Number Fields," Springer-Verlag (translated by Iain Adamson), Berlin, 1998.
- [IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Graduate Texts in Mathematics 84, Springer-Verlag, New York, 1990.
- [J] N. Jacobson, "Basic Algebra I," 2nd edition, W. H. Freeman and Company, New York, 1985.
- [Ja] G. Janusz, "Algebraic Number Fields," 2nd ed., Graduate Studies in Mathematics, Vol. 7, American Mathematical Society, Providence, RI, 1996.
- [L1] E. Lehmer, *On the Quadratic Character of some Quadratic Surds*, J. Reine Angew. Math. **250** (1971), 42-48.
- [L2] E. Lehmer, *Rational Reciprocity Laws*, Amer. Math. Monthly **85** (1978), 467-472.
- [Le1] F. Lemmermeyer, *Rational Quartic Reciprocity*, Acta Arith. **67** (1994), 387-390.
- [Le2] F. Lemmermeyer, "Reciprocity Laws," Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.
- [N] J. Neukirch, "Algebraic Number Theory," A Series of Comprehensive Studies in Mathematics Vol. 322 (translated by Norbert Schappacher), Springer-Verlag, Berlin, 1999.
- [S] A. Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$* , Math. Z. **39** (1934), 95-111.
- [Sc] T. Schönemann, *Theorie der Symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben*, J. Reine Angew. Math. **19** (1839), 289-308.
- [T] J. Tate, *Problem 9: The General Reciprocity Law*, Mathematical Developments Arising from Hilbert Problems, Proc. of Symp. in Pure Math. **28** (1974), 311-322.
- [W] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1997.

[Wi] K. Williams, *On Scholz's Reciprocity Law*, Proc. Amer. Math. Soc. **64** No. 1 (1977), 45-46.

[WHF] K. Williams, K. Hardy, and C. Friesen, *On the Evaluation of the Legendre Symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$* , Acta Arith. **45** (1985), 255-272.

Algebra, Algebraic Number Theory: [FT], [H], [IR], [J], [Ja], [N], [W]

Reciprocity: [BEK], [BW1], [BW2], [EP], [IR], [L1], [L2], [Le1], [Le2], [S], [Sc], [T], [Wi], [WHF]