PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 4, April 1990

ON RATIONAL RECIPROCITY

CHARLES HELOU

(Communicated by William Adams)

ABSTRACT. A method for deriving "rational" nth power reciprocity laws from general ones is described. It is applied in the cases $n = 3, 4, 8$, yielding results of von Lienen, Burde, Williams.

INTRODUCTION

Let n be a natural number greater than 1, and p, q two distinct prime numbers $\equiv 1 \pmod{n}$. Let ζ denote a primitive nth root of unity in $\mathbf{C}$ (the field of complex numbers), $K = \mathbf{Q}(\zeta)$, with $\mathbf{Q}$ the field of rational numbers, and $A = \mathbf{Z}[\zeta]$, with $\mathbf{Z}$ the ring of rational integers. Since $p \equiv 1 \pmod{n}$, it splits completely in K; so, if P is a prime ideal of A dividing p, the residue fields $\mathbf{Z}/p\mathbf{Z}$ and A/P are naturally isomorphic, and P has absolute norm p. For a in A not divisible by P, the nth power residue symbol in K, modulo P, $(a/P)_{n,K}$, is then the unique nth root of unity satisfying the congruence

$$(a/P)_{n,K} \equiv a^{(p-1)/n} \pmod{P}.$$

In particular, due to the residue fields isomorphism, for a in $\mathbf{Z}$ not divisible by p, $(a/P)_{n,K} = 1$ if and only if a is an nth power residue modulo p in $\mathbf{Z}$. Thus, if Q is a prime ideal of A dividing q, an expression for the "rational inversion factor" $(p/Q)_{n,K} \bullet (q/P)_{n,K}^{-1}$ may be considered as a rational reciprocity law between p and q.

2. A RATIONAL RECIPROCITY LAW

In what follows, we assume that p and q are the norms in $K/\mathbf{Q}$ of prime elements v and w of A, respectively, and that a general nth power reciprocity law is given in K. This means that an expression is given for

$$e(x, y) = (x/y) \cdot (y/x)^{-1}$$

where x and y are relatively prime, and prime to n, elements of A, and (x/y) denotes the symbol $(x/I)_{n,K}$ with $I = yA$. The latter symbol being

Received by the editors January 26, 1989 and, in revised form, May 5, 1989. Presented to the AMS meeting in Hoboken, NJ, October 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R04, 11A15.

0002-9939/90 $1.00 + $.25 per page

defined for any ideal I of A prime to n and x, from the ones with I prime, by multiplicativity in I.

Proposition. *Let $w = f(\zeta)$, with f a polynomial with coefficients in $\mathbf{Z}$ and z a rational integer $\equiv \zeta \pmod{v}$ (such a z exists and is unique modulo p, by the residue fields isomorphism). Then*

$$(p/w)\cdot(q/v)^{-1} = e(p,w)\cdot(m/v)$$

where m is a rational integer such that

$$m \equiv \prod_k f(z^k)^{k'-1} \pmod{p}$$

the product being extended to a set of positive representatives of the residue classes modulo n prime to n; and for every k, k' is a positive integer such that $kk' \equiv 1 \pmod{n}$.

Proof. Let G be the Galois group of $K/\mathbf{Q}$. It is isomorphic to the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$ of congruence classes modulo n relatively prime to n: to the class $k \pmod{n}$ corresponds the automorphism s_k of K characterized by $s_k(\zeta) = \zeta^k$. Since p (resp., q) is the product of the elements $s(v)$ (resp., $s(w)$), for s ranging in G, we have, by the bilinearity of the power residue symbol,

$$(p/w)\cdot(q/v)^{-1} = \prod_s (s(v)/w)\cdot(s(w)/v)^{-1}. \tag{1}$$

Now, for every s in G,

$$(s(v)/w)\cdot(s(w)/v)^{-1} = e(s(v),w)\cdot(w/s(v))\cdot(s(w)/v)^{-1}, \tag{2}$$

and, as follows easily from the definitions, $(w/s(v)) = s(s^{-1}(w)/v)$. Moreover, for every $k \pmod{n}$ in $(\mathbf{Z}/n\mathbf{Z})^*$,

$$s_k(w) = f(\zeta^k) \equiv f(z^k) \pmod{v},$$

and, since $s_k^{-1} = s_{k'}$ with $kk' \equiv 1 \pmod{n}$,

$$s_k^{-1}(w) \equiv f(z^{k'}) \pmod{v}.$$

Hence, $(w/s_k(v))\cdot(s_k(w)/v)^{-1} = (f(z^{k'})/v)^k \cdot (f(z^k)/v)^{-1}$. Therefore, in view of (2) and (1) and the bilinearity of $e(x,y)$,

$$(p/w)\cdot(q/v)^{-1} = e(p,w)\cdot\prod_k (f(z^{k'})^k/v)\cdot\prod_k (f(z^k)^{n-1}/v) \tag{3}$$

with $k \pmod{n}$ ranging in $(\mathbf{Z}/n\mathbf{Z})^*$, k and k' being positive. In the right-hand side of (3), one may exchange k and k' in the first product, then combine the two products into one, and eliminate the obvious nth power factors from the symbol. This yields the desired equality.

Remark. In order to determine z and the power residue character of m modulo v, in the proposition above, one may consider the norms x_j of v over some subfields of K. On the one hand, these x_j's have v as common divisor, and so by linear combination and the solution of some congruence equation modulo v, one obtains z. On the other hand, upon replacing z by ζ in the expression of m, some of these x_j's appear in the product and allow us to simplify the resulting expression for m which is obtained by rechanging ζ into z. As an interpretation of these x_j's, note that their norms over $\mathbf{Q}$ provide representations of p by some norm forms. Finally, the expression of (m/v) may, in some cases, be simplified further by using the power reduction property (if d is a positive divisor of n, then $(x/y)_{n,K}^{d} = (x/y)_{n/d,K}$) and the norm property (if x is in a subfield E of K containing ζ and N is the norm in K/E, then $(x/y)_{n,K} = (x/Ny)_{n,E}$). These follow from the fundamental properties of the symbol (for which, see [3], Chapter 14).

3. Examples

(i) $n = 3$. Let $v = a + b\zeta$, with ζ a primitive third root of unity, a and b in $\mathbf{Z}$. So $p = Nv = a^2 - ab + b^2$, and a, b are prime to p. Let b' be an inverse of b modulo p, in $\mathbf{Z}$. Let $w = c + d\zeta = f(\zeta)$. Then, by the proposition above, with $z \equiv -ab' \pmod{p}$,

$$(p/w) \cdot (q/v)^{-1} = e(p, w) \cdot (f(z^2)/v). \tag{4}$$

By the cubic reciprocity law ([2], p. 73), $e(p, w) = e(v, w) \cdot e(\overline{v}, w) = 1$ (where $\overline{v}$ is the complex conjugate of v), provided that v and w are primary, i.e. $a, c \equiv 2 \pmod{3}$ and $b, d \equiv 0 \pmod{3}$. Note also that $z^2 \equiv -a'b \pmod{p}$, with a' in Z such that $aa' \equiv 1 \pmod{p}$. Hence the right-hand side of (4) is $((c - da'b)/v) = (a^2(ac - bd)/v)$. The resulting expression was given by von Lienen in [4]. It can be simplified by again using the cubic reciprocity law which yields $(a/v) = \zeta^{(a+1)/3}$. We thus obtained

Corollary 1. *Let p, q be two prime numbers $\equiv 1 \pmod{3}$, $p = a^2 - ab + b^2$, $q = c^2 - cd + d^2$, with $a, c \equiv 2 \pmod{3}$ and $b, d \equiv 0 \pmod{3}$, in $\mathbf{Z}$. Let $v = a + b\zeta$ and $w = c + d\zeta$, in $K = \mathbf{Q}(\zeta)$, with ζ a primitive cubic root of unity. Then*

$$(p/w)_{3,K} \cdot (q/v)_{3,K}^{-1} = \zeta^{-(a+1)/3} \cdot ((ac - bd)/v)_{3,K}.$$

(ii) $n = 4$. Let $v = a + bi$, with i a primitive fourth root of unity, and a, b in $\mathbf{Z}$. So $p = Nv = a^2 + b^2$. Let a' and b' be inverses of a and b modulo p, respectively, in $\mathbf{Z}$. Then, by the proposition above, with $z \equiv -ab' \equiv a'b \pmod{p}$, and $w = c + di = f(i)$,

$$(p/w) \cdot (q/v)^{-1} = e(p, w) \cdot (f(z^3)/v)^2. \tag{5}$$

By the biquadratic reciprocity law ([2], p. 138), $e(p, w) = (-1)^{((p-1)/2)\cdot((c-1)/2)} = 1$, provided that w is primary, i.e. c is odd and $d \equiv c - 1 \pmod{4}$. Note

also that $z^3 \equiv -a'b \equiv ab' \pmod{p}$. Thus, using the power reduction and the norm properties of the symbol, the right-hand side of (5) is $((c-da'b)/v)_{4,K}^2 = (a/p)_{2,\mathbf{Q}} \cdot ((ac-bd)/p)_{2,\mathbf{Q}}$. Moreover, provided a is odd, the quadratic reciprocity law for the Jacobi symbol yields $(a/p)_{2,\mathbf{Q}} = 1$. Alternatively, with ab' substituted for z^3, we would have obtained, for the right-hand side of (5), $(b^2/v)_{4,K} \cdot ((bc+ad)/p)_{2,\mathbf{Q}}$; and $(b^2/v)_{4,K} = (-a^2/v)_{4,K} = (-1/v)_{4,K} = (-1)^{(p-1)/4}$. Finally, note that the left-hand side of (5) and both expressions obtained for the right-hand side are invariant if v or w is changed into its opposite (since -1 is a quadratic residue mod p). So it is enough to assume that a and c are odd, and then either v or $-v$ (resp., w or $-w$) is primary. Thus

Corollary 2. *Let p, q be two prime numbers $\equiv 1 \pmod 4$, $p = a^2 + b^2$, $q = c^2 + d^2$, with a, b, c, d in $\mathbf{Z}$ and a, c odd. Let $v = a + bi$ and $w = c + di$ in $K = \mathbf{Q}(i)$. Then*

$$(p/w)_{4,K} \cdot (q/v)_{4,K}^{-1} = ((ac-bd)/p)_{2,\mathbf{Q}} = (-1)^{(p-1)/4} \cdot ((ad+bc)/p)_{2,\mathbf{Q}}.$$

In particular, one obtains Burde's law [1] upon replacing v by its complex conjugate $\overline{v} = a - bi$ in the above, since $(q/v)_{4,K} = (q/\overline{v})_{4,K}^{-1}$.

(iii) $n = 8$. Since $K = \mathbf{Q}(\zeta)$, with ζ a primitive eighth root of unity, has class number 1, there always exist prime elements v and w in $A = \mathbf{Z}[\zeta]$ with norms, in $K/\mathbf{Q}$, p and q, respectively. Moreover, v and w may be chosen primary, i.e. $\equiv 1 \pmod{2(\zeta - 1)}$. The Galois group of $K/\mathbf{Q}$ consists of s_k, for $k = 1, 3, 5, 7$, where $s_k(\zeta) = \zeta^k$. So, K has two imaginary quadratic subfields $E_1 = \mathbf{Q}(i)$ and $E_2 = \mathbf{Q}(i\sqrt{2})$, fixed fields of $\{s_1, s_5\}$ and $\{s_1, s_3\}$, respectively. Let $x_1 = vs_5(v) = a_1 + b_1 i$ and $x_2 = vs_3(v) = a_2 + b_2(\zeta + \zeta^3)$ be the norms of v over E_1 and E_2, respectively, where a_1, b_1, a_2, b_2 are in $\mathbf{Z}$ (here $\zeta^2 = i; \zeta + \zeta^3 = i\sqrt{2}$). Then, taking norms over $\mathbf{Q}$, we get $p = a_1^2 + b_1^2 = a_2^2 + 2b_2^2$. Also, v being a common divisor of x_1 and x_2, we have $b_1 x_2 - \zeta b_2 x_1 = b_1 a_2 + b_2(b_1 - a_1)\zeta \equiv 0 \pmod{v}$. Thus, the value of $\zeta \pmod{v}$ is $z \equiv a_2 b_1 b_2'(a_1 - b_1)' \pmod{p}$, where, for r in $\mathbf{Z}$ not divisible by p, r' denotes an inverse of r modulo p. Let $w = f(\zeta)$, with f in $\mathbf{Z}[X]$. By the proposition above and the power reduction and the norm properties of the symbol, we have

$$(6) \qquad (p/w)_{8,K} \cdot (q/v)_{8,K}^{-1} = e(p, w) \cdot (f(z^3) f(z^5)^2 f(z^7)^3 / x_1)_{4,E_1}.$$

By Eisenstein's octic reciprocity law ([2], p. 616), provided w is primary, $e(p, w) = (-1)^{((p^4-1)/8)\cdot((q-1)/8)} = 1$.

Now, let $y_1 = f(\zeta)f(\zeta^5) = c_1 + d_1 i$ and $y_2 = f(\zeta)f(\zeta^3) = c_2 + d_2(\zeta + \zeta^3)$ be the norms of w over E_1 and E_2, respectively; so $q = c_1^2 + d_1^2 = c_2^2 + 2d_2^2$, with c_1, d_1, c_2, d_2 in $\mathbf{Z}$. We have

$$f(\zeta^3)f(\zeta^7) = s_3(y_1) = c_1 - d_1 i; \; f(\zeta^5)f(\zeta^7) = s_5(y_2) = c_2 - d_2(\zeta + \zeta^3).$$

So, in virtue of the residue fields isomorphism (and noting that $i = \zeta^2$), $f(z^3)f(z^7) \equiv c_1 - d_1 z^2 \pmod{p}$; $f(z^5)f(z^7) \equiv c_2 - d_2(z + z^3) \pmod{p}$. Hence, $f(z^3)f(z^5)^2 f(z^7)^3 \equiv (c_1 - d_1 z^2)(c_2 - d_2(z + z^3))^2 \pmod{p}$. It follows that the right-hand side of (6) is equal to $u_1 u_2$ where $u_1 = ((c_1 - d_1 z^2)/x_1)_{4,E_1}$ and $u_2 = ((c_2 - d_2(z + z^3))/p)_{2,\mathbf{Q}}$. Moreover, it is easily seen that $z^2 \equiv a_1' b_1 \equiv -a_1 b_1' \pmod{p}$ and $z + z^3 \equiv -a_2 b_2' \pmod{p}$. Hence

$$\begin{aligned} u_1 &= (a_1/x_1)_{4,E_1}^{-1} \cdot ((a_1 c_1 - b_1 d_1)/x_1)_{4,E_1} \\ &= (b_1/x_1)_{4,E_1}^{-1} \cdot ((a_1 d_1 + b_1 c_1)/x_1)_{4,E_1} \end{aligned}$$

and

$$u_2 = (b_2/p)_{2,\mathbf{Q}} \cdot ((a_2 d_2 + b_2 c_2)/p)_{2,\mathbf{Q}}.$$

Also, provided v is primary in A, its norm x_1 is primary in $\mathbf{Z}[i]$, and then, since $p = a_1^2 + b_1^2 \equiv 1 \pmod{8}$ and $b_1 \equiv a_1 - 1 \pmod{4}$, we have $a_1 \equiv 1 \pmod{4}$. So, by the biquadratic reciprocity law,

$$(a_1/x_1)_{4,E_1} = (x_1/a_1)_{4,E_1} = (i/a_1)_{4,E_1} = (-1)^{(p-1)/8}.$$

Consequently, $(b_1/x_1)_{4,E_1} = (ia_1/x_1)_{4,E_1} = 1$. On the other hand, using the fact that 2 is a quadratic residue modulo p and the quadratic reciprocity law, we get $(b_2/p)_{2,\mathbf{Q}} = 1$. Hence

$$u_1 = (-1)^{(p-1)/8} \cdot ((a_1 c_1 - b_1 d_1)/x_1)_{4,E_1} = ((a_1 d_1 + b_1 c_1)/x_1)_{4,E_1}$$

and $u_2 = ((a_2 d_2 + b_2 c_2)/p)_{2,\mathbf{Q}}$. Finally, note that u_1 and u_2 are unchanged if any of x_1, x_2, y_1, y_2 is replaced by its opposite; if x_1 is chosen a priori, having norm over $\mathbf{Q}$ equal to p and with a_1 odd, then a primary prime divisor v of p in A has for norm, over E_1, x_1 or $-x_1$; and the left-hand side of (6) is invariant if v (or w) is replaced by any of its associates. Similar remarks apply to y_1, and also to x_2 and to y_2. Thus

Corollary 3. *Let p and q be two prime numbers $\equiv 1 \pmod{8}$, $p = a_1^2 + b_1^2 = a_2^2 + 2b_2^2$ and $q = c_1^2 + d_1^2 = c_2^2 + 2d_2^2$, with $a_1, b_1, a_2, b_2, c_1, d_1, c_2, d_2$ in $\mathbf{Z}$ and a_1, a_2, c_1, c_2 odd. Let v (resp., w) be a common prime divisor in $\mathbf{Z}[\zeta]$ of $a_1 + b_1 i$ and $a_2 + b_2 i\sqrt{2}$ (resp., of $c_1 + d_1 i$ and $c_2 + d_2 i\sqrt{2}$), where ζ is a primitive eighth root of unity and $i = \zeta^2$. Also $K = \mathbf{Q}(\zeta)$, $E = \mathbf{Q}(i)$. Then*

$$\begin{aligned} (p/w)_{8,K} \cdot (q/v)_{8,K}^{-1} &= (-1)^{(p-1)/8} \cdot ((a_1 c_1 - b_1 d_1)/(a_1 + b_1 i))_{4,E} \\ &\quad \cdot ((a_2 d_2 + b_2 c_2)/p)_{2,\mathbf{Q}} \\ &= ((a_1 d_1 + b_1 c_1)/(a_1 + b_1 i))_{4,E} \cdot ((a_2 d_2 + b_2 c_2)/p)_{2,\mathbf{Q}}. \end{aligned}$$

In particular, one obtains Williams' law [5] upon replacing w by its complex conjugate and exchanging the roles of p and q.

References

1. K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175–184.
2. G. Eisenstein, *Mathematische Werke* I and II, Chelsea, 1975.
3. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer, Berlin, 1982.
4. H. von Lienen, *Reelle kubische und biquadratische Legendre-Symbole*, J. Reine Angew. Math. **305** (1979), 140–154.
5. K. S. Williams, *A rational octic reciprocity law*, Pacific J. Math. **63** (1976), 563–570.

Department of Mathematics, Pennsylvania State University, Delaware County Campus, 25 Yearsley Road, Media, Pennsylvania 19063