ACTA ARITHMETICA
LXVII.4 (1994)

Rational quartic reciprocity

by

FRANZ LEMMERMEYER (Heidelberg)

In 1985, K. S. Williams, K. Hardy and C. Friesen [11] published a reciprocity formula that comprised all known rational quartic reciprocity laws. Their proof consisted in a long and complicated manipulation of Jacobi symbols and was subsequently simplified (and generalized) by R. Evans [3]. In this note we give a proof of their reciprocity law which is not only considerably shorter but also sheds some light on the raison d'être of rational quartic reciprocity laws. For a survey on rational reciprocity laws, see E. Lehmer [7].

We want to prove the following

THEOREM. *Let* $m \equiv 1 \bmod 4$ *be a prime*, *and let* A, B, C *be integers such that*

$$A^2 = m(B^2 + C^2), \quad 2 \mid B,$$
$$(A, B) = (B, C) = (C, A) = 1, \quad A + B \equiv 1 \bmod 4.$$

Then, *for every odd prime* $p > 0$ *such that* $(m/p) = +1$,

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

Proof. Let $k = \mathbb{Q}(\sqrt{m})$; then $K = \mathbb{Q}(\sqrt{m}, \sqrt{A + B\sqrt{m}})$ is a quartic cyclic extension of $\mathbb{Q}$ containing k, as can be verified quickly by noting that $A^2 - mB^2 = mC^2 = (\sqrt{m}C)^2$ and $\sqrt{m}C \in k \setminus \mathbb{Q}$. We claim that K is the quartic subfield of $\mathbb{Q}(\zeta_m)$, the field of mth roots of unity. This will follow from the theorem of Kronecker and Weber once we have seen that no prime $\neq m$ is ramified in $K/\mathbb{Q}$. But the identity

$$2(A + B\sqrt{m})(A + C\sqrt{m}) = (A + B\sqrt{m} + C\sqrt{m})^2 \tag{2}$$

shows $K = k(\sqrt{2(A + C\sqrt{m})})$, and so the only odd primes that are possibly ramified in K/k are common divisors of $A^2 - mB^2 = mC^2$ and $A^2 - mC^2 = mB^2$. Since B and C are assumed to be prime to each other, only 2 and m can ramify. Now $\sqrt{m} \equiv 1 \bmod 2$ (since $m \equiv 1 \bmod 4$) implies $B\sqrt{m} \equiv B \bmod 4$, and we see $A + B\sqrt{m} \equiv A + B \equiv 1 \bmod 4$, which shows that 2 is not ramified in K/k (and therefore not ramified in $K/\mathbb{Q}$).

The reciprocity formula will follow by comparing the decomposition laws in $K/\mathbb{Q}$ and $\mathbb{Q}(\zeta_m)/\mathbb{Q}$: if $(m/p) = +1$, then p splits in $k/\mathbb{Q}$; if $f > 0$ is the smallest natural number such that $p^f \equiv 1 \bmod m$ (here we have to assume $p > 0$), then p splits into exactly $g = (m-1)/f$ prime ideals in $\mathbb{Q}(\zeta_m)$, and

$$\begin{aligned}\left(\frac{p}{m}\right)_4 = 1 \ &\Leftrightarrow p^{(m-1)/4} \equiv 1 \bmod m \Leftrightarrow f \text{ divides } \tfrac{1}{4}(m-1) = \tfrac{1}{4}fg \\ &\Leftrightarrow g \equiv 0 \bmod 4 \\ &\Leftrightarrow \text{the degree of the decomposition field } Z \text{ of } p \\ &\qquad \text{is divisible by } 4 \\ &\Leftrightarrow Z \text{ contains } K \text{ (because } \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \text{ is cyclic)} \\ &\Leftrightarrow p \text{ splits completely in } K/\mathbb{Q} \\ &\Leftrightarrow p \text{ splits completely in } K/k \text{ (since } p \text{ splits in } k/\mathbb{Q}) \\ &\Leftrightarrow \left(\frac{A + B\sqrt{m}}{p}\right) = 1.\end{aligned}$$

This completes the proof of the theorem.

Letting $m = 2$ and replacing the quartic subfield of $\mathbb{Q}(\zeta_m)$ used above by the cyclic extension $\mathbb{Q}(\sqrt{2+\sqrt{2}}\,)$ contained in $\mathbb{Q}(\zeta_{16})$ yields the equivalence

$$\left(\frac{A + B\sqrt{2}}{p}\right) = 1 \ \Leftrightarrow\ p \text{ splits in } \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\,\big) \ \Leftrightarrow\ p \equiv \pm 1 \bmod 16, \tag{3}$$

stated in a slightly different way in [11].

Formula (1) differs from the one given in [11], which reads

$$\left(\frac{A + B\sqrt{m}}{p}\right) = (-1)^{(p-1)(m-1)/8}\left(\frac{2}{p}\right)\left(\frac{p}{m}\right)_4, \tag{4}$$

where $A, B, C > 0$, B is odd and C is even. Formula (2) shows that

$$\left(\frac{A + B\sqrt{m}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{A + C\sqrt{m}}{p}\right),$$

and so, for B even and C odd, (4) is equivalent to

$$\left(\frac{A + B\sqrt{m}}{p}\right) = (-1)^{(p-1)(m-1)/8}\left(\frac{p}{m}\right)_4. \tag{5}$$

Now $A \equiv 1 \bmod 4$ since $A^2 = m(B^2 + C^2)$ is the product of $m \equiv 1 \bmod 4$ and of a sum of two relatively prime squares, and we have $A + B \equiv 1 \bmod 4 \Leftrightarrow 4 \mid B \Leftrightarrow m \equiv 1 \bmod 8$. The sign of B is irrelevant, therefore

$$\left(\frac{-1}{p}\right)^{B/2} = (-1)^{(p-1)(m-1)/8}.$$

This finally shows that (1) is in fact equivalent to (4).

Another version of (1) which follows directly from (5) is

$$\left(\frac{A+B\sqrt{m}}{p}\right) = \left(\frac{p^*}{m}\right)_4, \tag{6}$$

where $A, B > 0$ and $p^* = (-1)^{(p-1)/2}p$.

Formula (1) can be extended to composite values of m (where the prime factors of m satisfy certain conditions given in [11]) in very much the same way as Jacobi extended the quadratic reciprocity law of Gauss; this extension, however, is not needed in deriving the known rational quartic reciprocity laws of K. Burde [1], E. Lehmer [6, 7] and A. Scholz [9]. These follow from (1) by assigning special values to A and B, in other words: they all stem from the observation that the quartic subfield K of $\mathbb{Q}(\zeta_m)$ can be generated by different square roots over $k = \mathbb{Q}(\sqrt{m})$.

The fact that (1) is valid for primes $p \mid ABC$ (which has not been proved in [11]) shows that we no longer have to exclude the primes $q \mid ab$ in Lehmer's criterion (as was necessary in [11]), and it allows us to derive Burde's reciprocity law in a more direct way: let p and q be primes $\equiv 1 \bmod 4$ such that $p = a^2 + b^2$, $q = c^2 + d^2$, $2 \mid b$, $2 \mid d$, $(p/q) = +1$, and define

$$A = pq, \quad B = b(c^2 - d^2) + 2acd, \quad C = a(c^2 - d^2) - 2bcd, \quad m = q.$$

Then $2 \mid B$, $B \equiv 2d(ac + bd) \bmod q$ (since $c^2 \equiv -d^2 \bmod q$), the sign of A does not matter (since $q \equiv 1 \bmod 4$), and so formula (1) yields

$$\left(\frac{q}{p}\right)_4 = \left(\frac{A+B\sqrt{p}}{q}\right) = \left(\frac{B}{q}\right)\left(\frac{p}{q}\right)_4,$$

and the well-known $\left(\frac{2d}{q}\right) = +1$ implies Burde's law

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{ac - bd}{q}\right). \tag{7}$$

A rational reciprocity law equivalent to Burde's has already been found by T. Gosset [5], who showed that, for primes p and q as above,

$$\left(\frac{q}{p}\right)_4 \equiv \left(\frac{a/b - c/d}{a/b + c/d}\right)^{(q-1)/4} \bmod q. \tag{8}$$

Multiplying the numerator and denominator of the term on the right side of (8) by $a/b + c/d$ and observing that $c^2/d^2 \equiv -1 \bmod q$ yields

$$\begin{aligned}\left(\frac{q}{p}\right)_4 &= \left(\frac{a^2/b^2 + 1}{q}\right)_4 \left(\frac{a/b + c/d}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{b}{q}\right)\left(\frac{a/b + c/d}{q}\right) \\ &= \left(\frac{p}{q}\right)_4 \left(\frac{a + bc/d}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{d}{q}\right)\left(\frac{ad + bc}{q}\right),\end{aligned}$$

which is Burde's reciprocity law since $\left(\frac{2d}{q}\right) = +1$.

A more explicit form of Burde's reciprocity law for composite values of p and q has been given by L. Rédei [8]; letting $n = pq = A^2 + B^2$ in [8, §5, (17), (19)], we find $A = ac - bd$, $B = ad + bc$, and his reciprocity formula [8, (23)] gives our formula (7).

Yet another version of Burde's law is due to A. Fröhlich [4]; he showed

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{a+bj}{q}\right) = \left(\frac{c+di}{p}\right), \tag{9}$$

where i and j denote rational numbers such that $i^2 \equiv -1 \bmod p$, $j^2 \equiv -1 \bmod q$. Letting $i = b/a$ and $j = d/c$ and observing that $\left(\frac{a}{p}\right) = \left(\frac{c}{q}\right) = +1$ we find that (9) is equivalent to (7).

The reciprocity law of Lehmer [6, 7] is even older; it can be found in Dirichlet's paper [2] as Théorème I and II; Dirichlet's ideas are reproduced in the charming book of Venkov [10] and may be used to give proofs for other rational reciprocity laws using nothing beyond quadratic reciprocity.

References

[1] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), 175–184.

[2] G. Lejeune Dirichlet, *Recherche sur les diviseurs premiers d'une classe de formules du quatrième degré*, ibid. 3 (1828), 35–69; *Werke I*, 63–98.

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

[4] A. Fröhlich, *The restricted biquadratic residue symbol*, Proc. London Math. Soc. (3) 9 (1959), 189–207.

[5] T. Gosset, *On the law of quartic reciprocity*, Mess. Math. (2) 41 (1911), 65–90.

[6] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), 20–29.

[7] —, *Rational reciprocity laws*, Amer. Math. Monthly 85 (1978), 467–472.

[8] L. Rédei, *Über die Grundeinheit und die durch* 8 *teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 131–148.

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

[10] B. A. Venkov, *Elementary Number Theory*, Moscow, 1937 (in Russian); English transl.: H. Alderson (ed.), Wolters-Noordhoff, Groningen, 1970.

[11] K. S. 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.

ERWIN-ROHDE-STR. 19
69120 HEIDELBERG
GERMANY

Received on 13.12.1993 (2541)