Quadratic Reciprocity in a Finite Group

William Duke   Kimberly Hopkins

Dedicated to the memory of Abe Hillman

1 INTRODUCTION

The law of quadratic reciprocity is a gem from number theory. In this article we show that it has a natural interpretation that can be generalized to an arbitrary finite group. Our treatment relies almost exclusively on concepts and results known at least a hundred years ago.[1]

A key role in our story is played by group characters. Recall that a *character* χ of a finite Abelian group G is a homomorphism from G into $\mathbb{C}^*$, the multiplicative group of nonzero complex numbers. The set of all distinct characters forms a group under point-wise multiplication that is isomorphic to G. Later we will need the notion of a character defined on an arbitrary finite group G, which is the trace of a finite-dimensional representation of G.

A character χ of the group $(\mathbb{Z}/n\mathbb{Z})^*$ of reduced residue classes modulo a positive integer n gives rise to a *Dirichlet character* modulo n, also denoted by χ, which is the function on the integers defined by

$$\chi(a) = \begin{cases} \chi(a) & \text{if } a \text{ is prime to } n, \\ 0 & \text{otherwise.} \end{cases}$$

In case $n = p$ is an odd prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of (even) order $p-1$. Thus it has a unique character of order 2. Its associated Dirichlet character is called the *Legendre symbol* $\left(\frac{\cdot}{p}\right)$. Hence $\left(\frac{a}{p}\right) = 0$ if $p\,|\,a$; otherwise we have that $\left(\frac{a}{p}\right) = 1$ if a is a square modulo p and $\left(\frac{a}{p}\right) = -1$ if a is not a square modulo p.

[1]See [2, Chap.1] for a beautiful exposition of much of the nineteenth-century algebra and number theory we will take as known.

In 1872 Zolotarev [13] gave an interpretation of the Legendre symbol $\left(\frac{a}{p}\right)$ that is less well-known: it gives the sign of the permutation of the elements of $G = \mathbb{Z}/p\,\mathbb{Z}$ induced by multiplication by a, provided $p \nmid a$. To see this, first observe that this recipe defines a character on $(\mathbb{Z}/p\,\mathbb{Z})^*$. Furthermore, if it is not trivial, this character must have order 2 and hence give the Legendre symbol. But it is not trivial, for a generator of $(\mathbb{Z}/p\,\mathbb{Z})^*$ induces a $(p-1)$-cycle, which is an odd permutation. Motivated by this observation, we will define in section 3 below a quadratic symbol for any finite group G.

The classical law of quadratic reciprocity states that for distinct odd primes p and q the following hold:

$$\left(\tfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\tfrac{p}{q}\right), \quad \left(\tfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\tfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1}$$

This was first proven by Gauss in 1796 when he was nineteen years old. By 1818 he had published six proofs.[2] The ideas behind his sixth proof [5] (see [2, p.19]), based on the Gauss sum, led to proofs of quadratic reciprocity using the arithmetic of cyclotomic fields and the Frobenius automorphism, which was introduced in 1896 [3]. We will combine this classical technique with another invention of Frobenius from 1896 [4], the character table, to prove a law of reciprocity for the quadratic symbol for any finite group G. A corollary of our result, given in section 3, implies classical quadratic reciprocity when $G = \mathbb{Z}/p\,\mathbb{Z}$ and also extends Zolotarev's observation to any group of odd order.

2 THE KRONECKER SYMBOL

Before explaining this generalization, we restate the law of quadratic reciprocity in one formula by introducing the Jacobi and Kronecker symbols. The *Jacobi symbol* simply extends the Legendre symbol to $\left(\frac{\cdot}{n}\right)$ for an arbitrary odd positive integer n by multiplicativity: if $n > 1$ and $n = p_1 \cdots p_r$ is its factorization into (not necessarily distinct) primes, we have

$$\left(\tfrac{a}{n}\right) = \prod_{k=1}^{r} \left(\tfrac{a}{p_k}\right),$$

while $\left(\frac{a}{1}\right) = 1$.

[2] A good reference for the many known proofs of the law of quadratic reciprocity is [8]. Recently a novel elementary proof was found by S. Kim [7].

A *discriminant* is a nonzero integer d that is congruent to either 0 or 1 modulo 4.[3] For a discriminant d, the *Kronecker symbol* $\left(\frac{d}{\cdot}\right)$ further extends the Jacobi symbol via the definition

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{if } d \text{ is even,} \\ 1 & \text{if } d \equiv 1 (\bmod 8), \\ -1 & \text{if } d \equiv 5 (\bmod 8), \end{cases}$$

and by letting $\left(\frac{d}{-1}\right)$ be the sign of d. The value of $\left(\frac{d}{a}\right)$ is then defined for all integers a by multiplicativity, where we set $\left(\frac{d}{0}\right) = 0$ when $d \neq 1$ and $\left(\frac{1}{0}\right) = 1$. By means of these extensions, the law of quadratic reciprocity (1) takes an elegant form for n positive and odd and any integer a:

$$\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right), \tag{2}$$

where $n^* = (-1)^{\frac{n-1}{2}} n$. Note that n^* is a discriminant because n is odd.

3 THE QUADRATIC SYMBOL FOR A FINITE GROUP

Let G be a finite group of order n. An integer a that is prime to n induces a permutation, call it ϕ, of the m conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$ of G by sending each element g to g^a and hence C_j to C_j^a. Define the quadratic symbol for G at any integer a by

$$\left(\frac{a}{G}\right) = \begin{cases} 0 & \text{if } (a, n) \neq 1, \\ 1 & \text{if } \phi \text{ is even,} \\ -1 & \text{if } \phi \text{ is odd.} \end{cases} \tag{3}$$

It is easy to see that $\left(\frac{\cdot}{G}\right)$ defines a real Dirichlet character modulo n.[4] Zolotarev's observation from the introduction is that the quadratic symbol for $G = \mathbb{Z}/p\,\mathbb{Z}$ with an odd prime p is the Legendre symbol:

$$\left(\frac{a}{G}\right) = \left(\frac{a}{|G|}\right). \tag{4}$$

[3] We include the possibility that d is a square, which is usually disallowed.

[4] In fact, it is defined modulo the least common multiple of the orders of all elements of G.

A conjugacy class C in an arbitrary group G is said to be *real* if $C^{-1} = C$ and *complex* otherwise. Here C^{-1} denotes the image of C under the correspondence $g \mapsto g^{-1}$. Clearly the complex conjugacy classes occur in pairs C and C^{-1} with $|C| = |C^{-1}|$. We order the conjugacy classes so that the first r_1 are real. Thus $m = r_1 + 2r_2$, where r_2 is half the number of complex conjugacy classes. We then set

$$d = d(G) = (-1)^{r_2}|G|^{r_1}\prod_{j=1}^{r_1}|C_j|^{-1}. \tag{5}$$

This is a nonzero integer since for any conjugacy class C and any element g of C we have $|G|/|C| = |C_G(g)|$, where $C_G(g)$ signifies the centralizer of g [2, p.42]. It is clear that d is divisible by $n = |C_G(1)|$ and has the same prime divisors as n. We call d the *discriminant of* G, a name that is justified by the first statement of our main result.

Theorem 1 *Let G be a finite group with discriminant d as defined by (5). Then $d \equiv 0$ or $1 \pmod 4$, and for any integer a*

$$\left(\frac{a}{G}\right) = \left(\frac{d}{a}\right). \tag{6}$$

In particular, $\left(\frac{\cdot}{G}\right)$ is trivial if and only if d is a square.

In case G has odd order we have the following direct generalization of classical quadratic reciprocity (2):

Corollary 1 *If G has odd order n, then $d = n^*$ and for any integer a,*

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right). \tag{7}$$

Also, $\left(\frac{\cdot}{G}\right)$ is trivial if and only if n is a square.

It follows from (7) and (2) that Zolotarev's result (4) holds for any group G of odd order.

4 PROOFS

We shall refer to [6] and [10] for the basic facts we need about characters of finite groups and algebraic number fields.

Let G be a finite group G with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$. The character table of G (see [6, p.159]) is the $m \times m$ matrix:

$$M = \begin{pmatrix} \chi_1(C_1) & \ldots & \chi_1(C_m) \\ \vdots & \ddots & \vdots \\ \chi_m(C_1) & \ldots & \chi_m(C_m) \end{pmatrix}, \tag{8}$$

where $\chi_1 = 1, \chi_2, \ldots, \chi_m$ are the irreducible characters of G [6, p.119]. Here we use the convention that $\chi(C) = \chi(g)$ for any g in C. By the (second) orthogonality relations for characters [6, Theorem 16.4(2), p.161] we have

$$M^*M = \begin{pmatrix} |G||C_1|^{-1} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & |G||C_m|^{-1} \end{pmatrix}, \tag{9}$$

a diagonal matrix. Here M^* denotes the conjugate transpose of M. Since $\chi(C^{-1}) = \bar{\chi}(C)$ for any character χ and any conjugacy class C, it is easy to see that

$$\det \bar{M} = (-1)^{r_2} \det M. \tag{10}$$

Appealing to (9) and (5) we arrive at the identity

$$(\det M)^2 = \ell^2 d \tag{11}$$

for some positive integer ℓ.

Each entry $\chi_i(C_j)$ of M is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$. Now $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to $(\mathbb{Z}/n\,\mathbb{Z})^*$ by the map $\sigma_a \mapsto a$, with σ_a in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acting on ζ_n by

$$\sigma_a(\zeta_n) = \zeta_n^a$$

[10, Theorem 1 p.92]. Using this information, it is not difficult to check that

$$\sigma_a(\chi(g)) = \chi(g^a) \tag{12}$$

for any character χ and any element g of G.

To prove the first statement of Theorem 1, we apply an argument used by Schur [12] to prove Stickelberger's theorem about the discriminant of a number field. Observe that by the definition of the determinant

$$\det M = \sum \operatorname{sgn}(\rho)\chi_1(C_{\rho(1)})\chi_2(C_{\rho(2)})\ldots\chi_m(C_{\rho(m)}),$$

where the sum is over all permutations ρ of the integers $\{1,\ldots,m\}$ and where $\operatorname{sgn}(\rho) = \pm 1$ according to whether ρ is even or odd. Write this as $A - B$, where A is the sum of the even permutations and B is the sum of the odd permutations. By (12) both of the algebraic integers $A + B$ and AB are invariant under the Galois group, hence are ordinary integers. In particular, invoking (11) we see that

$$\ell^2 d = (A-B)^2 = (A+B)^2 - 4AB \equiv (A+B)^2 \equiv 0, 1 \pmod 4,$$

which proves the first statement.[5]

It is apparent from (8) and (12) that

$$\sigma_a(\det M) = \left(\frac{a}{G}\right) \det M, \tag{13}$$

so by (11) we have

$$\sigma_a(\sqrt{d}) = \left(\frac{a}{G}\right) \sqrt{d}. \tag{14}$$

Since $\left(\frac{\cdot}{G}\right)$ is a character modulo n, to prove (6) it is enough to show it for $a = p$ such that $p \nmid n$ and for $a = -1$. If $p \nmid n$ we use the automorphism σ_p, which is called the *Frobenius automorphism* of p. We say that a prime p *splits* in an algebraic number field K if the principal ideal generated by p in the ring of integers of K factors into $[K : \mathbb{Q}]$ distinct prime ideals, where $[K : \mathbb{Q}]$ is the degree of K over $\mathbb{Q}$. The Frobenius automorphism σ_p has the property that p splits in any subfield of $\mathbb{Q}(\zeta_n)$ if and only if σ_p fixes that subfield point-wise [10, p.91]. Thus p splits in $\mathbb{Q}(\sqrt{d})$ if and only if $\sigma_p(\sqrt{d}) = \sqrt{d}$. Furthermore, the Kronecker symbol has the fundamental property that p splits in $\mathbb{Q}(\sqrt{d})$ if and only if $\left(\frac{d}{p}\right) = 1$ [10, p. 77]. Thus we infer from (14) that for $p \nmid n$

$$\left(\frac{p}{G}\right) = \left(\frac{d}{p}\right).$$

[5] Added 12/8/09: Note that if ℓ is even then necessarily n is even and so there must be a non-trivial real conjugacy classes having an odd number of elements, so $4 \mid d$.

In view of (10) and (5) we have

$$\left(\frac{-1}{G}\right) = (-1)^{r_2} = \left(\frac{d}{-1}\right), \tag{15}$$

finishing the proof of (6).

It is a standard result [9, Theorem 3.3, p.72] that if d is not a square then $\left(\frac{d}{\cdot}\right)$, hence $\left(\frac{\cdot}{G}\right)$, is nontrivial. Thus we have established Theorem 1.

Suppose now that G has odd order n. Burnside [1, section 222 p.294] observed that C_1 is the only real conjugacy class. To see this, suppose that g is in a real conjugacy class. In particular, $h^{-1}gh = g^{-1}$ for some h. Then $h^{-2}gh^2 = g$, which places h^2 in $C_G(g)$. Since n is odd, the order of h is odd, say $2\ell + 1$. It follows that $h = (h^2)^{\ell+1}$, implying that h belongs to $C_G(g)$. Thus $g = g^{-1}$. Since g has odd order, $g = 1$.

Because $r_1 = 1$, it is clear from (5) that $d = (-1)^{\frac{m-1}{2}} n$. By the first statement of Theorem 1 we must have

$$d = (-1)^{\frac{n-1}{2}} n = n^*,$$

since n is odd.[6] The last statement of Corollary 1 follows from that of Theorem 1, for when n is odd n^* is a square if and only n is a square.

5 SOME EXAMPLES

We compute the discriminants of some groups with even order. Suppose first that G is Abelian and that the subgroup of G consisting of 1 and the elements of order 2 has order 2^t. Then $r_1 = 2^t$, so

$$d = (-1)^{\frac{n-2^t}{2}} n^{2^t}.$$

It follows that for an Abelian group G of even order n the symbol $\left(\frac{\cdot}{G}\right)$ is nontrivial if and only if $4 \mid n$ and $t = 1$, in which case we have

$$\left(\frac{a}{G}\right) = (-1)^{\frac{a-1}{2}}$$

whenever $(a, n) = 1$. The condition $t = 1$ holds for instance if G is cyclic.

In general, if G has only rational characters, then it follows easily from (12) that $\left(\frac{\cdot}{G}\right)$ is the trivial character and hence that d is a square. This holds

[6] A stronger result discovered by Burnside [1, p.295] is that $n \equiv m \pmod{16}$.

in particular for the symmetric group $G = S_k$, where one can also explicitly compute d.

On the other hand, it is not difficult to produce non-Abelian groups with only real characters and with nontrivial quadratic symbols. Consider, for example, the family of simple groups given by $G_r = \mathrm{SL}(2, \mathbb{F}_q)$ for $q = 2^r$ with $r > 1$ (i.e., the group of 2×2 matrices of determinant one with entries from the field $\mathbb{F}_q$ of order q). By [11, p.134 (= p.247 in Gesammelte Abhandlungen)] we have $n = q(q^2 - 1)$, $m = r_1 = q + 1$, and

$$d = q^2(q+1)(q^2-1)^{q/2},$$

which is a square if and only if $r = 3$. The last statement follows from the fact that if $q + 1 = x^2$, then $2^r = x^2 - 1 = (x-1)(x+1)$. Thus $x = 2\ell + 1$, so $2^{r-2} = \ell(\ell+1)$, which implies that $r = 3$. If $r = 2$ we obtain $G_2 = A_5$ and $\left(\frac{a}{A_5}\right) = \left(\frac{5}{a}\right)$. For $r = 16$, $\left(\frac{a}{G_{16}}\right) = \left(\frac{65537}{a}\right)$ with $65537 = 2^{16} + 1$, a prime.

ACKNOWLEDGMENTS: The research of the first author is partially supported by NSF Grant DMS-0355564. The research of the second author was supported by UC LEADS. We would like to thank Jeff Stopple and the referee for their helpful suggestions.

References

[1] W. Burnside, *Theory of Groups of Finite Order,* 2nd ed. Cambridge University Press, Cambridge, 1911.

[2] C. W. Curtis, *Pioneers of Representation Theory: Frobenius, Burnside, Schur and Brauer,* American Mathematical Society, Providence, 1999.

[3] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *S'ber. Akad. Wiss. Berlin*(1896) 689–703; also in *Gesammelte Abhandlungen*, vol.2, Springer-Verlag, Berlin, 1968, pp. 719–733.

[4] ———-, Über Gruppencharaktere, *S'ber. Akad. Wiss. Berlin* (1896) 985–1021; also in *Gesammelte Abhandlungen*, vol.3, Springer-Verlag, Berlin, 1968, pp.1–37.

[5] C. F. Gauss, Theorematis fundamentalis in doctrina de residuis quadraticus demonstrationes et ampliationes novæ, 1818; also in *Werke* vol.2, pp.47-64.

[6] G. G. James and M. Liebeck, *Representations and characters of groups,* 2nd ed., Cambridge University Press, New York, 2001.

[7] S. Y. Kim, An elementary proof of the quadratic reciprocity law, *Amer. Math. Monthly* **111** (2004), 48–50.

[8] F. Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein,* Springer-Verlag, Berlin, 2000.

[9] H. E. Rose, *A Course in Number Theory,* 2nd ed., Clarendon Press, Oxford, 1996

[10] P. Samuel, *Algebraic Theory of Numbers* (trans A. J. Silberger) Houghton Mifflin, Boston, 1970.

[11] I. Schur, Untersuchungen über die Darstellung der endliche Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angewant. Math.* **132** (1907) 85–137; also in *Gesammelte Abhandlungen* vol.1, Springer-Verlag, Berlin, 1973, pp. 198–250.

[12] ————, Elementarer Beweis eines Satzes von L. Stickelberger, *Math. Zeit.* **29** (1928) 464–465; also in *Gesammelte Abhandlungen* vol.3, Springer-Verlag, Berlin, 1973, pp.87–88.

[13] G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouvelles Ann. Math.* (2) **11** (1872) 354–362.

BILL DUKE was an undergraduate at the University of New Mexico and obtained his Ph.D. at the Courant Institute under the direction of Peter Sarnak in 1986. He taught at Rutgers until 2000, when he moved to UCLA and great weather the year round. His research has been in number theory, especially the analytic theory of L-functions and automorphic forms.

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555

duke@math.ucla.edu

KIMBERLY HOPKINS graduated from University of California, Santa Barbara, and is attending the University of Texas at Austin for her Ph.D. studies as a Donald D. Harrington Fellow. She was selected by the Association for Women in Mathematics to receive the 2004 Alice T. Schafer Prize under her maiden name, Kimberly Spears.

Department of Mathematics, University of Texas at Austin, Austin, Texas 78712

khopkins@math.utexas.edu