Bull. Cal. Math. Soc., **69**, 311–314 (1977)

ON EISENSTEIN'S SUPPLEMENT TO THE LAW OF CUBIC RECIPROCITY

KENNETH S. WILLIAMS

(*Received 18 July 1975*)

We denote the domain of rational integers by Z and let $Z[w]$ denote the integral domain $\{x+yw;\ x, y \in Z\}$, where w is the complex cube root of unity $(-1+\sqrt{-3})/2$. The elements of $Z[w]$ were used by Eisenstein (1844, 1845), in his work on cubic reciprocity and for this reason are sometimes called Eisenstein integers (for details of the arithmetic of Eisenstein integers see, for example, the delightful book by Ireland and Rosen (1972), whose notation we follow). If $\alpha \in Z[w]$ we write $N(\alpha) = \alpha\bar{\alpha}(\in Z)$ for its norm, where $\bar{\alpha}$ is the complex conjugate of α. There are exactly six units (elements of norm 1) in $Z[w]$, namely ± 1, $\pm w$, $\pm w^2$. Two non-zero Eisenstein integers α, β are said to be associates, written $\alpha \sim \beta$, if their quotient α/β is a unit. $Z[w]$ is a Euclidean domain so each non-zero, non-unit element is expressible in essentially a unique manner as a product of primes. The primes of $Z[w]$ consist of positive rational primes $q \equiv 2 \pmod 3$ and their associates, complex primes of the form $a+bw$ having norm a rational prime $\equiv 1 \pmod 3$, and $1-w$ and its associates. We remark that the norm of $1-w$ is 3, indeed $3 \sim (1-w)^2$.

If π is a prime in $Z[w]$, not an associate of the prime $1-w$ (written $\pi \chi/1-w$) then $N(\pi) \equiv 1 \pmod 3$ and the cubic residue character of $\alpha (\in Z[w])$ modulo π is defined by

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{if } \alpha \equiv 0 \pmod{\pi}, \\ w^r & \text{if } \alpha \not\equiv 0 \pmod{\pi} \text{ and } \alpha^{(N(\pi)-1)/3} \equiv w^r \pmod{\pi},\ r = 0, 1, 2. \end{cases} \tag{1}$$

This character enjoys the following properties : if $\alpha, \beta \in Z[w]$ then

$$\left(\frac{\bar{\alpha}}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3, \left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3, \tag{2}$$

and

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 \text{ if } \alpha \equiv \beta \pmod{\pi}. \tag{3}$$

Also we have

$$\left(\frac{-1}{\pi}\right)_3 = 1, \left(\frac{w}{\pi}\right)_3 = w^{(N(\pi)-1)/3}. \tag{4}$$

A prime π of $Z[w]$ will be called primary if it satisfies $\pi \equiv 2 \pmod 3$. If π is a prime $\chi/1-w$ then among its six associates exactly one is primary. Clearly $1-w$ and its associates are not primary. Eisenstein (1844) proved

The Law of Cubic Reciprocity: If π and λ are primary primes of $Z[w]$ then

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

Two proofs of this are given by Ireland and Rosen (1972) (see also Cooke, 1974). In the same year Eisenstein also proved

Supplement to the Law of Cubic of Reciprocity: Let π be a primary prime of $Z[w]$. If $\pi = q$ is rational, let $q = 3m-1$. If $\pi = a+bw$ is a primary complex prime, let $a = 3m-1$, $b = 3n$. Then

$$\left(\frac{1-w}{\pi}\right)_3 = w^{2m}.$$

Only the case π rational of the supplement to the law of cubic reciprocity is proved by Ireland and Rosen (1972), (see comment (c), p. 115). In this article we prove the supplement in a very simple manner by deducing it from the law of cubic reciprocity. Other proofs have been given by Cooke (1974) and the author (Williams, 1975); it is also a special case of Artin's power reciprocity law (Artin and Tate, 1967).

We begin by extending the definition of the cubic residue character to allow us to work with non-prime integers of $Z[w]$ in the denominator of the symbol, yet still retain properties analogous to (2), (3) and (4).

Let $\alpha \epsilon Z[w]$ and let $\tau \epsilon Z[w]$ be such that $\tau \not\equiv 0 \pmod{1-w}$. We set

$$\left(\frac{\alpha}{\tau}\right)_3 = \begin{cases} 1, & \text{if } \tau \text{ is a unit of } Z[w], \\ \left(\frac{\alpha}{\pi_1}\right) \cdots \left(\frac{\alpha}{\pi_r}\right), & \text{if } \tau \text{ is not a unit and } \tau = \pi_1 \ldots \pi_r \text{ where the } \pi_i \text{ are primes.} \end{cases} \tag{5}$$

As $Z[w]$ is a unique factorization domain the definition is a valid one. If $\alpha, \beta \epsilon Z[w]$, τ, $\rho \epsilon Z[w]$ with $\tau, \rho \not\equiv 0 \pmod{1-w}$ then it is easily verified using (2), (3), (4) and (5) that

$$\left(\frac{\bar{\alpha}}{\tau}\right)_3 = \left(\frac{\alpha}{\tau}\right)_3^2 = \left(\frac{\alpha}{\bar{\tau}}\right)_3, \left(\frac{\alpha\beta}{\tau}\right)_3 = \left(\frac{\alpha}{\tau}\right)_3 \left(\frac{\beta}{\tau}\right)_3, \left(\frac{\alpha}{\tau\rho}\right) = \left(\frac{\alpha}{\tau}\right)\left(\frac{\alpha}{\rho}\right)_3, \tag{6}$$

and

$$\left(\frac{\alpha}{\tau}\right)_3 = \left(\frac{\beta}{\tau}\right)_3 \text{ if } \alpha \equiv \beta \pmod{\tau}. \tag{7}$$

Also we have.

$$\left(\frac{-1}{\tau}\right)_{-3} = 1, \left(\frac{w}{\tau}\right)_3 = w^{(N(\tau)-1)/3}. \tag{8}$$

The last assertion involves checking that if π_1 and π_2 are primes of $Z[w]$ with $\pi_1 \not\chi 1-w$, $\pi_2 \not\chi 1-w$ then

$$\frac{N(\pi_1)-1}{3}+\frac{N(\pi_2)-1}{3}\equiv\frac{N(\pi_1\pi_2)-1}{3}\pmod 3.$$

We also note from (6) that if k is a rational integer $\not\equiv 0 \pmod 3$ and m is a rational integer such that $(k, m) = 1$ then

$$\left(\frac{m}{k}\right)_3^2=\left(\frac{\bar{m}}{\bar{k}}\right)_3=\left(\frac{m}{k}\right)_3,$$

so

$$\left(\frac{m}{k}\right)_3=1, \quad \text{as } (k,m)=1. \tag{9}$$

Further we note that if $\alpha, \beta \in Z[w]$ are such that $\alpha \equiv \beta \equiv 2 \pmod 3$, then a simple application of (6) and the law of cubic reciprocity gives

$$\left(\frac{\alpha}{\beta}\right)_3=\left(\frac{\beta}{\alpha}\right)_3. \tag{10}$$

Finally if k is a rational integer $\equiv 2 \pmod 3$, say $k = 3m-1$, then

$$\left(\frac{1-w}{k}\right)_3=\left(\frac{(1-w)^4}{k}\right)_3=\left(\frac{(1-w)^2}{k}\right)_3^2=\left(\frac{-3w}{k}\right)_3^2=\left(\frac{-3}{k}\right)_3^2\left(\frac{w}{k}\right)_3^2$$

$$=\left(\frac{w}{k}\right)_3^2 \text{(by (9))} = w^{2(N(k)-1)/3}=w^{2(k^2-1)/3}=w^{6m^2-4m},$$

showing that

$$\left(\frac{1-w}{k}\right)_3=w^{2m}. \tag{11}$$

Proof of Supplement to Law of Cubic Reciprocity. The case π rational is just the special case $k = q$ of (11). If π is not rational, $\pi = a+bw$ where $a = 3m-1$, $b = 3n$; then

$$\left(\frac{1-w}{\pi}\right)_3=\left(\frac{b}{a}\right)_3\left(\frac{1-w}{\pi}\right)_3 \qquad \text{(by (9))}$$

$$=\left(\frac{w}{a}\right)_3^2\left(\frac{bw}{a}\right)_3\left(\frac{1-w}{\pi}\right)_3 \qquad \text{(by (6))}$$

$$= w^{\frac{2(a^2-1)}{3}} \left(\frac{\pi}{a}\right)_3 \left(\frac{1-w}{\pi}\right)_3 \qquad \text{(by (7), (8))}$$

$$= w^{6m^2-4m} \left(\frac{a}{\pi}\right)_3 \left(\frac{1-w}{\pi}\right)_3 \qquad \text{(by (10))}$$

$$= w^{2m} \left(\frac{a-aw}{\pi}\right)_3 \qquad \text{(by (6))}$$

$$= w^{2m} \left(\frac{-(a+b)w}{\pi}\right)_3 \qquad \text{(by (3))}$$

$$= w^{2m} \left(\frac{w}{\pi}\right)_3 \left(\frac{a+b}{\pi}\right)_3 \qquad \text{(by (2), (4))}$$

$$= w^{2m+(p-1)/3} \left(\frac{\pi}{a+b}\right)_3 \qquad \text{(by (4), (10))}$$

$$= w^n \left(\frac{b(1-w)}{a+b}\right)_3 \qquad \text{(by (7))}$$

$$= w^n \left(\frac{b}{a+b}\right)_3 \left(\frac{1-w}{a+b}\right)_3 \qquad \text{(by (6))}$$

$$= w^{n+2(m+n)} \qquad \text{(by (9), (11))}$$

$$= w^{2m}.$$

References

Artin, E. and Tate, J. (1967): Class field theory, W. A. Benjamin, Inc. New York, 168.

Cooke, George, (1974) Notes "Lectures on the power reciprocity laws of algebraic number theory" Cornell University, 44.

Eisenstein, G. (1844): Beweis der Reciprocitätzsatz fur die cubische Reste, *Jour. für Reine und Angew, Math.*, **27**, 289.

Eisenstein, G. (1845): Nachtrag zum cubischen Reciprocitätssatze...., *Jour. für Reine and Angew, Math.*, **28**, 28.

Ireland, K. and Rosen, M. I. (1972): Elements of number theory, Bogden and Quigley.

Williams, K. S. (1975): Note on the supplement to the law of cubic reciprocity, *Proc. Amer. Math. Soc.*, **47**, 333.

CARLETON UNIVRRSITY
OTTAWA, ONTARIO, CANADA.