A GENERALIZATION OF THE LEGENDRE SYMBOL FOR FINITE ABELIAN GROUPS

Philippe DELSARTE

Philips Research Laboratory, Av. Van Becelaere 2, B-1170 Brussels, Belgium

Received 14 January 1977
Revised 27 February 1979

Let \( G \) be a finite Abelian group. Given an integer \( n \) relatively prime to the order of \( G \), let \( \sigma_n \) be the permutation on \( G \) defined by \( \sigma_n(x) = x^n \). The problem studied in the paper is to determine the parity of \( \sigma_n \). Generalizations of well-known theorems on the Legendre symbol are obtained in this context.

1. Introduction

Consider the following general problem: how to characterize the automorphisms of a finite group \( G \) that act as even or odd permutations? When \( G \) has prime order, this problem is solved by the classical theory of the Legendre symbol [1]. The present note is concerned with an Abelian group \( G \) and the signature of any central automorphism, which has the form \( x \mapsto x^a (G \to G) \) for a given integer \( a \); the generalized Legendre symbol \( (a \mid G) \) is introduced to denote this signature.

The main results can be summarized as follows. Let \( n \) be the order of \( G \), and \( t \) the number of involutions in \( G \). For an integer \( a \), relatively prime to \( n \), let us write

\[
a = (-1)^\alpha 2^\beta p_1 p_2 \cdots p_s,
\]

where \( p_1, \ldots, p_s \) are odd primes, \( \alpha = 0 \) or \( 1 \), and \( \beta \) is a nonnegative integer.

Define the integer \( \gamma \) by

\[
8 \gamma = 2(n-1-t)(2\alpha - s + p_1 + \cdots + p_s) + \beta (n^2 - 1).
\]

Let \( (a \mid p) \) be the ordinary Legendre symbol with respect to an odd prime \( p \). Then the generalized Legendre symbol \( (a \mid G) \) is given by the formula

\[
(a \mid G) = (-1)^\gamma \prod_{i=1}^s (n \mid p_i)^\alpha.
\]

In order to prove this we shall derive expressions for \( (-1 \mid G) \), for \( (2 \mid G) \) and for \( (p \mid G) \), which are generalizations of classical results. Our method essentially uses group characters over finite fields [2].
2. Definitions and preliminary results

Let $G$ be a finite Abelian group, with multiplicative notation. We shall denote by $n$ the order of $G$ and by $m$ its period, i.e., the smallest positive integer such that $x^m = 1$ holds for every $x$ in $G$. Thus $m$ divides $n$, and $m$ is divisible by each prime factor of $n$.

Given an integer $a$, relatively prime to $m$ (or, equivalently, to $n$), let us define the automorphism $\sigma_a$ of the group $G$ by

$$\sigma_a(x) = x^a \text{ for all } x \in G.$$  \hspace{1cm} (1)

**Definition.** The Legendre symbol of $a$ with respect to $G$, denoted by $(a \mid G)$, is the signature of $\sigma_a$. In other words, $(a \mid G) = -1$ or $1$ according to whether $\sigma_a$ acts as an even or odd permutation on $G$.

The classical Legendre symbol $(a \mid q)$ is defined as follows [1, p. 68]. Let $q$ be an odd prime and $a$ any integer not divisible by $q$. Then $(a \mid q) = 1$ or $-1$ according to whether the congruence $z^2 \equiv a \pmod{q}$ has or has not a solution for $z$. We quote the well-known formula

$$(a \mid q) = a^{(q-1)/2} \pmod{q}. \hspace{1cm} (2)$$

**Theorem 1.** Let $G$ be the cyclic group of order $q$, where $q$ is an odd prime. Then $(a \mid G)$ coincides with the ordinary Legendre symbol $(a \mid q)$.

**Proof.** Define $k$ to be the order of $a$ modulo $q$, i.e., the smallest divisor of $q - 1$ satisfying $a^k = 1 \pmod{q}$. The permutation $\sigma_a$ consists of one fixed point and $(q - 1)/k$ cycles of length $k$. Hence $(a \mid G) = (-1)^{(q-1)/k}$. On the other hand, $(2)$ yields $(a \mid q) = 1$ if and only if $(q-1)/k$ is even. So $(a \mid G) = (a \mid q)$. \qed

For $a \in \mathbb{Z}$ let $(a)$ denote the residue class of $a$ modulo $m$, that is, $(a) = m\mathbb{Z} + a$. The set $A$ of classes $(a)$ with $a$ relatively prime to $m$ is an Abelian group, for the product $(a)(b) = (ab)$, and its order $|A|$ is the Euler function $\phi(m)$. The following result is immediate.

**Theorem 2.** The value of $(a \mid G)$ depends only on the class $(a) \in A$. On the other hand, $(ab \mid G) = (a \mid G)(b \mid G)$ holds.

For a given group $G$ let us define the subsets $A_0$ and $A_1$ of $A$ as follows: $A_i$ consists of the classes $(a)$ with $(a \mid G) = (-1)^i$. Since, by Theorem 2, the mapping $(a) \to (a \mid G)$ is a group homomorphism from $A$ into $\{1, -1\}$, there are two possibilities: either $A_0 = A$ and $A_1 = \emptyset$, or $A_0$ is a subgroup of index 2 of $A$. We shall see later on (Theorem 8) to which type of groups these two cases correspond.

**Example.** Let $G$ be the cyclic group of order $n = m = 63$. So $|A| = \phi(m) = 36$. 

Writing \( a \) instead of \((a)\) for convenience, one has

\[
A_n = \{1, 2, 4, 8, 11, 16, 22, 23, 25, 29, 32, 37, 43, 44, 46, 50, 53, 58\},
\]

and \( A_1 = -A_n \). This can be checked directly from the definitions. A simple method for computing the Legendre symbol and hence the sets \( A_i \) will be given in the sequel; see Theorems 3, 6 and 7.

We shall now find an expression for \((-1 \mid G)\). An involution of \( G \) by definition is an element of order 2. It is easily seen that the involutions together with the identity form an elementary Abelian 2-group of order \( 2^r \), where \( r \) is the number of factors in the decomposition of the Sylow 2-subgroup of \( G \) as a direct product of cyclic groups.

**Theorem 3.** Let \( n = |G| \) and let \( t = 2^r - 1 \) be the number of involutions of \( G \). Then

\[
(-1 \mid G) = (-1)^{t-1} \cdot 1^{1/2}
\]

**Proof.** It is clear that the cycle structure of \( \sigma_a \), consists of \( t+1 \) fixed points and \((n - t - 1)/2\) transpositions.

Let \( P_a \) denote the permutation matrix representing \( \sigma_a \), for a given group \( G \). Thus \( P_a \) is the square matrix of order \( n \), having \( G \) as row and column labelling set, defined by \( P_a(x, y) = 1 \) if \( x \cdot y \) according to whether \( x^a = y \) or \( x^a \neq y \) (see (1)). Then the Legendre symbol is equal to

\[
(a \mid G) = \det(P_a).
\]

We now give a result showing how, in certain cases, computation of the Legendre symbol can be decomposed into simpler problems.

**Theorem 4.** The Legendre symbol with respect to the direct product of two Abelian groups \( G \) and \( G' \) is given by

\[
(a \mid G \times G') = (a \mid G)^n (a \mid G')^n,
\]

where \( n = |G|, n' = |G'| \) and \( a \) is any integer relatively prime to \( nn' \).

**Proof.** Let \( P_a, P'_a \) and \( Q_a \) denote the permutation matrices representing the automorphism \( \sigma_a \), for the groups \( G, G' \) and \( G \times G' \), respectively. Clearly, \( Q_a = P_a \otimes P'_a \). Then (4) follows from (3), by the well-known formula for the determinant of a Kronecker product.

**Example.** Decomposing the cyclic group \( C_{63} \) as \( C_7 \times C_9 \) we deduce \((a \mid C_{63}) = (a \mid C_7)(a \mid C_9)\) from Theorem 4. Now \((a \mid C_9) = 1\) (see Theorem 8 below), whence \((a \mid C_{63}) = (a \mid 7)\), by Theorem 1, so that \((a \mid C_{63}) = 1\) holds if and only if \( a = 1, 2 \) or \( 4 \) (mod 7).
Remark. As a consequence of Theorems 1 and 4, it appears that \((a \mid G)\) coincides with the Jacobi symbol \((a \mid n)\) in the particular case of an Abelian group \(G\) of order \(n\) all Sylow subgroups of which are elementary.

3. Main theorems

Let \(p\) be an odd prime not dividing the period \(m\) of the Abelian group \(G\), and let \(k\) be the order of \(p\) modulo \(m\). An irreducible \(p\)-character of \(G\) is a homomorphic mapping from \(G\) into the multiplicative group of the Galois field \(GF(p^k)\). The set of all such characters is known to constitute a group isomorphic to \(G\) itself (see [2, p. 73]). Moreover, the characters \(\psi = \psi_x\) can be numbered by the elements \(x\) of \(G\) in such a way as to satisfy \(\psi_x(y) = \psi_y(x)\) for all \(x, y \in G\). For any integer \(a\) relatively prime to \(n\) let us define the square matrix \(S_a\) with \(G\) as row and column labelling set, over an extension field of \(GF(p^k)\) containing \(n^{1/2}\), by the formula

\[ S_a(x, y) = n^{-1/2} \psi_y(x^a), \quad x, y \in G. \]  

(5)

Lemma 5. For \((a)\) varying over \(A\) the matrices \(P_a\) and \(S_a\) together form a group of order \(2\phi(m)\), with the relations

\[ P_a P_b = P_{ab}, \quad P_a S_b = S_{ab}, \quad S_a P_b = S_{ab}^{-1}, \quad S_a S_b = P_{-ab}. \]

Proof. The first three identities are immediate. Then the orthogonality relation on group characters, written in the form \(S_a S_{-a} = I\), yields the fourth identity as a consequence of the third one. \(\square\)

In view of Theorems 3 and 4, computation of the Legendre symbol \((a \mid G)\) reduces to that of \((p \mid G)\) for the prime numbers \(p\). Theorems 6 and 7 below precisely indicate how to determine \((p \mid G)\); the results appear as generalizations of the “quadratic reciprocity law” and of the “quadratic character of two”, respectively.

Theorem 6. For an odd prime \(p\) not dividing \(n = |G|\), one has

\[ (p \mid G) = (1 \mid G)^{n-1/2} (n \mid p)^n. \]  

(6)

Proof. Let \(a\) and \(b\) be relatively prime to \(n\). Using (3) and Lemma 5 one obtains

\[ \det (S_{ab}) = (a \mid G) \det (S_b). \]  

(7)

On the other hand, Lemma 5 yields \(\det (S_b) \det (S_{-b}) = 1\). Hence from (7) with \(a = -1\) one deduces \((\det (S_b))^2 = (1 \mid G)\); so

\[ (\det (S_b))^p = (1 \mid G)^{n-1/2} \det (S_b). \]  

(8)
Next, observe that, in view of (5), the entries of the matrix \( n^{1/2}S_{pb} \) are the \( p \)th powers of those of \( n^{1/2}S_{b} \). Hence the following identity holds over a field of characteristic \( p \):

\[
\det(n^{1/2}S_{pb}) = (\det(n^{1/2}S_{b}))^p.
\]

(9)

Using (7) with \( a = p \) for the left member, and (8) for the right member, one can write in the form

\[
n^{m/2}(p \mid G) \det(S_{p}) = n^{m/2}(-1 \mid G)^{(p-1)/2} \det(S_{p}).
\]

This yields the desired result (6), since \( \det(S_{p}) \neq 0 \) and \( n^{(p-1)/2} = (n \mid p) \) over any field of characteristic \( p \) (see (2)).

**Theorem 7.** For a group \( G \) of odd order \( n \), one has

\[
(2 \mid G) = (-1)^{(n^2-1)/8}.
\]

(10)

**Proof.** Assume first \( n \equiv 1 \pmod{4} \). Define \( c = \frac{1}{2}(n + 1) \) and let \( c = p_1p_2\cdots p_s \) be its canonical decomposition as the product of (odd) primes \( p_i \). By Theorem 2 one has

\[
(2 \mid G) = (c \mid G) = \prod(p_i \mid G).
\]

Hence, applying Theorem 6 and observing that \( n = 1 \pmod{p_i} \) holds for each \( i \), one easily obtains

\[
(2 \mid G) = \prod_{i=1}^{s} (n \mid p_i) = \prod_{i=1}^{s} (-1)^{(p_i-1)/2}.
\]

(11)

by use of (2). When \( c \equiv 1 \pmod{4} \) there is an even number of factors \( p_i \equiv -1 \pmod{4} \), so that (11) yields \( (2 \mid G) = 1 \). Analogously, \( (2 \mid G) = -1 \) when \( c \equiv -1 \pmod{4} \).

The case \( n \equiv -1 \pmod{4} \) can be treated by a similar method. It suffices to replace \( c \) by \( \frac{1}{2}(n - 1) \) in the above argument. The result turns out to be \( (2 \mid G) = \pm 1 \) for \( \frac{1}{2}(n - 1) \equiv \pm 1 \pmod{4} \); the details are left to the reader. Thus one has shown \( (2 \mid G) = 1 \) for \( n \equiv \pm 1 \pmod{8} \) and \( (2 \mid G) = -1 \) for \( n \equiv \pm 3 \pmod{8} \), which is equivalent to (10). □

**Theorem 8.** An Abelian group \( G \) of order \( n \) satisfies \((a \mid G) = 1\) for all \( a \) if and only if one of the following three conditions holds.

(i) \( n \equiv 0 \pmod{4} \) and \( G \) contains more than one involution.
(ii) \( n \equiv 2 \pmod{4} \).
(iii) \( n \) is the square of an odd integer.

**Proof.** The "if" proposition is easily proved by use of Theorems 3, 6 and 7. Let us now assume \((a \mid G) = 1\) for all \( a \). When \( n \) is even, the condition \((-1 \mid G) = 1\) yields \( n - 1 - t \equiv 0 \pmod{4} \), i.e., \( n \equiv 0 \pmod{4} \) and \( t = 2r - 1 \) with \( r \geq 2 \), or \( n \equiv 2 \pmod{4} \) and \( t = 1 \). When \( n \) is odd, \((-1 \mid G) \equiv (p \mid G) = 1\) implies \((n \mid p) = 1\).
for every odd prime $p$ not dividing $n$, as a consequence of Theorem 6. If $n$ is not a square, let us write $n = b^2 q_1 q_2 \cdots q_s$ where $b$ is an integer and the $q_i$'s are distinct primes. Owing to the quadratic reciprocity law, $(n \mid p) = 1$ can be written as
\[
\prod_{i=1}^{s} (p \mid q_i) (-1)^{(p-1)(q_i-1)/4} = 1. \tag{12}
\]
Let $c$ be any integer such that $(c \mid q_i) = -1$ holds. By Dirichlet's theorem [1, p. 13] there exists a prime $p$ satisfying $p \equiv 1 \pmod{4}$, $p \equiv c \pmod{q_i}$ and $p \equiv 1 \pmod{q_i}$ for $i = 2, \ldots, s$. For such a prime the left member of (12) equals $-1$. This contradiction shows that $n$ must be a square. \qed

Acknowledgment

The author is grateful to a referee for useful remarks.

References