ACTA ARITHMETICA
129.4 (2007)

A supplement to Scholz's reciprocity law

by

Franz Lemmermeyer (Jagstzell)

1. Introduction. Let us start by fixing some notation:

- p and q denote primes $\equiv 1 \bmod 4$;
- $h(d)$ denotes the class number (in the usual sense) of the quadratic number field with discriminant d;
- $\mathcal{O}_p$ and $\mathcal{O}_q$ denote the rings of integers in $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$;
- ε_p and ε_q denote the fundamental units of $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$, respectively;
- $[\alpha/\mathfrak{p}]$ denotes the quadratic residue symbol in a quadratic number field; recall that it takes values ± 1 and is defined for ideals $\mathfrak{p} \nmid 2\alpha$ by $[\alpha/\mathfrak{p}] \equiv \alpha^{(N\mathfrak{p}-1)/2} \bmod \mathfrak{p}$.

Given primes $p \equiv q \equiv 1 \bmod 4$ with $(p/q) = +1$, we have $p\mathcal{O}_q = \mathfrak{p}\mathfrak{p}'$ and $q\mathcal{O}_p = \mathfrak{q}\mathfrak{q}'$; the symbol $[\varepsilon_p/\mathfrak{q}]$ does not depend on the choice of $\mathfrak{q}$, so we can simply denote it by (ε_p/q). Scholz's reciprocity law then says that we always have $(\varepsilon_p/q) = (\varepsilon_q/p)$ (for details, see [5–7]). Scholz's reciprocity law was first proved by Schönemann [13], and then rediscovered by Scholz [11] (Scholz mentioned his reciprocity law and the connection to the parity of the class number of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ in a letter to Hasse from Aug. 25, 1928; see [10]). In [12], Scholz found that in fact $(\varepsilon_p/q) = (\varepsilon_q/p) = (p/q)_4(q/p)_4$, and showed that these residue symbols are connected to the structure of the 2-class group of $\mathbb{Q}(\sqrt{pq})$.

2. Hilbert's supplementary laws. To extend these results we have to recall the notions of primary and hyper-primary integers (see Hecke [3]).

Lemma 1. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\alpha \in \mathcal{O}_K$ be an element with odd norm. Then the following assertions are equivalent*:

2000 *Mathematics Subject Classification*: Primary 11R21; Secondary 11R29, 11R18.
Key words and phrases: quadratic number field, reciprocity law, 2-class group.

(1) $\alpha \gg 0$ *is totally positive and* $\alpha \equiv \xi^2 \bmod 4$ *for some* $\xi \in \mathcal{O}_K$;
(2) *the extension* $K(\sqrt{\alpha})/K$ *is unramified at all primes above* 2∞.

If the conditions of Lemma 1 are satisfied, we say that α is *primary*.

LEMMA 2. *Assume that* $2\mathcal{O}_K = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_r^{e_r}$; *then the following assertions are equivalent*:

(1) α *is primary, and* $\alpha \equiv \xi^2 \bmod \mathfrak{l}_j^{2e_j+1}$ *for all* j;
(2) *every prime above* 2 *splits in the extension* $K(\sqrt{\alpha})/K$.

If the conditions of Lemma 2 are satisfied, we say that α is *hyper-primary*. Observe that the conditions in (1) are equivalent to $\alpha \equiv \xi^2 \bmod 4\mathfrak{l}_1 \cdots \mathfrak{l}_r$. Also note α is allowed to be a square in Lemmas 1 and 2.

Our next result is related to the First Supplementary Law of quadratic reciprocity for fields with odd class number; it was stated and proved in a special case by Hilbert ([4]), and proved in full generality by Furtwängler. Nowadays, this result is almost forgotten; for a proof of Hilbert's Supplementary Laws (for arbitrary number fields) based on class field theory, see [9]; Hecke [3, Thm. 171] gives a proof based on his theory of Gauss sums and theta functions over algebraic number fields.

THEOREM 1 (Hilbert's First Supplementary Law). *Let* $\mathfrak{a}$ *be an ideal of odd norm in some number field* k *with odd class number* h, *and let* $(\cdot/\cdot)$ *denote the quadratic residue symbol in* $\mathcal{O}_k$. *Then the following assertions are equivalent*:

(1) $(\varepsilon/\mathfrak{a}) = +1$ *for all units* $\varepsilon \in \mathcal{O}_k^\times$;
(2) $\mathfrak{a}^h = (\alpha)$ *for some primary* $\alpha \in \mathcal{O}_k$.

Hilbert calls an ideal $\mathfrak{a}$ with odd norm *primary* if condition (1) above is satisfied, i.e., if $(\varepsilon/\mathfrak{a}) = +1$ for all units ε in k. Hilbert's Second Supplementary Law can be given the following form:

THEOREM 2 (Hilbert's Second Supplementary Law). *Let* $\mathfrak{a}$ *be a primary ideal of odd norm in some number field* k *with odd class number* h. *Then the following assertions are equivalent*:

(1) $(\lambda/\mathfrak{a}) = +1$ *for all* $\lambda \in \mathcal{O}_k$ *whose prime divisors consist only of primes above* 2;
(2) $\mathfrak{a}^h = (\alpha)$ *for some primary* $\alpha \in \mathcal{O}_k$.

Hilbert calls ideals satisfying condition (1) above *hyper-primary*. A proof of a generalization of Theorem 2 to arbitrary number fields can be found in [3, Thm. 175]. Now we can state

THEOREM 3. *Let* $p \equiv q \equiv 1 \bmod 4$ *be primes with* $(p/q) = +1$. *Then* $p\mathcal{O}_q = \mathfrak{p}\mathfrak{p}'$ *and* $q\mathcal{O}_p = \mathfrak{q}\mathfrak{q}'$ *split. The class numbers* $h(p)$ *and* $h(q)$ *are odd,*

and there exist elements $\pi \in \mathcal{O}_q$ *and* $\varrho \in \mathcal{O}_p$ *such that* $\mathfrak{p}^{h(p)} = (\pi)$ *and* $\mathfrak{q}^{h(q)} = (\varrho)$. *Then the following assertions are equivalent*:

(1) $(\varepsilon_p/q) = +1$;
(2) ϱ *can be chosen primary*;
(3) $h(pq) \equiv 0 \bmod 4$.

Proof. Genus theory (see e.g. [7, Chap. 2]) implies that $h(p) \equiv h(q) \equiv 1 \bmod 2$. The equivalence (1)⇔(2) is a special case of Hilbert's First Supplementary Law for fields with odd class number ([4]); observe, however, that Hilbert stated and proved this law only for a very narrow class of fields—the general statement was proved only by Furtwängler. The equivalence (1)⇔(3) is due to Scholz [12].

It is not hard to prove these statements directly using class field theory; below we will do this in an analogous situation. ∎

Observe that part (3) of Theorem 3 is symmetric in p and q, which immediately implies Scholz's reciprocity law $(\varepsilon_p/q) = (\varepsilon_q/p)$. Note that we can state this reciprocity law in the following form:

Corollary 1. *Let* p *and* q *satisfy the assumptions of Theorem* 3. *If the ideals above* q *in* $\mathbb{Q}(\sqrt{p})$ *are primary, then so are the ideals above* p *in* $\mathbb{Q}(\sqrt{q})$.

In the next section we will prove an analogous result connected to Hilbert's Second Supplementary Law of Quadratic Reciprocity.

3. A supplement to Scholz's reciprocity law. Assume that $p \equiv q \equiv 1 \bmod 8$ are primes. Then 2 splits in $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$, and we can write $2\mathcal{O}_p = \mathfrak{ll}'$ and $2\mathcal{O}_q = \mathfrak{mm}'$. Now pick elements λ_p, λ_q such that $\mathfrak{l}^{h(p)} = (\lambda_p)$ and $\mathfrak{m}^{h(q)} = (\lambda_q)$. Since both fields have units with independent signatures, we may assume that $\lambda_p, \lambda_q \gg 0$. The quadratic residue symbol $[\lambda_p/\mathfrak{q}]$, where $q\mathcal{O}_p = \mathfrak{qq}'$, does not depend on the choice of λ_p or $\mathfrak{q}$, so we may denote it by (λ_p/q).

Theorem 4. *Let* $p \equiv q \equiv 1 \bmod 8$ *be primes with* $(p/q) = +1$, *and assume that* $(\varepsilon_p/q) = (\varepsilon_q/p) = +1$. *Then the following assertions are equivalent*:

(1) $(\lambda_p/q) = +1$;
(2) ϱ *can be chosen hyper-primary*;
(3) *the ideal classes generated by the ideals above* 2 *in* $F = \mathbb{Q}(\sqrt{pq})$ *are fourth powers in* $\mathrm{Cl}(F)$.

Proof. Let $F = \mathbb{Q}(\sqrt{pq})$; then $F_1 = F(\sqrt{p})$ is an unramified quadratic extension; since ϱ is primary, the extension $F(\sqrt{\varrho})/F$ is unramified, and it is easily checked that it is the unique cyclic quartic unramified extension

of F. Since 2 splits completely in $\mathbb{Q}(\sqrt{p},\sqrt{q})/\mathbb{Q}$, it will split completely in $F(\sqrt{\varrho})/\mathbb{Q}$ if and only if 2 splits completely in $\mathbb{Q}(\sqrt{p},\sqrt{\varrho})$, which happens if and only if ϱ is hyper-primary. On the other hand, the decomposition law in unramified abelian extensions shows that the prime ideals above 2 split completely in $F(\sqrt{\varrho})/F$ if and only if their ideal classes are fourth powers in $\mathrm{Cl}(F)$. This proves that (2)⇔(3).

The equivalence (1)⇔(2) is a special case of the Second Supplementary Law of Hilbert's Quadratic Reciprocity Law in number fields with odd class number. Here is a direct argument using class field theory.

Consider the quadratic extension $K = F(\sqrt{\varrho})$ of F. Then ϱ is hyper-primary if and only if the prime $\mathfrak{l}$ (and, therefore, also its conjugate $\mathfrak{l}'$) above 2 splits in K/F. Since K is the unique quadratic subextension of the ray class field modulo $\mathfrak{q}$ over F, which has degree $2h(p)$, the prime $\mathfrak{l}$ will split in K/F if and only if $\mathfrak{l}^{h(p)} = (\lambda_p)$ for some $\lambda_p \equiv \xi^2 \bmod \mathfrak{q}$. This shows that (1)⇔(2). ∎

The symmetry of p and q in the third statement of Theorem 4 then implies

Corollary 2. *We have* $(\lambda_p/q) = (\lambda_q/p)$.

While the proof of Theorem 4 required class field theory, the actual reciprocity law in Corollary 2 can be proved with elementary means. We will now give a proof à la Brandler [1]. To this end, write $\lambda_p = (a + b\sqrt{p})/2$; then $a^2 - pb^2 = 2^u$, where $u = h(p) + 2 = 2m + 1$ is odd. From $a^2 - 2^u = pb^2$ we find that $a + 2^m\sqrt{2} = \pi_2\beta^2$ and $a - 2^m\sqrt{2} = \pi_2'\beta'^2$, where $\pi_2\pi_2' = p$ for some totally positive $\pi_2 \equiv 1 \bmod 2$. Moreover $\beta\beta' = b$ and $2a = \pi\beta^2 + \pi'\beta'^2$.

Now $(\pi_2\beta + \beta'\sqrt{p}\,)^2 = \pi_2(\pi\beta^2 + \pi_2'\beta'^2 + 2y\sqrt{p}\,) = 2\pi_2\lambda$. Standard arguments then show that $[\pi_2/\varrho_2] = (\lambda/q)$, where $\varrho_2\varrho_2' = q$.

The quadratic reciprocity law in $\mathbb{Z}[\sqrt{2}\,]$ shows that $[\pi_2/\varrho_2] = [\varrho_2/\pi_2]$, and this implies the following elementary form of the supplement to Scholz's reciprocity law:

$$\left(\frac{\lambda_p}{q}\right) = \left[\frac{\pi_2}{\varrho_2}\right] = \left[\frac{\varrho_2}{\pi_2}\right] = \left(\frac{\lambda_q}{p}\right).$$

4. Additional remarks. We close this article with a few remarks and questions.

Remark 1. Since $p \equiv q \equiv 1 \bmod 8$, we can also write $p = N\pi_2^*$ and $q = N\varrho_2^*$ for elements $\pi_2^*, \varrho_2^* \in \mathbb{Z}[\sqrt{-2}\,]$ with $\pi_2^* \equiv \varrho_2^* \equiv 1 \bmod 2$. Then [8, Prop. 2] states that

$$\left[\frac{\pi_2}{\varrho_2}\right]\left[\frac{\pi_2^*}{\varrho_2^*}\right] = \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4.$$

Under the assumptions of Theorem 4, this means that

$$\left(\frac{\lambda_p}{q}\right) = \left(\frac{\lambda_q}{p}\right) = \left[\frac{\pi_2}{\varrho_2}\right] = \left[\frac{\pi_2^*}{\varrho_2^*}\right].$$

REMARK 2. Hilbert's Supplementary Law as we have stated it applies to all (quadratic) fields with odd class number, not just the fields with prime discriminant. Here we give an example that shows what to expect in this more general situation.

Consider primes $p \equiv q \equiv 3 \bmod 4$ and primes $r \equiv 1 \bmod 4$ with $(pq/r) = +1$. Let ε_{pq} denote the fundamental unit in $k = \mathbb{Q}(\sqrt{pq})$. Then the prime ideals $\mathfrak{r}$ and $\mathfrak{r}'$ above r in k satisfy $\mathfrak{r}^{h(pq)} = (\varrho)$ for some primary ϱ if and only if $(\varepsilon_{pq}/r) = +1$. Since $p\varepsilon_{pq}$ is a square in k, we have $(\varepsilon_{pq}/r) = (p/r)$.

Assume now that ϱ can be chosen primary, and consider the dihedral extension $L/\mathbb{Q}$ with $L = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{\varrho})$. Clearly ϱ is primary if and only if $L/\mathbb{Q}(\sqrt{pqr})$ is cyclic and unramified. It is then easy to show that the quadratic extensions of $\mathbb{Q}(\sqrt{r})$ different from $\mathbb{Q}(\sqrt{pq}, \sqrt{r})$ can be generated by a primary element α with prime ideal factorization $(\mathfrak{pq})^{h(r)}$ for a suitable choice of prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ above p and q, respectively. Note that if $\mathfrak{pq}$ is primary, then $\mathfrak{pq}'$ is not, since $\mathfrak{qq}' = (q)$ is not primary (we have either $q < 0$ or $q \equiv 3 \bmod 4$).

The upshot of this discussion is: if ϱ is primary, then exactly one of the ideals $\mathfrak{pq}$ and $\mathfrak{pq}'$ is primary, say the first one, and then Hilbert's Supplementary Law shows that $(\varepsilon_r/pq) := [\varepsilon_r/\mathfrak{pq}] = +1$. Conversely, if $\mathfrak{pq}$ is primary, then $(\varepsilon_r/pq) = (\varepsilon_{pq}/r) = +1$. We have shown:

PROPOSITION 1. *Let $p \equiv q \equiv 3 \bmod 4$ and $r \equiv 1 \bmod 4$ be primes with $(pq/r) = +1$. Then the following assertions are equivalent*:

(1) $(\varepsilon_{pq}/r) = +1$;
(2) $(p/r) = +1$;
(3) *the ideal $\mathfrak{r}$ in $\mathbb{Q}(\sqrt{pq})$ above r is primary*;
(4) $h(pqr) \equiv 0 \bmod 4$;
(5) *there is a unique primary ideal $\mathfrak{a}$ (up to conjugation) of norm pq in $\mathbb{Q}(\sqrt{r})$, and $(\varepsilon_r/pq) := [\varepsilon_r/\mathfrak{a}] = +1$.*

Note that (ε_r/pq) is not well defined if $(p/r) = -1$ since in this case we do not have a canonical way to single out the prime ideals above p and q in $\mathbb{Q}(\sqrt{r})$.

As an example, consider the case $p = 3$, $q = 7$, $r = 37$; then the elements of norm 21 in the ring of integers in $\mathbb{Q}(\sqrt{37})$ are $\pm 13 \pm 2\sqrt{37}$ (these elements are not primary: the element $-13 + 2\sqrt{37} \equiv 1 \bmod 4$ is not totally positive) and $(\pm 11 \pm \sqrt{37})/2$. It is easy to check that $\beta = (11 + \sqrt{37})/2$ is primary; now $\varepsilon_r = 6 + \sqrt{37}$, and $[\varepsilon_r/\beta] = (-5/21) = +1$ as claimed, whereas $[\varepsilon_r/(13 \pm 2\sqrt{37})] = -1$.

REMARK 3. Above we have seen that, under suitable assumptions, the ideal class generated by a prime above 2 in $\mathbb{Q}(\sqrt{pq})$ is a fourth power in the class group if and only if $[\pi_2/\varrho_2] = +1$, where $\pi_2, \varrho_2 \in \mathbb{Z}[\sqrt{2}]$ are elements $\equiv 1 \bmod 2$ with norms p and q, respectively. Does an analogous statement hold with 2 replaced by an odd prime $\ell \neq p, q$?

REMARK 4. Budden, Eisenmenger & Kish [2] have generalized Scholz's reciprocity law to higher powers; can the reciprocity law $(\lambda_p/q) = (\lambda_q/p)$ proved above also be generalized in this direction?

References

[1] J. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory 5 (1973), 271–287.

[2] M. Budden, J. Eisenmenger and J. Kish, *A generalization of Scholz's reciprocity law*, J. Théor. Nombres Bordeaux, to appear.

[3] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

[4] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Ann. 51 (1899), 1–127.

[5] F. Lemmermeyer, *Rational quartic reciprocity*, Acta Arith. 67 (1994), 387–390.

[6] —, *Rational quartic reciprocity. II*, ibid. 80 (1997), 273–276.

[7] —, *Reciprocity Laws. From Euler to Eisenstein*, Springer, 2000.

[8] —, *Some families of non-congruent numbers*, Acta Arith. 110 (2003), 15–36.

[9] —, *Selmer groups and quadratic reciprocity*, Abh. Math. Sem. Hamburg 76 (2006), 279–293.

[10] —, *Die Korrespondenz Hasse–Scholz*, in preparation.

[11] A. Scholz, *Zwei Bemerkungen zum Klassenkörperturm*, J. Reine Angew. Math. 161 (1929), 201–207.

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

[13] Th. Schönemann, *Ueber die Congruenz* $x^2 + y^2 \equiv 1 \pmod{p}$, J. Reine Angew. Math. 19 (1839), 93–112.

Mörikeweg 1
73489 Jagstzell, Germany
E-mail: hb3@ix.urz.uni-heidelberg.de

Received on 12.9.2006 (5298)