ACTA ARITHMETICA
LXXX.3 (1997)

Rational quartic reciprocity II

by

FRANZ LEMMERMEYER (Saarbrücken)

1. Introduction. Let $m = p_1 \dots p_r$ be a product of primes $p_i \equiv 1 \bmod 4$ and assume that there are integers $A, B, C \in \mathbb{Z}$ such that $A^2 = m(B^2 + C^2)$ and $A - 1 \equiv B \equiv 0 \bmod 2$, $A + B \equiv 1 \bmod 4$. Then

$$\left(\frac{A + B\sqrt{m}}{p}\right) = \left(\frac{p}{m}\right)_4 \tag{1}$$

for every prime $p \equiv 1 \bmod 4$ such that $(p/p_j) = +1$ for all $1 \le j \le r$. This is "the extension to composite values of m" that was referred to in [3], to which this paper is an addition. Here I will fill in the details of the proof, on the one hand because I was requested to do so, and on the other hand because this general law can be used to derive general versions of Burde's and Scholz's reciprocity laws.

Below I will sketch an elementary proof of (1) using induction built on the results of [3], and then use the description of abelian fields by characters to give a direct proof.

2. Proof by induction. Using induction over the number of prime factors of m we may assume that (1) is true if m has r different prime factors.

Now assume that $m = p_1 m'$; we choose integers A, B, A_1, B_1 such that B and B_1 are even, $A + B \equiv A_1 + B_1 \equiv 1 \bmod 4$, $A^2 = m(B^2 + C^2)$, $A_1^2 = p_1(B_1^2 + C_1^2)$, and put $\alpha = A + B\sqrt{m}$ and $\alpha_1 = A_1 + B_1\sqrt{p_1}$. Then $K = \mathbb{Q}(\sqrt{\alpha})$ and $K_1 = \mathbb{Q}(\sqrt{\alpha_1})$ are cyclic quartic extensions of conductors m and p_1, respectively.

Consider the compositum K_1K; it is an abelian extension of type $(4, 4)$ over $\mathbb{Q}$, and it clearly contains $F = \mathbb{Q}(\sqrt{m'}, \sqrt{p_1})$. Moreover, F has three quadratic extensions in K_1K, namely $F(\sqrt{\alpha})$, $F(\sqrt{\alpha_1})$, and $L = F(\sqrt{\alpha\alpha_1})$. It is not hard to see that L is the compositum of a cyclic quartic extension $\mathbb{Q}(\sqrt{\alpha'})$ of conductor m' and $\mathbb{Q}(\sqrt{p_1})$. Since $\alpha\alpha_1$ and α' differ at most by

1991 *Mathematics Subject Classification*: 11R16, 11A15.

a square in F, we find $(\alpha'/p) = (\alpha/p)(\alpha_1/p)$. On the other hand, by the induction hypothesis we have $(\alpha'/p) = (p/m')_4$, hence we find

$$\left(\frac{\alpha}{p}\right) = \left(\frac{\alpha'}{p}\right)\left(\frac{\alpha_1}{p}\right) = \left(\frac{p}{m'}\right)_4\left(\frac{p}{p_1}\right)_4 = \left(\frac{p}{m}\right)_4.$$

This is what we wanted to prove.

3. Proof via characters. Let K be a cyclotomic field with conductor f. Then it is well known (see [6] for the necessary background) that the subfields of $\mathbb{Q}(\zeta_f)$ correspond biuniquely to the subgroups of the character group of $(\mathbb{Z}/f\mathbb{Z})^\times$.

Let $m = p_1 \dots p_r$ be a product of primes $p \equiv 1 \bmod 4$, and let ϕ_j denote the quadratic character modulo p_j. There exist two quartic characters modulo p_j, namely ω_j (say) and $\omega_j^{-1} = \phi_j\omega_j$; for primes p such that $\chi_j(p) = (p/p_j) = +1$ we have $\omega_j(p) = (p/p_j)_4$.

The quadratic subfield $\mathbb{Q}(\sqrt{m})$ of $L = \mathbb{Q}(\zeta_m)$ corresponds to the subgroup $\langle\phi\rangle$, where $\phi = \phi_1 \dots \phi_r$; similarly, there is a cyclic quartic extension K contained in L which corresponds to $\langle\omega\rangle$, where ω is a character of order 4 and conductor m. Moreover, K contains $\mathbb{Q}(\sqrt{m})$, hence we must have $\omega^2 = \phi$. This implies at once that $\omega = \omega_1 \dots \omega_r \cdot \phi'$, where ϕ' is a suitably chosen quadratic character. By the decomposition law in abelian extensions a prime p splitting in $\mathbb{Q}(\sqrt{m})$ will split completely in K if and only if $\omega(p) = +1$, i.e. if and only if $(p/m)_4 = +1$ (the quadratic character ϕ' does not influence the splitting of p since $\phi'(p) = 1$).

By comparing this with the decomposition law in Kummer extensions we see immediately that (1) holds.

Remark. If we define $(p/2)_4 = (-1)^{(p-1)/8}$ for all primes $p \equiv 1 \bmod 8$, then the above proofs show that (1) is also valid for even m; one simply has to replace the cyclic quartic extension of conductor p by the totally real cyclic quartic extension of conductor 8, i.e. the real quartic subfield of $\mathbb{Q}(\zeta_{16})$.

4. Some rational quartic reciprocity laws

Burde's reciprocity law. Let m and n be coprime integers, and assume that $m = \prod p_i$ and $n = \prod q_j$ are products of primes $\equiv 1 \bmod 4$. Assume moreover that $(m/q_j) = (n/p_i) = +1$ for all p_i and q_j. Write $m = a^2 + b^2$, $n = c^2 + d^2$ with ac odd; then we can prove as in [3] that

$$\left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4 = \left(\frac{ac-bd}{m}\right) = \left(\frac{ac-bd}{n}\right).$$

Remark. It is easy to deduce Gauss' criterion for the biquadratic character of 2 from Burde's law. In fact, assume that $p = a^2 + 16b^2 \equiv 1 \bmod 8$

is prime, and choose the sign of a in such a way that $a \equiv 1 \bmod 4$; then

$$\left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4 = \left(\frac{a-4b}{2}\right) = \left(\frac{2}{a-4b}\right).$$

Since $(p/2) = (-1)^{(p-1)/8}$ and $p-1 = a^2-1+16b^2 \equiv (a-1)(a+1) \bmod 16$ we find

$$\frac{p-1}{8} = \frac{a-1}{4}\cdot\frac{a+1}{2} \equiv \frac{a-1}{4} \bmod 2,$$

and this gives $(-1)^{(p-1)/8} = (2/a)$. Thus

$$\left(\frac{2}{p}\right)_4 = \left(\frac{2}{a}\right)\left(\frac{2}{a+4b}\right) = \left(\frac{2}{a^2+4b}\right) = \left(\frac{2}{1+4b}\right) = (-1)^b.$$

Scholz's reciprocity law. Let $\varepsilon_m = t + u\sqrt{m}$ be a unit in $\mathbb{Q}(\sqrt{m})$ with norm -1. Putting $\varepsilon_m\sqrt{m} = A + B\sqrt{m}$ we find immediately

$$\left(\frac{\varepsilon_m}{p}\right) = \left(\frac{m}{p}\right)_4\left(\frac{p}{m}\right)_4 \tag{2}$$

for all primes $p \equiv 1 \bmod 4$ such that $(p_j/p) = 1$ for all $p_j \mid m$. If n is a product of such primes p, this implies

$$\left(\frac{\varepsilon_m}{n}\right) = \left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4.$$

Moreover, if the fundamental unit of $\mathbb{Q}(\sqrt{n})$ has negative norm, we conclude that

$$\left(\frac{\varepsilon_m}{n}\right) = \left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4 = \left(\frac{\varepsilon_n}{m}\right).$$

The general version of Scholz's reciprocity law has a few nice corollaries:

COROLLARY 1. *Let m and n satisfy the conditions above, and suppose that $m = rs$; assume moreover that the fundamental units ε_r and ε_s of $\mathbb{Q}(\sqrt{r})$ and $\mathbb{Q}(\sqrt{s})$ have negative norm. Then*

$$\left(\frac{\varepsilon_m}{n}\right) = \left(\frac{\varepsilon_r}{n}\right)\left(\frac{\varepsilon_s}{n}\right).$$

Proof. This is a simple computation:

$$\left(\frac{\varepsilon_m}{n}\right) = \left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4 = \left(\frac{r}{n}\right)_4\left(\frac{n}{r}\right)_4\left(\frac{s}{n}\right)_4\left(\frac{n}{s}\right)_4 = \left(\frac{\varepsilon_r}{n}\right)\left(\frac{\varepsilon_s}{n}\right),$$

where we have twice applied (2).

COROLLARY 2. *Let $m = p_1 \ldots p_t$ and n satisfy the conditions above. Then $(\varepsilon_m/n) = (\varepsilon_1/n)\ldots(\varepsilon_t/n)$, where ε_j denotes the fundamental unit in $\mathbb{Q}(\sqrt{p_j})$.*

This is a result due to Furuta [1]; its proof is clear.

5. Some remarks on the 4-rank of class groups. The reciprocity laws given above are connected with the 4-rank of class groups: let k be a real quadratic number field of discriminant d, and assume that d can be written as a sum of two squares. It is well known ([5]) that the quadratic unramified extensions of k correspond to factorizations $d = d_1 d_2$ of d into two relatively prime discriminants d_1, d_2 with at least one of the d_i positive, and that cyclic quartic extensions which are unramified outside ∞ correspond to C_4-extensions $d = d_1 d_2$, where $(d_1/p_2) = (d_2/p_1) = +1$ for all primes $p_j \mid d_j$.

Let $K = k(\sqrt{\alpha})$ be such an extension, corresponding to $d = d_1 d_2$. Then any quartic cyclic extension of k which contains $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and which is unramified outside ∞ has the form $K' = k(\sqrt{d'\alpha})$, where d' is a product of prime discriminants occurring in the factorization of d as a product of prime discriminants. Since these prime discriminants are all positive, either all of these extensions K'/k are totally real, or all of them are totally complex. Scholz [5] has sketched a proof for the fact that the K' are totally real if and only if $(d_1/d_2)_4 = (d_2/d_1)_4$; an elementary proof was given in [4].

In addition to the references given in [3] we should remark that Kaplan [2] has also proved the general version of Burde's reciprocity law and noticed the connection with the structure of the 2-class groups of real quadratic number fields.

References

[1] Y. Furuta, *Norms of units of quadratic fields*, J. Math. Soc. Japan 11 (1959), 139–145.

[2] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1974), 313–363.

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

[4] —, *The 4-class group of real quadratic number fields*, submitted.

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

[6] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1982.

Fachbereich Informatik
Universität des Saarlandes
D-66041 Saarbrücken, Germany
E-mail: lemmermf@cs.uni-sb.de

Received on 9.10.1996
and in revised form on 23.12.1996 (3060)