Journal de Théorie des Nombres
de Bordeaux **19** (2007), 583–594

A generalization of Scholz's reciprocity law

par Mark BUDDEN, Jeremiah EISENMENGER et Jonathan KISH

Résumé. Nous donnons une généralisation de la loi de réciprocité de Scholz fondée sur les sous-corps $K_{2^{t-1}}$ et K_{2^t} de $\mathbb{Q}(\zeta_p)$ de degrés 2^{t-1} et 2^t sur $\mathbb{Q}$, respectivement. La démonstration utilise un choix particulier d'élément primitif pour K_{2^t} sur $K_{2^{t-1}}$ et est basée sur la division du polynôme cyclotomique $\Phi_p(x)$ sur les sous-corps.

Abstract. We provide a generalization of Scholz's reciprocity law using the subfields $K_{2^{t-1}}$ and K_{2^t} of $\mathbb{Q}(\zeta_p)$, of degrees 2^{t-1} and 2^t over $\mathbb{Q}$, respectively. The proof requires a particular choice of primitive element for K_{2^t} over $K_{2^{t-1}}$ and is based upon the splitting of the cyclotomic polynomial $\Phi_p(x)$ over the subfields.

1. Introduction

In 1934, Scholz [12] 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 [11]) that it had been proved much earlier in 1839 by Schönemann [13]. Since then, Scholz's reciprocity law has been proved using many different methods (see [3], [7], [10], and [14] for other proofs). The unfamiliar reader is referred to Emma Lehmer's expository article [9] for an overview of rational reciprocity laws and Williams, Hardy, and Friesen's article [15] for a proof of an all-encompassing rational quartic reciprocity law that was subsequently simplified by Evans [4] and Lemmermeyer [10].

We begin by stating Scholz's reciprocity law and an octic version of the law proved by Buell and Williams [2]. We will need the following notations. For a quadratic field extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, with squarefree positive $d \in \mathbb{Z}$, let ε_d denote the fundamental unit and $h(d)$ denote the class number. The standard notation $\left(\frac{\cdot}{\cdot}\right)$ will be used to denote the Legendre symbol. We will also need to define the rational power residue symbol. Assume that a is an integer such that $(a, p) = 1$ that satisfies

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

Manuscrit reçu le 21 juillet 2006.

for a rational prime p and a positive 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 values as $\left(\frac{a}{\mathfrak{p}}\right)_{\mathbb{Q}(\zeta_{2n})}$, the $2n^{th}$ power residue symbol where $\mathfrak{p}$ is any prime above p in $\mathbb{Q}(\zeta_{2n})$. For our purposes, n will usually be a power of 2. It should also be noted that the Legendre symbol is equivalent to our rational power residue symbol when $n = 1$. By convention, we define $\left(\frac{a}{p}\right)_1 = 1$ for all a such that $(a, p) = 1$.

Theorem 1.1 (Scholz's Reciprocity Law)**.** *Let $p \equiv q \equiv 1 \pmod 4$ be distinct rational primes such that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Then*

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

In [1], Buell and Williams conjectured, and in [2] they proved, an octic reciprocity law of Scholz-type which we refer to below as Buell and Williams' reciprocity law. Although their law is more complicated to state, it does provide insight into the potential formulation of a general rational reciprocity law of Scholz-type.

Theorem 1.2 (Buell and Williams' Reciprocity Law)**.** *Let $p \equiv q \equiv 1 \pmod 8$ be distinct rational primes such that $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. Then*

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

where N is the norm map for the extension $\mathbb{Q}(\sqrt{pq})$ over $\mathbb{Q}$.

Buell and Williams succeed in providing a rational octic reciprocity law involving the fundamental units of quadratic fields, but it loses some of the simplicity of the statement of Scholz's reciprocity law and requires the introduction of class numbers. 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 a general rational reciprocity law similar to that of Scholz.

In Section 2, we describe a primitive element for the unique subfield K_{2^t} of $\mathbb{Q}(\zeta_p)$ satisfying $[K_{2^t} : \mathbb{Q}] = 2^t$, when $p \equiv 1 \pmod{2^t}$ and $\left(\frac{2}{p}\right)_{2^{t-2}} = 1$. Our choice of a primitive element involves a specific choice of a unit $\eta_{2^t} \in \mathcal{O}_{K_{2^{t-1}}}^{\times}$. Section 3 provides the proof of a generalization of Scholz's reciprocity law after giving a thorough description of the rational residue symbols used in the theorem. We show that whenever $p \equiv q \equiv 1 \pmod{2^t}$ are distinct primes with $t \geq 2$ and

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

then

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

where $\beta_{2^t} = \prod_{k=2}^{t} \eta_{2^k}^{2^{k-2}} \in \mathcal{O}_{K_{2^{t-1}}}^{\times}$ and $\lambda \in \mathcal{O}_{K_{2^{t-1}}}$ is any prime above q. Our proof is based upon the splitting of the cyclotomic polynomial $\Phi_p(x)$ over the fields in question. In the special case where $t = 2$, we note that $\left(\frac{\eta_4}{\lambda}\right) = \left(\frac{\varepsilon_p}{q}\right)$, resulting in the statement of Scholz's reciprocity law.

Since our rational reciprocity law takes on a simpler octic form than Buell and Williams' reciprocity law, comparing the two results in an interesting corollary. It is observed that if $p \equiv q \equiv 1 \pmod 8$ are distinct primes satisfying

$$\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1,$$

then

$$\left(\frac{\eta_8}{\lambda}\right) = \left(\frac{\varepsilon_q}{p}\right)_4 (-N(\varepsilon_{pq}))^{h(pq)/4},$$

where $\lambda \in \mathcal{O}_{K_4}$ is any prime above q.

Acknowledgements The work contained here was partially supported by two internal grants from Armstrong Atlantic State University. The authors would like to thank Sungkon Chang for carefully reading a preliminary draft of this manuscript and providing comments which cleaned up some of our arguments and fixed an oversight in Section 3. Thanks are also due to the referee for several comments that improved the exposition.

2. Subfields of $\mathbb{Q}(\zeta_p)$

When p is an odd rational prime, it is well-known that the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $K_2 = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}p$. In this section, we provide a useful description of the subfield K_{2^t} of $\mathbb{Q}(\zeta_p)$ of degree 2^t over $\mathbb{Q}$ when $p \equiv 1 \pmod{2^t}$ and $\left(\frac{2}{p}\right)_{2^{t-2}} = 1$. We will need the following variant of Gauss's Lemma that is due to Emma Lehmer (see [8] or Proposition 5.10 of [11]) which we state without proof.

Lemma 2.1. *Let ℓ and $q = 2mn+1$ be rational primes such that $\left(\frac{\ell}{q}\right)_n = 1$ and let*

$$A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$$

be a half-system of n^{th} power residues. Then

$$\ell\alpha_j \equiv (-1)^{a(j)}\alpha_{\pi(j)} \pmod q$$

for some permutation π of $\{1, 2, \ldots, m\}$ and

$$\left(\frac{\ell}{q}\right)_{2n} = (-1)^{\mu} \quad \textit{where} \quad \mu = \sum_{i=1}^{m} a(i).$$

It should be noted that Lemma 2.1 can be applied to the evaluation of $\left(\frac{\ell}{q}\right)_{2n}$ for all $1 \leq \ell < q$ by using Dirichlet's theorem on arithmetic progressions and the observation that the rational residue symbol is well-defined on congruence classes modulo q. The statement of Scholz's Reciprocity Law utilizes the fundamental unit of K_2. Our general rational reciprocity law will similarly require the units described in the following theorem.

Theorem 2.2. *Let $p \equiv 1 \pmod{2^t}$ be a rational prime with $t \geq 2$ such that $\left(\frac{2}{p}\right)_{2^{t-2}} = 1$ and set*

$$A_{2^t} = \left\{1 \leq a \leq \frac{p-1}{2} \;\middle|\; \left(\frac{a}{p}\right)_{2^{t-1}} = 1\right\}$$

and

$$B_{2^t} = \left\{1 \leq b \leq \frac{p-1}{2} \;\middle|\; \left(\frac{b}{p}\right)_{2^{t-2}} = 1 \ \textit{ and } \ \left(\frac{b}{p}\right)_{2^{t-1}} = -1\right\}.$$

Then the element

$$\eta_{2^t} = \frac{\prod\limits_{b \in B_{2^t}} \left(\zeta_{2p}^{b} - \zeta_{2p}^{-b}\right)}{\prod\limits_{a \in A_{2^t}} \left(\zeta_{2p}^{a} - \zeta_{2p}^{-a}\right)}$$

is a unit in $\mathcal{O}_{K_{2^{t-1}}}$.

Proof. Let $p \equiv 1 \pmod{2^t}$ be a prime such that $\left(\frac{2}{p}\right)_{2^{t-2}} = 1$ (ie., $2 \in A_{2^t} \cup B_{2^t}$) and suppose that η_{2^t} is defined as in the statement of the theorem. We begin by noting that $\zeta_{2p} \in \mathbb{Q}(\zeta_p)$. This is easily checked by observing that $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{2p})$ and that both fields have degree $p-1$ over $\mathbb{Q}$. One can check that $\eta_{2^t} \in \mathbb{Z}[\zeta_p]^{\times}$ by computing the norm of η_{2^t} in $\mathbb{Q}(\zeta_p)$ and noting that A_{2^t} and B_{2^t} have the same cardinality. Next, we show that $\eta_{2^t} \in \mathcal{O}_{K_{2^{t-1}}}$. To do this, we define the element

$$\widetilde{\eta}_{2^t} = \frac{\prod\limits_{b \in B_{2^t}} \left(\zeta_{p}^{b} - \zeta_{p}^{-b}\right)}{\prod\limits_{a \in A_{2^t}} \left(\zeta_{p}^{a} - \zeta_{p}^{-a}\right)}.$$

If $\left(\frac{2}{p}\right)_{2^{t-1}} = 1$, then $2a \equiv \pm a' \pmod{p}$, $2b \equiv \pm b' \pmod{p}$, and

$$\widetilde{\eta}_{2^t} = \frac{\prod\limits_{b \in B_{2^t}} \left(\zeta_p^b - \zeta_p^{-b}\right)}{\prod\limits_{a \in A_{2^t}} \left(\zeta_p^a - \zeta_p^{-a}\right)} = \frac{\prod\limits_{b \in B_{2^t}} \left(\zeta_{2p}^{2b} - \zeta_{2p}^{-2b}\right)}{\prod\limits_{a \in A_{2^t}} \left(\zeta_{2p}^{2a} - \zeta_{2p}^{-2a}\right)} = \frac{\prod\limits_{b' \in B_{2^t}} \left(\zeta_{2p}^{b'} - \zeta_{2p}^{-b'}\right)}{\prod\limits_{a' \in A_{2^t}} \left(\zeta_{2p}^{a'} - \zeta_{2p}^{-a'}\right)} = \eta_{2^t}.$$

Applying a similar argument to the case $\left(\frac{2}{p}\right)_{2^{t-1}} = -1$, we have that

$$\widetilde{\eta}_{2^t} = \begin{cases} \eta_{2^t} & \text{if } \ 2 \in A_{2^t} \\ \eta_{2^t}^{-1} & \text{if } \ 2 \in B_{2^t}. \end{cases}$$

Next, we show that $\widetilde{\eta}_{2^t} \in K_{2^{t-1}}$ by showing that it is fixed under all automorphisms $\sigma_r \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $r \in (\mathbb{Z}/p\mathbb{Z})^{\times 2^{t-1}}$. For such residues, we have $ra \equiv \pm a' \pmod{p}$ and $rb \equiv \pm b' \pmod{p}$, which gives

$$\sigma_r(\widetilde{\eta}_{2^t}) = \frac{\prod\limits_{b \in B_{2^t}} \left(\zeta_p^{rb} - \zeta_p^{-rb}\right)}{\prod\limits_{a \in A_{2^t}} \left(\zeta_p^{ra} - \zeta_p^{-ra}\right)} = (-1)^{\mu_{B_{2^t}} + \mu_{A_{2^t}}} \frac{\prod\limits_{b' \in B_{2^t}} \left(\zeta_p^{b'} - \zeta_p^{-b'}\right)}{\prod\limits_{a' \in A_{2^t}} \left(\zeta_p^{a'} - \zeta_p^{-a'}\right)},$$

where $\mu_{A_{2^t}}$ (respectively, $\mu_{B_{2^t}}$) counts the number of negatives resulting from $ra \equiv -a' \pmod{p}$ (respectively, $rb \equiv -b' \pmod{p}$). By Lemma 2.1, it follows that

$$\sigma_r(\widetilde{\eta}_{2^t}) = \left(\frac{r}{p}\right)_{2^t} \widetilde{\eta}_{2^t}.$$

Thus, we see that $\widetilde{\eta}_{2^t} \in K_{2^{t-1}} \cap \mathbb{Z}[\zeta_p] = \mathcal{O}_{K_2^{t-1}}$. Similarly, it can be shown that $\widetilde{\eta}_{2^t}^{-1} \in K_{2^{t-1}} \cap \mathbb{Z}[\zeta_p] = \mathcal{O}_{K_2^{t-1}}$ and we conclude that

$$\eta_{2^t}, \eta_{2^t}^{-1} \in K_{2^{t-1}} \cap \mathbb{Z}[\zeta_p] = \mathcal{O}_{K_2^{t-1}},$$

resulting in the claim of the theorem. □

The description of η_4 and the fact that

$$K_4 = \mathbb{Q}\left(\sqrt{\eta_4(-1)^{(p-1)/4}\sqrt{p}}\right)$$

when $p \equiv 1 \pmod{4}$ was shown in Proposition 5.9 and the discussion in Section 3.4 of Lemmermeyer's book [11], where it was subsequently used to prove Scholz's Reciprocity Law. The following theorem includes a proof of this claim along with its extension to describe the subfield K_{2^t} when $t \geq 3$.

Theorem 2.3. *If* $p \equiv 1 \pmod{2^t}$ *is prime with* $t \geq 2$ *and* $\left(\frac{2}{p}\right)_{2^{t-2}} = 1$, *then* $K_{2^t} = \mathbb{Q}(\alpha_{2^t})$, *where*

$$\alpha_{2^t} = \eta_{2^t}^{1/2} \eta_{2^{t-1}}^{1/4} \cdots \eta_4^{1/2^{t-1}} (-1)^{(p-1)/2^{t+1}} p^{(2^{t-1}-1)/2^t}$$

and K_{2^t} is the unique subfield of $\mathbb{Q}(\zeta_p)$ satisfying $[K_{2^t}:\mathbb{Q}]=2^t$.

Proof. We begin with the cases $t=2,3$ then proceed by induction on t. Define

$$N_{2^t}=\prod_{b\in B_{2^t}}\left(\zeta_{2p}^{b}-\zeta_{2p}^{-b}\right)\qquad\text{and}\qquad R_{2^t}=\prod_{a\in A_{2^t}}\left(\zeta_{2p}^{a}-\zeta_{2p}^{-a}\right)$$

so that $\eta_{2^t}=\frac{N_{2^t}}{R_{2^t}}$ for all $t\geq 2$. First consider the case when $p\equiv 1 \pmod 4$ and

$$\begin{aligned}N_4^2R_4^2&=\left(\prod_{b\in B_4}(\zeta_{2p}^{b}-\zeta_{2p}^{-b})\right)^2\left(\prod_{a\in A_4}(\zeta_{2p}^{a}-\zeta_{2p}^{-a})\right)^2\\&=\prod_{k=1}^{p-1}(\zeta_{2p}^{k}-\zeta_{2p}^{-k})=\prod_{k=1}^{p-1}\zeta_{2p}^{k}(1-\zeta_{p}^{-k})\\&=(-1)^{(p-1)/2}N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)=p.\end{aligned}$$

Then the sign of N_4R_4 is $(-1)^{(p-1)/4}$ resulting in

$$N_4R_4=(-1)^{(p-1)/4}p^{1/2}.$$

Substituting $N_4\eta_4^{-1}=R_4$, we have

$$N_4^2=\eta_4(-1)^{(p-1)/4}p^{1/2}\quad\Longrightarrow\quad N_4=\eta_4^{1/2}(-1)^{(p-1)/8}p^{1/4}.$$

Since $N_4\notin K_2$, but $N_4\in\mathbb{Q}(\zeta_p)$, and using the fact that $\mathbb{Q}(\zeta_p)$ is a cyclic extension of $\mathbb{Q}$, we see that $K_4=K_2(N_4)=\mathbb{Q}(N_4)$. Now for the $t=3$ case we assume $p\equiv 1 \pmod 8$, in which case we have $\left(\frac{2}{p}\right)=1$. Then

$$N_4^2R_4^2=N_4^2N_8^2R_8^2=p,$$

$$N_8^2R_8^2=\left(\eta_4(-1)^{(p-1)/4}p^{1/2}\right)^{-1}p=\eta_4^{-1}(-1)^{(p-1)/4}p^{1/2},$$

and

$$N_8R_8=\eta_4^{-1/2}(-1)^{(p-1)/8}p^{1/4}.$$

Using $\eta_8=\frac{N_8}{R_8}$, we have

$$N_8^2=\eta_8\eta_4^{-1/2}(-1)^{(p-1)/8}p^{1/4},$$

and

$$N_8=\eta_8^{1/2}\eta_4^{-1/4}(-1)^{(p-1)/16}p^{1/8}.$$

We handle the remaining cases by induction on $t\geq 3$. Suppose that for $k>3$, $p\equiv 1 \pmod{2^k}$, $\left(\frac{2}{p}\right)_{2^{k-2}}=1$, and

$$N_{2^{k-1}}=\eta_{2^{k-1}}^{1/2}\eta_{2^{k-2}}^{-1/4}\cdots\eta_4^{-1/2^{k-2}}(-1)^{(p-1)/2^k}p^{1/2^{k-1}}$$

is a primitive element for $K_{2^{k-1}}$. Using $\eta_{2^{k-1}} = \frac{N_{2^{k-1}}}{R_{2^{k-1}}}$, $\eta_{2^k} = \frac{N_{2^k}}{R_{2^k}}$, and $R_{2^{k-1}} = N_{2^k} R_{2^k} = N_{2^k}^2 \eta_{2^k}^{-1}$, we have

$$N_{2^k}^2 = \eta_{2^k} R_{2^{k-1}} = \eta_{2^k} N_{2^{k-1}} \eta_{2^{k-1}}^{-1},$$
$$N_{2^k}^2 = \eta_{2^k} \eta_{2^{k-1}}^{-1/2} \cdots \eta_4^{-1/2^{k-2}} (-1)^{(p-1)/2^k} p^{1/2^{k-1}},$$

and

$$N_{2^k} = \eta_{2^k}^{1/2} \eta_{2^{k-1}}^{-1/4} \cdots \eta_4^{-1/2^{k-1}} (-1)^{(p-1)/2^{k+1}} p^{1/2^k}.$$

Again applying the fact that $\mathrm{Gal}\,(\mathbb{Q}(\zeta_{\mathrm{p}})/\mathbb{Q})$ is cyclic we have that

$$K_{2^k} = K_{2^{k-1}}(N_{2^k}) = \mathbb{Q}(N_{2^k})$$

is the unique subfield of $\mathbb{Q}(\zeta_p)$ with $[K_{2^k} : \mathbb{Q}] = 2^k$. For our purposes, we will need the following description of K_{2^t}. Note that the element

$$\alpha_{2^t} = \prod_{j=2}^{t} N_{2^j}$$

is also a primitive element for K_{2^t} over $K_{2^{t-1}}$ and a simple inductive argument shows that

$$\alpha_{2^t} = \eta_{2^t}^{1/2} \eta_{2^{t-1}}^{1/4} \cdots \eta_4^{1/2^{t-1}} (-1)^{(p-1)/2^{t+1}} p^{(2^{t-1}-1)/2^t}$$

for all $t \geq 2$. □

3. Generalized Scholz-type reciprocity law

Before describing the main result, we need to explain the meaning of the symbol $\left(\frac{\eta}{\lambda}\right)_{2^t}$ whenever $p \equiv q \equiv 1 \pmod{2^t}$, $\left(\frac{p}{q}\right)_{2^{t-1}} = 1$, $\eta \in \mathcal{O}_{K_{2^{t-1}}}^{\times}$, and $\lambda \in \mathcal{O}_{K_{2^{t-1}}}$ is any prime above q. In this case, q splits completely in $\mathcal{O}_{K_{2^{t-1}}}$ and we have

$$\mathcal{O}_{K_{2^{t-1}}}/\lambda\mathcal{O}_{K_{2^{t-1}}} \cong \mathbb{Z}/q\mathbb{Z}.$$

Recall that if $\gamma, \delta \in \mathcal{O}_{K_{2^{t-1}}}$, we write

$$\gamma \equiv \delta \pmod{\lambda}$$

if and only if λ divides $\gamma - \delta$ (see Chapter 9, Section 2 of [5]). While this definition makes sense for γ and δ in the ring of integers of integers of any extension field of $K_{2^{t-1}}$, every element of $\mathcal{O}_{K_{2^{t-1}}}$ can be identified with a unique element from the set

$$\{0, 1, \ldots, q-1\}$$

since its elements are incongruent modulo λ and may therefore be used as coset representatives in $\mathcal{O}_{K_{2^{t-1}}}/\lambda\mathcal{O}_{K_{2^{t-1}}}$.

Let $a_\lambda \in \{0, 1, \ldots, q-1\}$ be the unique element (which depends upon the choice of λ) such that

$$\eta \equiv a_\lambda \pmod{\lambda}.$$

Whenever we have

$$a_\lambda^{(q-1)/2^{t-1}} \equiv 1 \pmod{q},$$

then one can define

$$\left(\frac{\eta}{\lambda}\right)_{2^t} := \left(\frac{a_\lambda}{q}\right)_{2^t} \equiv a_\lambda^{(q-1)/2^t} \pmod{q}.$$

Of course, the symbol $\left(\frac{\eta}{\lambda}\right)_{2^t}$ is only defined when $\left(\frac{\eta}{\lambda}\right)_{2^{t-1}} = 1$. This symbol is well-defined, but we must not forget its dependence on λ.

Next, we state our rational reciprocity law using the rational symbols defined above. The proof of the reciprocity law depends upon the splitting of the cyclotomic polynomial $\Phi_p(x)$ over the subfields $K_{2^{t-1}}$ and K_{2^t} and is modelled after the proof of quadratic reciprocity given after Proposition 3.4 in Lemmermeyer's book [11].

Theorem 3.1. *If $p \equiv q \equiv 1 \pmod{2^t}$ are distinct odd primes with $t \geq 2$ and*

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

then

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

where $\beta_{2^t} = \prod\limits_{k=2}^{t} \eta_{2^k}^{2^{k-2}} \in \mathcal{O}_{K_{2^{t-1}}}^\times$ and $\lambda \in \mathcal{O}_{K_{2^{t-1}}}$ is any prime above q.

Proof. Let p and q be primes satisfying the hypotheses of Theorem 3.1. The minimal polynomial of ζ_p over $K_{2^{t-1}}$ is given by

$$\varphi(x) = \prod_{r \in \mathcal{R}_{2^{t-1}}} (x - \zeta_p^r) \in \mathcal{O}_{K_{2^{t-1}}}[x],$$

where

$$\mathcal{R}_{2^{t-1}} = \left\{ 1 \leq r \leq p-1 \;\middle|\; \left(\frac{r}{p}\right)_{2^{t-1}} = 1 \right\}.$$

Factoring $\varphi(x)$ over $\mathcal{O}_{K_{2^t}}$, we obtain $\varphi(x) = \psi_1(x)\psi_2(x)$ where

$$\psi_1(x) \prod_{r \in \mathcal{R}_{2^t}} (x - \zeta_p^r) \quad \text{and} \quad \psi_2(x) = \prod_{n \in \mathcal{N}_{2^t}} (x - \zeta_p^n),$$

$\mathcal{R}_{2^t}$ is defined analogously to $\mathcal{R}_{2^{t-1}}$, and $\mathcal{N}_{2^t} = \mathcal{R}_{2^{t-1}} - \mathcal{R}_{2^t}$. Also define the polynomial

$$\vartheta(x) = \psi_1(x) - \psi_2(x) \in \mathcal{O}_{K_{2^t}}[x].$$

Let σ denote the nontrivial automorphism in $\mathrm{Gal}(K_{2^t}/K_{2^{t-1}})$, and note that $\sigma = \sigma_m|_{K_{2^t}}$ where

$$\sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_{2^{t-1}}) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

is the automorphism $\sigma_m(\zeta_p) = \zeta_p^m$ with $m \in \mathcal{N}_{2^t}$. It follows that

$$\sigma(\vartheta(x)) = -\vartheta(x)$$

and since $K_{2^t} = K_{2^{t-1}}(\alpha_{2^t})$, we have

$$\sigma(\alpha_{2^t}\vartheta(x)) = \alpha_{2^t}\vartheta(x) \in \mathcal{O}_{K_{2^{t-1}}}[x].$$

Thus, it is possible to write $\vartheta(x) = \alpha_{2^t}\phi(x)$ for some $\phi(x) \in \mathcal{O}_{K_{2^{t-1}}}[x]$. Following the discussion before Theorem 3.1, let λ denote any prime above q in $\mathcal{O}_{K_{2^{t-1}}}$. Consider the congruence

$$(\vartheta(x))^q = (\psi_1(x) - \psi_2(x))^q \equiv \left(\frac{q}{p}\right)_{2^t} \vartheta(x^q) \pmod{\lambda}, \tag{3.1}$$

which is actually defined on the ring $\mathcal{O}_{K_{2^t}}$. On the other hand, we have

$$(\vartheta(x))^q \equiv \alpha_{2^t}^q(\phi(x))^q \pmod{\lambda}.$$

By an analogue of Fermat's little theorem, whenever $\kappa \in \mathcal{O}_{K_{2^{t-1}}}$,

$$\kappa^q \equiv \kappa^{N(\lambda)-1}\kappa \equiv \kappa \pmod{\lambda},$$

where the norm map N is the norm of the field extension $K_{2^{t-1}}$ over $\mathbb{Q}$. Since $\phi(x) \in \mathcal{O}_{K_{2^{t-1}}}[x]$, we have

$$\begin{aligned}(\vartheta(x))^q &\equiv \alpha_{2^t}^{q-1}\alpha_{2^t}\phi(x^q) \pmod{\lambda} \\ &\equiv (\alpha_{2^t}^{2^t})^{(q-1)/2^t}\vartheta(x^q) \pmod{\lambda}.\end{aligned} \tag{3.2}$$

Comparing (3.1) and (3.2) gives

$$\left(\frac{q}{p}\right)_{2^t} \vartheta(x^q) \equiv (\alpha_{2^t}^{2^t})^{(q-1)/2^t}\vartheta(x^q) \pmod{\lambda}. \tag{3.3}$$

Next, we show that

$$\vartheta(X) = \psi_1(X) - \psi_2(X) \not\equiv 0 \pmod{\lambda}.$$

By Kummer's Theorem ([6], Theorem 7.4), the ideal generated by q in $\mathbb{Z}[\zeta_p]$ decomposes in exactly the same way as $\Phi_p(X)$ decomposes in $(\mathbb{Z}/q\mathbb{Z})[X]$. Since p and q are distinct primes, the ideal generated by q in $\mathbb{Z}[\zeta_p]$ is unramified. If

$$\varphi(X) \equiv (\psi_1(X))^2 \pmod{\lambda},$$

then we can pick $\{0, 1, \dots q-1\}$ as coset representatives of $\mathcal{O}_{K_{2^{t-1}}}/\lambda\mathcal{O}_{K_{2^{t-1}}} \cong \mathbb{Z}/q\mathbb{Z}$ 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 $\mathbb{Z}[\zeta_p]$. Thus, (3.3) simplifies to

$$\left(\frac{q}{p}\right)_{2^t} \equiv (\alpha_{2^t}^{2^t})^{(q-1)/2^t} \pmod{\lambda}, \tag{3.4}$$

and we note that $\alpha_{2^t} \in \mathcal{O}_{K_{2^{t-1}}}$, which can therefore be identified with an element in $\{0, 1, \dots, q-1\}$. The proof is completed by induction on $t \geq 2$. If $t = 2$, we have

$$\left(\frac{q}{p}\right)_4 \equiv (\alpha_4^4)^{(q-1)/4} \equiv \left(\frac{\eta_4^2 p}{\lambda}\right)_4 \pmod{\lambda}.$$

Both residue symbols only take on the values ±1 so that we have

$$\left(\frac{q}{p}\right)_4 = \left(\frac{\eta_4^2 p}{\lambda}\right)_4 = \left(\frac{\eta_4}{\lambda}\right)_2 \left(\frac{p}{\lambda}\right)_4 = \left(\frac{\eta_4}{\lambda}\right)_2 \left(\frac{p}{q}\right)_4$$

since $\left(\frac{p}{\lambda}\right)_4$ is independent of the choice of λ. Now suppose that the theorem holds for $t = k-1 \geq 2$, $p \equiv q \equiv 1 \pmod{2^k}$, and

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

In particular, we have

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

Then (3.4) gives

$$\left(\frac{q}{p}\right)_{2^k} \equiv (\alpha_{2^k}^{2^k})^{(q-1)/2^k} \equiv \left(\frac{\beta_{2^k}^2 p}{\lambda}\right)_{2^k} \equiv \left(\frac{\beta_{2^k}}{\lambda}\right)_{2^{k-1}} \left(\frac{p}{\lambda}\right)_{2^k} \pmod{\lambda}.$$

Again, the value of $\left(\frac{p}{\lambda}\right)_{2^k}$ is independent of the choice of λ and all of the residue symbols only take on the values ±1, resulting in

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

Finally, it should be noted that the symbol

$$\left(\frac{\beta_{2^k}}{\lambda}\right)_{2^{k-1}} = \left(\frac{\eta_{2^k}^{2^{k-2}} \beta_{2^{k-1}}}{\lambda}\right)_{2^{k-1}} = \left(\frac{\eta_{2^k}}{\lambda}\right) \left(\frac{\beta_{2^{k-1}}}{\lambda}\right)_{2^{k-1}}$$

is defined by the inductive hypothesis, completing the proof of the theorem. □

Theorem 3.1 holds regardless of the choice of prime λ above q. Noting that the left-hand side of the law is independent of λ, we see that the residuacity of β_{2^t} only depends upon the prime q. Hence, we may write

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

allowing us to interpret our law as a true rational reciprocity law.

When $p \equiv 1 \pmod 4$, it is known that $\eta_4 = \varepsilon_p^h$ for an odd integer h, and a proof can be found in Proposition 3.24 of [11]. In particular, if

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1,$$

then

$$\left(\frac{\beta_4}{\lambda}\right) = \left(\frac{\eta_4}{\lambda}\right) = \left(\frac{\varepsilon_p}{q}\right),$$

so that Theorem 3.1 results in Scholz's reciprocity law. The octic case of Theorem 3.1 states that if $p \equiv 1 \pmod 8$ and

$$\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1,$$

then

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{\beta_8}{\lambda}\right)_4 = \left(\frac{\eta_8}{\lambda}\right)\left(\frac{\eta_4}{\lambda}\right)_4.$$

The separation of the last residue symbol is justified since η_4 is a quadratic residue by Scholz's reciprocity law. Our law takes on a simpler form than that of Buell and Williams and comparing the two octic laws results in the following corollary.

Corollary 3.2. *If $p \equiv q \equiv 1 \pmod 8$ are distinct primes satisfying*

$$\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1,$$

then

$$\left(\frac{\eta_8}{\lambda}\right) = \left(\frac{\varepsilon_q}{p}\right)_4 (-N(\varepsilon_{pq}))^{h(pq)/4},$$

where $\lambda \in \mathcal{O}_{K_4}$ is any prime above q.

In conclusion, we note that Lemmermeyer commented at the end of [10] that he had "generalized Scholz's reciprocity law to all number fields with odd class number in the strict sense." Lemmermeyer's generalization has not been published, but has appeared in his online notes on class field towers. His generalization is quite different from ours and does not lend itself to an easy comparison. Despite the differences in the two generalizations, all of the work contained here was motivated by the techniques used by Lemmermeyer [11] leading up to his proof of Scholz's Reciprocity Law.

References

[1] D. Buell and K. Williams, *Is There an Octic Reciprocity Law of Scholz Type?*. Amer. Math. Monthly **85** (1978), 483–484.

[2] D. Buell and K. Williams, *An Octic Reciprocity Law of Scholz Type*. Proc. Amer. Math. Soc. **77** (1979), 315–318.

[3] D. Estes and G. Pall, *Spinor Genera of Binary Quadratic Forms*. J. Number Theory **5** (1973), 421–432.

[4] R. Evans, *Residuacity of Primes*. Rocky Mountain J. of Math. **19** (1989), 1069–1081.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. 2^{nd} edition, Graduate Texts in Mathematics **84**, Springer-Verlag, 1990.

[6] G. Janusz, *Algebraic Number Fields*. 2^{nd} ed., Graduate Studies in Mathematics **7**, American Mathematical Society, Providence, RI, 1996.

[7] E. Lehmer, *On the Quadratic Character of some Quadratic Surds*. J. Reine Angew. Math. **250** (1971), 42–48.

[8] E. Lehmer, *Generalizations of Gauss' Lemma*. Number Theory and Algebra, Academic Press, New York, 1977, 187–194.

[9] E. Lehmer, *Rational Reciprocity Laws*. Amer. Math. Monthly **85** (1978), 467–472.

[10] F. Lemmermeyer, *Rational Quartic Reciprocity*. Acta Arith. **67** (1994), 387–390.

[11] F. Lemmermeyer, *Reciprocity Laws*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[12] A. Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$*. Math. Z. **39** (1934), 95–111.

[13] 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.

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

[15] 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.

Mark Budden
Department of Mathematics
Armstrong Atlantic State University
11935 Abercorn St.
Savannah, GA USA 31419
E-mail : Mark.Budden@armstrong.edu
URL: http://www.math.armstrong.edu/faculty/budden

Jeremiah Eisenmenger
Department of Mathematics
University of Florida
PO Box 118105
Gainesville, FL USA 32611-8105
E-mail : eisenmen@math.ufl.edu

Jonathan Kish
Department of Mathematics
University of Colorado at Boulder
Boulder, CO USA 80309
E-mail : jonathan.kish@colorado.edu