Indian J. pure appl. Math., 17 (2) : 169-174 February 1986

A SIMPLE PROOF OF EISENSTEIN'S RECIPROCITY LAW FROM STICKELBERGER'S THEOREM

BLAIR K. SPEARMAN

Department of Mathematics, College of New Caledonia
Prince George, British Columbia, Canada V2N 1P8

AND

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics, Carleton University
Ottawa, Ontario, Canada K1S 5B6

(*Received* 21 *June* 1985)

A simple proof of Eisenstein's law of reciprocity is given.

1. INTRODUCTION

Let l be an odd prime and set $\zeta_l = \exp(2\pi i/l)$. The ring of integers of the cyclotomic field $Q(\zeta_l)$ is denoted by $Z[\zeta_l]$. An element α of $Z[\zeta_l]$ is called primary if it is prime to l and congruent to a rational integer modulo $(1-\zeta_l)^2$. For any $\delta \in Z[\zeta_l]$ prime to l there is a unique integer d modulo l such that $\zeta_l^d\ \delta$ is primary.

Let P be a prime ideal of $Z[\zeta_l]$ not dividing l. The norm of P, written $N(P)$, is of the form $p^f \equiv 1 \pmod{l}$, where p is a rational prime. The lth power residue symbol χ_p is defined for $\beta \in GF(p^f)^* = GF(p^f) - \{0\}$ by

$$\chi_p(\beta) = \zeta_l^k, \text{ where } \beta^{(p^f-1)/l} \equiv \zeta_l^k \pmod{P}.$$

For any proper ideal A of $Z[\zeta_l]$ prime to l, the symbol χ_A is defined in terms of the symbols χ_{P_i} $(1 \leqq i \leqq s)$, where $A = P_1 P_2 \dots P_s$ (with $N(P_j) = p_j^{f_j}$, $1 \leqq j \leqq s$) is the prime ideal decomposition of A in $Z[\zeta_l]$, as follows : for $\gamma \in \Gamma = GF\left(p_1^{f_1}\right)^* \oplus \dots \oplus GF\left(p_s^{f_s}\right)^*$, say $\gamma = \gamma_1 + \dots + \gamma_s$ with $\gamma_j \in GF\left(p_j^{f_j}\right)^*$ $(1 \leqq j \leqq s)$, we set

$$\chi_A(\gamma) = \prod_{j=1}^{s} \chi_{P_j}(\gamma_j).$$

---

* Research supported by Natural Sciences and Engineering Research Council Canada, Grant No. A-7233.

Finally if A is a principal ideal, say $A = (\kappa)$, we set $\chi_\kappa = \chi_{(\kappa)}$.

Eisenstein's reciprocity law asserts that if l is an odd prime, a is a rational integer ($\neq \pm 1$) coprime with l, and α is a primary non-unit element of $Z[\zeta_l]$ prime to a, then

$$\chi_a(\alpha) = \chi_\alpha(a). \qquad \ldots(1.1)$$

This law was first proved by Eisenstein[2]. A number of proofs of it have been given, see for example [ref. (1) pp. 70-95], [ref. (3) p. 77], [ref. (4) Satz 140], [ref. (5) Chap. 14] and refs. (7, 9). The purpose of this short note is to give a simple proof which deduces the law from a well-known identity involving Gauss and Jacobi sums by means of Stickelberger's theorem.

2. Proof of Eisenstein's Reciprocity Law

It suffices to prove (1.1) with a prime, say $a = q$ (prime) $\neq l$, and we define m to be the least positive integer such that $q^m \equiv 1 \pmod{l}$.

For any proper ideal A of $Z[\zeta_l]$ prime to l, the Gauss sum $G\left(\chi_A^r\right)$ $(r \in Z)$ is defined by

$$G\left(\chi_A^r\right) = \sum_{\gamma = \sum_{j=1}^{s} \gamma_j \in \Gamma} \chi_A^r(\gamma) \exp\left(2\pi i \sum_{j=1}^{s} (tr_j\, \gamma_j)/p_j\right) \qquad \ldots(2.1)$$

where $tr_j\, \gamma_j$ denotes the trace of γ_j from $GF\left(p_j^{f_j}\right)$ to $GF(p_j)$. The Jacobi sum $J\left(\chi_A^r, \chi_A^s\right)$ $(r, s \in Z)$ is defined by

$$J\left(\chi_A^r, \chi_A^s\right) = \sum_{1 \neq \gamma \in \Gamma} \chi_A^r(\gamma)\, \chi_A^s(1-\gamma). \qquad \ldots(2.2)$$

These sums are related by the identity

$$G\left(\chi_A^l\right) = N(A) \prod_{k=1}^{l-2} J\left(\chi_A, \chi_A^k\right). \qquad \ldots(2.3)$$

Taking $r = 1$ and $A = (\alpha)$, where α is a primary non-unit element of $Z[\zeta_l]$ prime to q, in (2.1) and raising both sides to the q^mth power, we obtain working modulo q and using $q^m \equiv 1 \pmod{l}$,

$$G(\chi_\alpha)^{q^m} \equiv \sum_{\gamma \in \Gamma} \chi_\alpha(\gamma) \exp\left(2\pi i \sum_{j=1}^{s} \left(tr_j(q^m \gamma_j)\right)/p_j\right) \pmod{q}$$

$$\equiv \sum_{\gamma \in \Gamma} \chi_\alpha(q^{-m}\gamma) \exp\left(2\pi i \sum_{j=1}^{s} \left(tr_j \gamma_j)/p_j\right) \pmod{q}$$

$$\equiv \chi_\alpha^{-m}(q)\, G(\chi_\alpha) \bmod q)$$

so that, as $| G(\chi_\alpha) |^2 = N(\alpha)$ is prime to q

$$G(\chi_\alpha)^{q^m - 1} \equiv \chi_\alpha^{-m}(q) \pmod{q}. \qquad \text{.. (2.4)}$$

Next, by Stickelberger's theorem[8], we have for $j = 1, .., s$ and $k, = 1, ., l-2$

$$\left(J\left(\chi_{P_j}, \chi_{P_j}^k\right)\right) = \prod_{i=1}^{l-1} \sigma_{i^{-1}}(P_j), \qquad \text{...(2.5)}$$

$$\left\{\frac{i}{l}\right\} + \left\{\frac{ki}{l}\right\} < 1$$

where σ_i $(1 \leqq i \leqq l-1)$ is the automorphism of $Q(\zeta_l)$ which maps ζ_l to ζ_l^i, for $1 \leqq i \leqq l-1$ the integer i^{-1} denotes the unique integer satisfying $i \,.\, i^{-1} \equiv 1 \pmod{l}$ and $1 \leqq i^{-1} \leqq l-1$, and $\{x\}$ denotes the fractional part of the real number x. From (2.5) we obtain

$$\left(\prod_{k=1}^{l-2} J\left(\chi_{P_j}, \chi_{P_j}^k\right)\right) = \prod_{i=1}^{l-1} \sigma_{i^{-1}}^{l-i-1}(P_j)$$

and so

$$\left(\prod_{k=1}^{l-2} J\left(\chi_\alpha, \chi_\alpha^k\right)\right) = \left(\prod_{k=1}^{l-2} \prod_{j=1}^{s} J\left(\chi_{P_j}, \chi_{P_j}^k\right)\right)$$

(*equation continued on p.* 172)

$$= \left(\prod_{j=1}^{s} \prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-i-1} (P_j) \right)$$

$$= \left(\prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-1} \left((\alpha) \right) \right)$$

giving

$$\left(N\left((\alpha) \right) \prod_{k=1}^{l-2} J\left(\chi_\alpha, \chi_\alpha^k \right) \right) = \left(\prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-i} \left((\alpha) \right) \right)$$

$$= \left(\prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-i} (\alpha) \right)$$

and thus

$$N(\alpha) \prod_{k=1}^{l-2} J\left(\chi_\alpha, \chi_\alpha^k \right) = \epsilon \prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-i} (\alpha) \qquad \ldots(2.6)$$

where ϵ is a unit of $Z[\zeta_l]$. Since α is primary so are all its conjugates. In addition $J\left(\chi_\alpha, \chi_\alpha^k \right) \equiv (-1)^s \pmod{(1-\zeta_l)^2}$ so $J\left(\chi_\alpha, \chi_\alpha^k \right)$ is primary. Hence from (2.6) we see that ϵ is a primary unit. Further taking the square of the modulus of (2.6), we obtain

$$N(\alpha)^2 \, . \, N(\alpha)^{l-2} = |\epsilon|^2 N(\alpha)^l$$

so that $|\epsilon| = 1$. Hence as ϵ is of the form $\zeta_l^m r$, where r is a real number and $0 \leqq m \leqq l-1$, (see for example, Pollard[6], Lemma 10.11), we must have $\epsilon = \pm \zeta_l^m$, $0 \leqq m \leqq l-1$. Since ϵ is primary we deduce that $m = 0$, that is, $\epsilon = \pm 1$, and (2.6) becomes

$$N(\alpha) \prod_{k=1}^{l-2} J\left(\chi_\alpha, \chi_\alpha^k \right) = \pm \prod_{i=1}^{l-1} \sigma_{l^{-1}}^{l-i} (\alpha). \qquad \ldots(2.7)$$

Appealing to (2.3) with $A = (\alpha)$ we have

$$G(\chi_\alpha)^l = \pm \prod_{i=1}^{l-1} \sigma_{i^{-1}}^{l-i}(\alpha)$$

and so

$$G(\chi_\alpha)^{q^m-1} = \left[\prod_{i=1}^{l-1} \sigma_{i^{-1}}^{l-i}(\alpha)\right]^{(q^m-1)/l}. \qquad \ldots(2.8)$$

Let Q denote one of the prime ideal factors of q in $Z[\zeta_l]$. Then, from (2.4) and (2.8) we obtain

$$\chi_\alpha^{-m}(q) \equiv \chi_Q\left(\prod_{i=1}^{l-1} \sigma_{i^{-1}}^{l-i}(\alpha)\right) \pmod{Q}$$

$$\equiv \prod_{i=1}^{l-1} \chi_Q^{l-i}(\sigma_{i^{-1}}(\alpha)) \pmod{Q}$$

$$\equiv \prod_{i=1}^{l-1} \sigma_{l-i}\left(\chi_Q(\sigma_{i^{-1}}(\sigma))\right) \pmod{(Q)}$$

$$\equiv \prod_{i=1}^{l-1} \chi_{\sigma_{l-i}(Q)}\left(\sigma_{l-i}(\sigma_{i^{-1}}(\alpha))\right) \pmod{Q}$$

$$\equiv \prod_{i=1}^{l-l} \chi_{\sigma_{l-i}(Q)}(\sigma_{l-1}(\alpha)) \pmod{Q}$$

$$\equiv \chi_{\prod_{i=1}^{l-i} \sigma_i(Q)}(\sigma_{l-1}(\alpha)) \pmod{Q}$$

$$\equiv \chi_{(q)^m}(\sigma_{l-1}(\alpha)) \pmod{Q}$$

$$\equiv \chi_{(q)^m}(\sigma_{l-1}(\alpha)) \pmod{Q}$$

$$\equiv \chi_q^m (\sigma_{l-1}(\alpha)) \pmod{Q}$$

that is

$$\chi_\alpha^{-m}(q) \equiv \chi_q^{-m}(\alpha) \pmod{Q}. \quad ..(2.9)$$

As both sides of (2.9) are powers of ζ_l we must have

$$\chi_\alpha^{-m}(q) = \chi_q^{-m}(\alpha).$$

Finally, as $(m, l) = 1$, we obtain

$$\chi_\alpha(q) = \chi_q(\alpha)$$

as required.

References

1. G. Cooke, *Notes, Lectures on the Power Reciprocity Laws of Algebraic Number Theory*, Cornell University, 1974, pp. 97.
2. G. Eisenstein, Beweis des allgemeinsten Reciprocitätsgesetze zwischen reelen und complexen Zahlen, in : *Mathematische Werke, Band II*, pp. 189–198. Chelsea, New York, 1975.
3. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper Teil II : Reziprozitätsgesetz, Physica-Verlag, Würzburg-Wien 1970.
4. D. Hilbert, *Jahr. Deutschen Math.-Ver.* **4** (1897), 175–546.
5. K. Ireland, and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics No. 84, Springer Verlag, New York, 1982.
6. H. Pollard, *The Theory of Algebraic Numbers*, Carus Math. Monograph No. 9, Math. Assoc. Amer. (1950).
7. Th. Skolen, *Math. Scand.* **9** (1961), 229–42.
8. L. Stickelberger, *Math. Ann.* **37** (1890), 321–67.
9. A. Weil, *Enseign. Math.* **20** (1974), 247–63.