ON SCHOLZ'S RECIPROCITY LAW

KENNETH S. WILLIAMS

Abstract. An elementary proof is given of a reciprocity law proved by Scholz using class-field theory.

In this note we shall be concerned with distinct primes $p \equiv 1 \pmod{4}$ and $q \equiv 1 \pmod{4}$, which are quadratic residues of one another, so that we can regard $\sqrt{q}$ as an integer modulo $p$. We let $\varepsilon_q$ denote the fundamental unit of the real quadratic field $Q(\sqrt{q})$. Although $\sqrt{q}$ is only defined modulo $p$ up to sign, nevertheless, the Legendre symbol $(\frac{q}{p})$ is uniquely defined, as $\varepsilon_q$ has norm $-1$ and $(\frac{-1}{p}) = 1$. Moreover, since $(\frac{q}{p}) = 1$, we can define $(\frac{q}{p})_4$ to be $+1$ or $-1$, according as $q$ is or is not a fourth power (mod $p$). In 1934, Scholz [4] proved the following reciprocity law using class-field theory, namely,

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

In 1971, Lehmer [3] gave a proof of (1), using Dirichlet's formula for the class number of the real quadratic field $Q(\sqrt{q})$ and some facts from cyclotomy. Another proof, using spinor genera, has been given by Estes and Pall [2]. It is the purpose of this note to give an elementary proof, which depends essentially only on manipulation of Jacobi symbols and Jacobi's law of quadratic reciprocity.

We set

$$
\lambda = \begin{cases} 
1, & \text{if } q \equiv 1 \pmod{8}, \\
3, & \text{if } q \equiv 5 \pmod{8}.
\end{cases}
$$

It is well known that there are positive integers $T$ and $U$ such that

$$
\varepsilon_q^\lambda = T + U\sqrt{q}, \quad T \equiv 0 \pmod{2}, \quad U \equiv 1 \pmod{4}.
$$

Moreover, as $(\frac{q}{p}) = 1$, there are positive coprime integers $u$ and $v$, with $u$ odd, such that $p^{\lambda h} = u^2 - 4qv^2$, where $h \equiv 1 \pmod{2}$ is the class number of $Q(\sqrt{q})$ (see for example [1, Theorem 1, p. 184 and Theorem 6, p. 187]). Then, as $u/2v \equiv \sqrt{q} \pmod{p}$, we have

Received by the editors September 30, 1976.

\[
\left( \frac{e_q}{p} \right) = \left( \frac{e_q}{p} \right) = \left( \frac{T + U\sqrt{q}}{p} \right) = \left( \frac{T + U(u/2v)}{p} \right)
\]

\[
= \left( \frac{2}{p} \right) (v) \left( \frac{Uu + 2Tv}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{p}{Uu + 2Tv} \right)
\]

\[
= \left( \frac{2}{p} \right) (v) \left( \frac{p^{\lambda_h}}{Uu + 2Tv} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{u^2 - 4qv^2}{Uu + 2Tv} \right)
\]

\[
= \left( \frac{2}{p} \right) (v) \left( \frac{U^2u^2 - 4qU^2v^2}{Uu + 2Tv} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{4T^2v^2 - 4qU^2v^2}{Uu + 2Tv} \right)
\]

\[
= \left( \frac{2}{p} \right) (v) \left( \frac{T^2 - qU^2}{Uu + 2Tv} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{-1}{Uu + 2Tv} \right)
\]

\[
= \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{-1}{u} \right)
\]

\[
= \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{p^{\lambda_h}q}{u} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{q}{u} \right) = \left( \frac{2}{p} \right) \left( \frac{v}{p} \right) \left( \frac{u}{q} \right)
\]

\[
= \left( \frac{2}{p} \right) \left( \frac{(uv)^2}{p} \right) \left( \frac{u^2}{q} \right) = \left( \frac{2}{p} \right) \left( \frac{4q}{p} \right) \left( \frac{p^{\lambda_h}}{q} \right)
\]

\[
= \left( \frac{2}{p} \right) \left( \frac{2}{p} \right) \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) = \left( \frac{p}{q} \right) \left( \frac{q}{p} \right)
\]

as required.

The author acknowledges some suggestions of the referee which enabled him to shorten his original proof.

REFERENCES


DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use