The Eisenstein reciprocity law and l^nth power residue

Mari Kouchiwa

(Received March 28, 2016)

Abstract: Taking an odd prime number l and a natural number n, we study a reciprocity law for the l^nth power residue symbol along the same lines as in a proof given in Ireland and Rosen [1] to the Eisenstein reciprocity law.

1 Definitions and preliminaries

For any natural number m, let $\zeta_m = e^{2\pi i/m}$. We denote by $\mathbb{Q}$ the field of rational numbers and by $\mathbb{Z}$ the ring of rational integers. It follows that $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_m)$ of mth roots of unity. We fix m in the rest of this paper.

Definition 1. *For each $\alpha \in \mathbb{Z}[\zeta_m]$ and each prime ideal P of $\mathbb{Z}[\zeta_m]$ not containing m, define $\left(\frac{\alpha}{P}\right)_m$ as follows. If $\alpha \in P$, let*

$$\left(\frac{\alpha}{P}\right)_m = 0.$$

If $\alpha \notin P$, let $\left(\frac{\alpha}{P}\right)_m$ denote the unique mth root of unity such that

$$\left(\frac{\alpha}{P}\right)_m \equiv \alpha^{(N(P)-1)/m} \pmod{P},$$

where $N(P)$ stands for the absolute norm of P, i.e., $N(P) = |\mathbb{Z}[\zeta_m]/P|$. We call $\left(\frac{\alpha}{P}\right)_m$ the mth power residue symbol.

As is well known, the above definition gives the following result for any $\alpha_1 \in \mathbb{Z}[\zeta_m]$, any $\alpha_2 \in \mathbb{Z}[\zeta_m]$ and any prime ideal P of $\mathbb{Z}[\zeta_m]$ not containing m (cf. [1, Proposition 14.2.2 and its Corollary]).

Proposition 1. — (i) *If $\alpha_1 \equiv \alpha_2 \pmod{P}$, then $\left(\frac{\alpha_1}{P}\right)_m = \left(\frac{\alpha_2}{P}\right)_m$.*

(ii) $\left(\frac{\alpha_1\alpha_2}{P}\right)_m = \left(\frac{\alpha_1}{P}\right)_m \left(\frac{\alpha_2}{P}\right)_m$.

(iii) $\left(\frac{\alpha_1}{P}\right)_m = 1$ *if and only if $x^m \equiv \alpha_1 \pmod{P}$ for some $x \in \mathbb{Z}[\zeta_m] \setminus P$.*

(iv) $\left(\frac{\zeta_m}{P}\right)_m = \zeta_m^{(N(P)-1)/m}$.

Definition 2. *For each $\theta \in \mathbb{Z}[\zeta_m]$, we put $(\theta) = \theta\mathbb{Z}[\zeta_m]$. Suppose that A is an ideal of $\mathbb{Z}[\zeta_m]$ relatively prime to (m). Let $A = P_1P_2\cdots P_s$ be the prime decomposition of A in $\mathbb{Z}[\zeta_m]$. For each $\alpha \in \mathbb{Z}[\zeta_m]$, define*

$$\left(\frac{\alpha}{A}\right)_m = \left(\frac{\alpha}{P_1}\right)_m \left(\frac{\alpha}{P_2}\right)_m \cdots \left(\frac{\alpha}{P_s}\right)_m,$$

and for each $\beta \in \mathbb{Z}[\zeta_m]$ *relatively prime to* m*, define*

$$\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m.$$

The following result of Gauss for $m = 2$ is famous as main part of law of quadratic reciprocity: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)_2.$$

Whereas Gauss discovered a similar result for $m = 4$, Eisenstein proved it completely. For the case in which m is an odd prime, a result on the mth power residue symbol still analogous to law of quadratic reciprocity was first proved by Eisenstein and is called the Eisenstein reciprocity law (cf. [1, Chapters 9 and 14]).

From now on, we treat the case $m = l^n$, where l is an odd prime and n is a natural number.

Definition 3. *A nonzero element* α *of* $\mathbb{Z}[\zeta_{l^n}]$ *is called primary if it is not a unit but it is relatively prime to* l *and congruent to a rational integer modulo* $(1 - \zeta_{l^n})^2$*.*

Proposition 2. *For any* $\alpha \in \mathbb{Z}[\zeta_{l^n}]$ *prime to* l*, there exists* $c \in \mathbb{Z}$*, uniquely determined modulo* l*, such that* $\zeta_{l^n}^c \alpha$ *is primary.*

Proof. Let $\lambda = 1 - \zeta_{l^n}$. Since the prime ideal (λ) of $\mathbb{Z}[\zeta_{l^n}]$ has degree 1, there is a rational integer a such that $\alpha \equiv a \pmod{(\lambda)}$. We then have $(\alpha - a)/\lambda \in \mathbb{Z}[\zeta_{l^n}]$, so there is a rational integer b such that $(\alpha - a)/\lambda \equiv b \pmod{(\lambda)}$. Consequently, $\alpha \equiv a + b\lambda \pmod{(\lambda)^2}$. Since α is relatively prime to l, the rational integer a is also relatively prime to l. Choose a rational integer c to satisfy $ac \equiv b \pmod{l}$. Since $\zeta_{l^n} = 1 - \lambda$, we have $\zeta_{l^n}^c \equiv 1 - c\lambda \pmod{(\lambda)^2}$. It follows that

$$\zeta_{l^n}^c \alpha \equiv a + (b - ac)\lambda \pmod{(\lambda)^2}.$$

Therefore, $\zeta_{l^n}^c \alpha \equiv a \pmod{(\lambda)^2}$ and so $\zeta_{l^n}^c \alpha$ is primary.

Next assume that $\zeta_{l^n}^{c'} \alpha \equiv a' \pmod{(\lambda)^2}$ with rational integers c' and a'. Then

$$(\zeta_{l^n}^{c'-c} - 1)\zeta_{l^n}^c \alpha = (\zeta_{l^n}^{c'} - \zeta_{l^n}^c)\alpha \equiv a' - a \pmod{(\lambda)^2}.$$

This implies $a' - a \equiv 0 \pmod{(\lambda)}$, i.e., $a' - a \equiv 0 \pmod{l}$. As $l \equiv 0 \pmod{(\lambda)^2}$, it follows that $(\zeta_{l^n}^{c'-c} - 1)\zeta_{l^n}^c \alpha \equiv 0 \pmod{(\lambda)^2}$. Hence $c' \equiv c \pmod{l}$. □

If $\alpha \in \mathbb{Z}[\zeta_{l^n}]$ is given and $\zeta_{l^n}^c \alpha$ is primary with $c \in \mathbb{Z}$, then by Proposition 1, any nonzero prime ideal P of $\mathbb{Z}[\zeta_{l^n}]$ fulfilles

$$\left(\frac{\alpha}{P}\right)_{l^n} = \left(\frac{\zeta_{l^n}^{-c}}{P}\right)_{l^n}\left(\frac{\zeta_{l^n}^c \alpha}{P}\right)_{l^n} = \zeta_{l^n}^{-c(N(P)-1)/l^n}\left(\frac{\zeta_{l^n}^c \alpha}{P}\right)_{l^n}.$$

In such a sense, for the study of the l^nth power residue symbol, it suffices to consider only primary elements of $\mathbb{Z}[\zeta_{l^n}]$.

Now, let P be a nonzero prime ideal of $\mathbb{Z}[\zeta_{l^n}]$. Note that the multiplicative group of the field $\mathbb{Z}[\zeta_{l^n}]/P$ is $(\mathbb{Z}[\zeta_{l^n}]/P) \setminus \{P\}$:

$$(\mathbb{Z}[\zeta_{l^n}]/P)^\times = (\mathbb{Z}[\zeta_{l^n}]/P) \setminus \{P\}.$$

By Proposition 1, we can define a multiplicative character χ_P of $\mathbb{Z}[\zeta_{l^n}]/P$ by

$$\chi_P(P) = 0 \qquad \text{and} \qquad \chi_P(u) = \left(\frac{\alpha}{P}\right)_{l^n}^{-1} \qquad \text{for } u \in (\mathbb{Z}[\zeta_{l^n}]/P)^\times,\ \alpha \in u.$$

Let p be the prime number in P. Then $\mathbb{Z}[\zeta_{l^n}]/P$ becomes canonically a finite extension over the prime field $\mathbb{Z}/p\mathbb{Z}$. Further ζ_p^w is also defined canonically for each $w \in \mathbb{Z}/p\mathbb{Z}$. Thus we can define an additive character ψ_P of (the additive group of) $\mathbb{Z}[\zeta_{l^n}]/P$ by

$$\psi_P(u) = \zeta_p^{tr(u)} \qquad \text{for } u \in \mathbb{Z}[\zeta_{l^n}]/P,$$

where tr denotes the trace map from $\mathbb{Z}[\zeta_{l^n}]/P$ to $\mathbb{Z}/p\mathbb{Z}$. Naturally $\psi_P(P) = \zeta_p^{tr(P)} = 1$.

Definition 4. *With P as above, set*

$$g(P) = \sum_{u \in \mathbb{Z}[\zeta_{l^n}]/P} \chi_P(u)\psi_P(u).$$

For this Gauss sum, we difine

$$\Phi(P) = g(P)^{l^n}.$$

Obviously it follows that $g(P)$ belongs to $\mathbb{Q}(\zeta_{l^n}, \zeta_p)$, but $\Phi(P)$ is known to belong to $\mathbb{Z}[\zeta_{l^n}]$ (cf. [1, Proposition 14.3.1]).

Definition 5. *Let A be an ideal of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to (l), α an element of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to l. Let $A = P_1P_2\cdots P_s$ be the prime decomposition of A in $\mathbb{Z}[\zeta_{l^n}]$. We then define*

$$\Phi(A) = \Phi(P_1)\Phi(P_2)\cdots\Phi(P_s), \quad \Phi(\alpha) = \Phi((\alpha)).$$

Proposition 3. *Let A be an ideal of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to (l). Then $\Phi(A) \equiv \pm 1 \pmod{l}$*

Proof. Let P be a prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to l. By Definition 5, it is enough to show that $\Phi(P) \equiv -1 \pmod{l}$. We obtain from Definition 4

$$\Phi(P) = g(P)^{l^n} \equiv \sum_{u \in \mathbb{Z}[\zeta_{l^n}]/P} \chi_P(u)^{l^n}\psi_P(u)^{l^n} \pmod{l},$$

so that, by Definition 1,

$$\Phi(P) \equiv \sum_{u \in (\mathbb{Z}[\zeta_{l^n}]/P)^\times} \psi_P(u)^{l^n} \pmod{l}.$$

Since ψ_P is an additive character of $\mathbb{Z}[\zeta_{l^n}]/P$, the right hand side above is

$$\sum_{u \in (\mathbb{Z}[\zeta_{l^n}]/P)^\times} \psi_P(l^n u) = \sum_{u \in (\mathbb{Z}[\zeta_{l^n}]/P)^\times} \psi_P(u) = -\psi_P(P) = -1.$$

□

2 Main results

Let G denote the Galois group of $\mathbb{Q}(\zeta_{l^n})$ over $\mathbb{Q}$: $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{l^n})/\mathbb{Q})$. Writing $\alpha^\sigma = \sigma(\alpha)$ for each $\alpha \in \mathbb{Q}(\zeta_{l^n})$ and each $\sigma \in G$, we regard the multiplicative group $\mathbb{Q}(\zeta_{l^n})^\times$ as the module over $\mathbb{Z}[G]$, the group ring of G over $\mathbb{Z}$, in the obvious way. Let A be any ideal of $\mathbb{Z}[\zeta_{l^n}]$. For each $\theta \in \mathbb{Z}[G]$, we put

$$A^\theta = \{\beta^\theta \mid \beta \in A\}.$$

For every $\sigma \in G$, A^σ is also an ideal of $\mathbb{Z}[\zeta_{l^n}]$; further, when A is relatively prime to (l), Proposition 1 and Definitions 1, 2 yield

$$\left(\frac{\beta_1}{A}\right)_{l^n}^{\sigma} = \left(\frac{\beta_1^\sigma}{A^\sigma}\right)_{l^n}, \quad \left(\frac{\beta_1}{\beta_2}\right)_{l^n}^{\sigma} = \left(\frac{\beta_1^\sigma}{\beta_2^\sigma}\right)_{l^n} \tag{1}$$

for every $\beta_1 \in \mathbb{Z}[\zeta_{l^n}]$ and for every $\beta_2 \in \mathbb{Z}[\zeta_{l^n}]$ relatively prime to l. When t is any rational integer relatively prime to l, we denote by σ_t the element of G mapping ζ_{l^n} to $\zeta_{l^n}^t$. In $\mathbb{Z}[G]$, let

$$\gamma = \sum_t t\sigma_t^{-1}, \tag{2}$$

where the sum is taken over all natural numbers $t < l^n$ relatively prime to l. Let P be a nonzero prime ideal of $\mathbb{Z}[\zeta_{l^n}]$. A celebrated theorem of Stickelberger (cf. [1, Chapter 14, Theorem 2]) then guarantees that $(\Phi(P))$ is decomposed in $\mathbb{Z}[\zeta_{l^n}]$ as

$$(\Phi(P)) = P^\gamma = \prod_t (P^{\sigma_t^{-1}})^t. \tag{3}$$

This induces a relation $(\Phi(A)) = A^\gamma$. Now, take any $\alpha \in \mathbb{Z}[\zeta_{l^n}] \setminus \{0\}$. Since $(\Phi(\alpha)) = (\alpha)^\gamma = (\alpha^\gamma)$, we can define a unit $\varepsilon(\alpha)$ of $\mathbb{Z}[\zeta_{l^n}]$ by

$$\Phi(\alpha) = \varepsilon(\alpha)\alpha^\gamma. \tag{4}$$

Actually $\varepsilon(\alpha)$ turns out to be a root of unity in $\mathbb{Z}[\zeta_{l^n}]$, namely,

$$\varepsilon(\alpha) = \pm\zeta_{l^n}^j \tag{5}$$

for some $j \in \mathbb{Z}$ (cf. [1, Proposition 14.5.2]). Moreover, as $\left(\dfrac{-1}{P}\right)_{l^n} = 1$, Proposition 1 gives

$$\left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n} = \zeta_{l^n}^{j(N(P)-1)/l^n} = \pm\varepsilon(\alpha)^{(N(P)-1)/l^n}. \tag{6}$$

Proposition 4. *If $\alpha \in \mathbb{Z}[\zeta_{l^n}]$ is primary, then $\varepsilon(\alpha) = \pm\zeta_{l^{n-1}}^k$ with some $k \in \mathbb{Z}$.*

Proof. We assume that $\alpha \in \mathbb{Z}[\zeta_{l^n}]$ is primary, whence

$$\varepsilon(\alpha)\alpha^\gamma \equiv \pm 1 \pmod{l} \tag{7}$$

by (4) and Proposition 3. Let $\lambda = 1 - \zeta_{l^n}$. Since l is totally ramified in $\mathbb{Q}(\zeta_{l^n})$ or, equivalently, $(\lambda)^{l^{n-1}(l-1)} = (l)$, we have $(\lambda)^\sigma = (\lambda)$ for all $\sigma \in G$. Furthermore, by Definition 3, there is a rational integer a such that $\alpha \equiv a \pmod{(\lambda)^2}$. Hence (2) gives $\alpha^\gamma \equiv a^{\sum_t t} \pmod{(\lambda)^2}$, where the sum is taken over the natural numbers $t < l^n$ relatively prime to l. Therefore

$$\alpha^\gamma \equiv a^{l^{2n-1}(l-1)/2} \equiv a^{(l-1)/2} \equiv \pm 1 \pmod{(\lambda)^2}$$

and, consequently, (5) and (7) yield $\zeta_{l^n}^j \equiv \pm 1 \pmod{(\lambda)^2}$ with some $j \in \mathbb{Z}$. On the other hand,

$$\zeta_{l^n}^j = (1-\lambda)^j \equiv 1 - j\lambda \pmod{(\lambda)^2}.$$

Thus $1 - j\lambda \equiv \pm 1 \pmod{(\lambda)^2}$. If $1 - j\lambda \equiv -1 \pmod{(\lambda)^2}$, however, λ would divide 2. This contradiction shows that $1 - j\lambda \equiv 1 \pmod{(\lambda)^2}$, i.e., l divides j. □

We are now ready to prove our main theorem.

Theorem 1. *Let p be a prime number different from l, α a primary element of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to p, and P any prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ containing p. Then*

$$\left(\frac{\alpha}{p}\right)_{l^n}^f \left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n} = \left(\frac{p}{\alpha}\right)_{l^n}^f;$$

here f denotes the degree of P, whence f is the order of p modulo l^n, namely, the smallest natural number such that $p^f \equiv 1 \pmod{l^n}$.

Proof. Let Q be any prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ dividing (α). By Definitions 1, 4 and the definitions of χ_Q, ψ_Q,

$$g(Q)^{p^f} \equiv \sum_{u\in\mathbb{Z}[\zeta_{l^n}]/Q} \chi_Q(u)^{p^f}\psi_Q(u)^{p^f} \pmod{p},$$

$$\sum_{u\in\mathbb{Z}[\zeta_{l^n}]/Q} \chi_Q(u)^{p^f}\psi_Q(u)^{p^f} = \sum_{u\in\mathbb{Z}[\zeta_{l^n}]/Q} \chi_Q(u)\psi_Q(p^f u)$$

$$= \sum_{u\in\mathbb{Z}[\zeta_{l^n}]/Q} \chi_Q(p^f)^{-1}\chi_Q(p^f u)\psi_Q(p^f u) = \left(\frac{p^f}{Q}\right)_{l^n} g(Q).$$

Furthermore, (3) implies that $g(Q)$ is relatively prime to p. Hence

$$g(Q)^{p^f-1} \equiv \left(\frac{p^f}{Q}\right)_{l^n} \pmod{P}.$$

On the other hand, since $p^f = N(P)$, we obtain from Definitions 1 and 4

$$g(Q)^{p^f-1} = \Phi(Q)^{\frac{p^f-1}{l^n}} \equiv \left(\frac{\Phi(Q)}{P}\right)_{l^n} \pmod{P}$$

and, in $\mathbb{Z}[\zeta_{l^n}]/P$, the cosets of $1, \zeta_{l^n}, \dots \zeta_{l^n}^{l^n-1}$ are distinct. Thus

$$\left(\frac{\Phi(Q)}{P}\right)_{l^n} = \left(\frac{p^f}{Q}\right)_{l^n}.$$

This, together with Proposition 1 and Definitions 2, 5, implies that

$$\left(\frac{\Phi(\alpha)}{P}\right)_{l^n} = \left(\frac{p^f}{\alpha}\right)_{l^n} = \left(\frac{p}{\alpha}\right)_{l^n}^f.$$

Hence (4) gives

$$\left(\frac{\alpha^\gamma}{P}\right)_{l^n}\left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n} = \left(\frac{p}{\alpha}\right)_{l^n}^f.$$

Succesively by (2), Proposition 1, Definition 1, (1) and Definition 2, we also have

$$\left(\frac{\alpha^\gamma}{P}\right)_{l^n} = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{P}\right)_{l^n} = \prod_t \left(\frac{\alpha^{\sigma_t^{-1}}}{P}\right)_{l^n}^t = \prod_t \left(\frac{\alpha^{\sigma_t^{-1}}}{P}\right)_{l^n}^{\sigma_t}$$

$$= \prod_t \left(\frac{\alpha}{P^{\sigma_t}}\right)_{l^n} = \left(\frac{\alpha}{N(P)}\right)_{l^n} = \left(\frac{\alpha}{p^f}\right)_{l^n} = \left(\frac{\alpha}{p}\right)_{l^n}^f,$$

where t ranges over the natural numbers less than l^n and relatively prime to l. It therefore follows that

$$\left(\frac{\alpha}{p}\right)_{l^n}^f \left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n} = \left(\frac{p}{\alpha}\right)_{l^n}^f.$$

□

Let $n = 1$ in Theorem 1. Then, by Proposition 4, $\varepsilon(\alpha) = \pm 1$ so that $\left(\frac{\varepsilon(\alpha)}{P}\right)_l = 1$. Furthermore, since f divides $l-1$, we have

$$\left(\frac{\alpha}{p}\right)_l = \left(\frac{p}{\alpha}\right)_l,$$

taking the $(l-(l-1)/f)$th power of both sides of the equality in Theorem 1. The above equality is none other than essential part of the Eisenstein reciprocity law. Thus Theorem 1 combined with Proposition 4 can be regarded as a narrow generalization of the Eisenstein reciprocity law.

The following result is deduced directly from Theorem 1.

Corollary 1. *Let p be a prime number different from l, α a primary element of $\mathbb{Z}[\zeta_{l^n}]$ relatively prime to p, P a prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ containing p, and f the order of p modulo l^n. If f is relatively prime to l, i.e., $p^{l-1} \equiv 1 \pmod{l^n}$, then*

$$\left(\frac{\alpha}{p}\right)_{l^n}\left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n}^h = \left(\frac{p}{\alpha}\right)_{l^n}$$

for any natural number h such that $fh \equiv 1 \pmod{l^n}$.

Proof. Assume f to be relatively prime to l, and take a rational integer h with $fh \equiv 1 \pmod{l^n}$. Then, by Theorem 1,

$$\left(\frac{\alpha}{p}\right)_{l^n}\left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n}^h = \left(\left(\frac{\alpha}{p}\right)_{l^n}^f\left(\frac{\varepsilon(\alpha)}{P}\right)_{l^n}\right)^h = \left(\frac{p}{\alpha}\right)_{l^n}^{fh} = \left(\frac{p}{\alpha}\right)_{l^n}.$$

□

3 Additional results

In this last section, we add some results which are proved by means of Theorem 1.

Proposition 5. *Let p and q be distinct prime numbers different from l, and f the order of p modulo l^n. Then*

$$\left(\frac{q}{p}\right)_{l^n}^f = \left(\frac{p}{q}\right)_{l^n}^f.$$

Proof. By Theorem 1,

$$\left(\frac{q}{p}\right)_{l^n}^f\left(\frac{\varepsilon(q)}{P}\right)_{l^n} = \left(\frac{p}{q}\right)_{l^n}^f,$$

where P is a prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ containing p. Therefore it suffices to prove $\varepsilon(q) = \pm 1$. Let r be a prime number such that $r \equiv 1 \pmod{q}$ and $r \equiv l^n + 1 \pmod{l^{2n}}$. We take a prime ideal R of $\mathbb{Z}[\zeta_{l^n}]$ containing r. Let t range over the natural numbers less than l^n and relatively prime to l. Since $r \equiv 1 \pmod{l^n}$, the degree of R is 1 and $(r) = \prod_t R^{\sigma_t}$. Hence Theorem 1 shows that

$$\left(\frac{r}{q}\right)_{l^n} = \left(\frac{q}{r}\right)_{l^n}\left(\frac{\varepsilon(q)}{R}\right)_{l^n} = \left(\frac{\varepsilon(q)}{R}\right)_{l^n}\prod_t\left(\frac{q}{R^{\sigma_t}}\right)_{l^n}. \tag{8}$$

Here, by (1),

$$\prod_t\left(\frac{q}{R^{\sigma_t}}\right)_{l^n} = \prod_t\left(\frac{q}{R}\right)_{l^n}^{\sigma_t} = \prod_t\left(\frac{q}{R}\right)_{l^n}^t = \left(\frac{q}{R}\right)_{l^n}^{\sum_t t} = \left(\frac{q}{R}\right)_{l^n}^{l^{2n-1}(l-1)/2} = 1.$$

On the other hand, for every prime ideal Q of $\mathbb{Z}[\zeta_{l^n}]$ containing q, we obtain $\left(\frac{r}{Q}\right)_{l^n} = 1$ from $r \equiv 1 \pmod{q}$, so that $\left(\frac{r}{q}\right)_{l^n} = 1$ follows. We also see that $\left(\frac{\varepsilon(q)}{R}\right)_{l^n} = \pm\varepsilon(q)^{(N(R)-1)/l^n}$ by (6), and that $\varepsilon(q)^{(N(R)-1)/l^n} = \varepsilon(q)$ since $(N(R)-1)/l^n = (r-1)/l^n \equiv 1 \pmod{l^n}$. Hence (8) implies $\varepsilon(q) = \pm 1$. □

The above result yields the following.

Theorem 2. *Let p and q be distinct prime numbers different from l, and g the greatest common divisor of the orders of p and q modulo l^n. Then*

$$\left(\frac{q}{p}\right)_{l^n}^{g} = \left(\frac{p}{q}\right)_{l^n}^{g}.$$

In particular,

$$\left(\frac{q}{p}\right)_{l^n} = \left(\frac{p}{q}\right)_{l^n}$$

if g is relatively prime to l, namely, either $p^{l-1} \equiv 1 \pmod{l^n}$ or $q^{l-1} \equiv 1 \pmod{l^n}$.

Proof. Let f and f' be the orders of p and q modulo l^n, respectively. Then, by Proposition 5,

$$\left(\frac{q}{p}\right)_{l^n}^{f} = \left(\frac{p}{q}\right)_{l^n}^{f}, \quad \left(\frac{p}{q}\right)_{l^n}^{f'} = \left(\frac{q}{p}\right)_{l^n}^{f'}.$$

These clearly give the first assertion of the theorem. Naturally the second assertion is an immediate consequence of the first. □

We finally touch upon the special case where $l^n = 3^2 = 9$.

Theorem 3. *Let p be a prime number different from 3, α an element of $\mathbb{Z}[\zeta_3] \setminus \{\pm 1, \pm\zeta_3\}$ relatively prime to 3, and f the order of p modulo 9. Then*

$$\left(\frac{\alpha}{p}\right)_{9}^{f} = \left(\frac{p}{\alpha}\right)_{9}^{f};$$

in other words,

$$\left(\frac{\alpha}{p}\right)_{9} = \left(\frac{p}{\alpha}\right)_{9} \quad \textit{or} \quad \left(\frac{\alpha}{p}\right)_{9}^{3} = \left(\frac{p}{\alpha}\right)_{9}^{3}$$

according to whether $p \equiv \pm 1 \pmod 9$ or $p \not\equiv \pm 1 \pmod 9$.

Proof. There exist rational integers a and b with $\alpha = a + b\zeta_3$. Since $\zeta_3 \equiv 1 \pmod{(1-\zeta_9)^2}$, we have $\alpha \equiv a + b \pmod{(1-\zeta_9)^2}$. Therefore, by the assumption, α is a primary element of $\mathbb{Z}[\zeta_9]$.

Next, let us prove $\varepsilon(\alpha) = \pm 1$, which concludes our proof. Let q be a prime number such that $q \equiv 4 \pmod 9$, and let Q be a prime ideal of $\mathbb{Z}[\zeta_{l^n}]$ containing q. As the order of q modulo 9 is 3, Theorem 1 implies that

$$\left(\frac{\alpha}{q}\right)_{9}^{3} \left(\frac{\varepsilon(\alpha)}{Q}\right)_{9} = \left(\frac{q}{\alpha}\right)_{9}^{3}.$$

In view of (1), we find $\left(\frac{\alpha}{q}\right)_{9}^{3} = 1$, because

$$\left(\frac{\alpha}{q}\right)_{9}^{4} = \left(\frac{\alpha}{q}\right)_{9}^{\sigma_4} = \left(\frac{\alpha^{\sigma_4}}{q}\right)_{9} = \left(\frac{\alpha}{q}\right)_{9}.$$

Similarly, by (1), we have $\left(\frac{q}{\alpha}\right)_{9}^{3} = 1$. Hence, by (6),

$$1 = \left(\frac{\varepsilon(\alpha)}{Q}\right)_{9} = \pm\varepsilon(\alpha)^{(N(Q)-1)/9}.$$

However

$$\frac{N(Q)-1}{9} = \frac{(q-4)}{9}((q-4)^2 + 12(q-4) + 48) + 7 \equiv 1 \pmod 3.$$

Since Proposition 4 gives $\varepsilon(\alpha) = \pm\zeta_3^k$ for some $k \in \mathbb{Z}$, it then follows that $1 = \pm\varepsilon(\alpha)$. □

References

[1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics 84, Springer, 1990.

Mari Kouchiwa
Adress: 3-3-1-1410 Kawaguchi, Kawaguchi-shi, Saitama 332-0015
E-mail: kouchiwamari@gmail.com