AN EXPRESSION FOR THE LEGENDRE SYMBOL FROM A PRODUCT-SUM FORMULA

B. Sury
Statistics and Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore, India.
surybang@gmail.com

Received: 11/30/21, Revised: 1/22/22, Accepted: 2/22/22, Published: 2/28/22

Abstract

The fact that quadratic number fields are cyclotomic is elementary to prove. Using the idea of its proof, we obtain a product-sum formula which yields an interesting expression for the Legendre symbol.

1. Introduction

It is well known that for quadratic number fields, the assertion of the Kronecker-Weber theorem is elementary to prove. In fact, one can give a 'one-sentence' proof of it. Following up on this idea, we observe in this note a product-sum relation that emanates by comparison with Gauss sums. It is an intriguing question whether the product-sum relation can be viewed as an instance or as an analogue of the Weyl character formula. Using the product-sum formula, we obtain an explicit expression for any Legendre symbol in terms of roots of unity. This is reminiscent of an expression in terms of trigonometric functions due to Eisenstein, but does not appear to be the same.

2. A Product-Sum Identity

The fact that quadratic fields are cyclotomic is elementary to prove, but we recall a proof here as we need that idea. The proof can be stated as a single sentence but we break it into parts for ease of communication. Let $\zeta_n = e^{2i\pi/n}$ for any positive integer n. Observe that $\prod_{r=1}^{n-1}(1-\zeta_n^r) = n$. As a consequence, we obtain

$$(-1)^{\binom{n}{2}} \prod_{0\le l<k\le n-1} (\zeta_n^l - \zeta_n^k)^2 = \prod_{l\ne k} (\zeta_n^l - \zeta_n^k)$$

$$= \prod_l \zeta_n^l \prod_{k \neq l} (1 - \zeta_n^{k-l}) = \prod_l (n\zeta_n^l) = n^n \zeta_n^{\binom{n}{2}} = n^n$$

for odd n. Combining this with the evident equality $\sqrt{2} = e^{2i\pi/8} + e^{-2i\pi/8}$, it follows that for any positive integer m, $\sqrt{m}$ and $\sqrt{-m}$ are both expressible as polynomials in ζ_N with integer coefficients. Here $N = 8\prod_{i=1}^{r} p_i$, where the p_i's are the odd prime factors of m.

For an odd prime p, the above proof yields

$$(-1)^{(p-1)/2} p^p = \prod_{0 \leq s < r < p} (\zeta_p^r - \zeta_p^s)^2,$$

with $\zeta_p = e^{2i\pi/p}$. Thus, the left-hand side is p^p or $-p^p$ according as to whether $p \equiv 1$ or 3 mod 4. Therefore, we note that $\prod_{0 \leq s < r < p} (\zeta_p^r - \zeta_p^s) = \pm p^{p/2}$ or $\pm i p^{p/2}$ according as to whether $p \equiv 1$ or 3 mod 4.

On the other hand, it is well known that the Gauss sum $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a = \sqrt{p}$ or $i\sqrt{p}$ according as to whether $p \equiv 1$ or 3 mod 4. Here $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Therefore, up to sign, $\prod_{0 \leq s < r < p} (\zeta_p^r - \zeta_p^s)$ and $p^{\frac{p-1}{2}} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$ are equal. We prove more precisely the following product-sum formula.

Theorem 1. *Let $\zeta_p = e^{2i\pi/p}$. Then,*

$$\prod_{0 \leq s < r < p} (\zeta_p^r - \zeta_p^s) = (-1)^{\frac{p^2-1}{8}} p^{\frac{p-1}{2}} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a.$$

It should be borne in mind that the sign in the identity depends on the choice of the primitive p-th root of unity.

The product-sum identity seems tantalizingly close to an instance of the Weyl character formula recalled below, but we do not know if it can be so viewed:

$$\chi_\lambda(T) \prod_{\alpha > 0} (e^{\alpha(T)/2} - e^{-\alpha(T)/2}) = \sum_{w \in W} sgn(w) e^{\lambda + \rho}(wT)$$

where χ_λ is the character of an irreducible representation of a compact connected Lie group, with highest weight λ, the sum runs over the positive roots, ρ is one-half the sum of positive roots and T is in the Lie algebra of a maximal torus.

3. An Expression for the Legendre Symbol

Before proving the theorem, we first deduce from it an expression for the Legendre symbol.

Corollary 1. *For an odd prime p, and $(b,p)=1$, writing $\zeta_p = e^{2i\pi/p}$, we have the expression*

$$\left(\frac{b}{p}\right) = \zeta_p^{\binom{p}{3}(b-1)} \prod_{t=1}^{p-2} \left(\prod_{k=1}^{t} \frac{\zeta_p^{-k}-1}{\zeta_p^{-kb}-1} \right).$$

The proof follows immediately from the theorem by looking at the effect of the transformation $\zeta_p \mapsto \zeta_p^b$ for $(b,p)=1$ which multiplies its right-hand side by $\left(\frac{b}{p}\right)$. This proves the corollary.

The expression in the corollary is reminiscent of an expression in terms of trigonometric functions due to Eisenstein but does not appear to be the same.

4. Proof of the Product-Sum Identity

The proof of Theorem 1 requires us to determine the sign of the left-hand side of the statement. We accomplish this by closely following a matrix calculation attributed to Schur that determines the sign of the Gauss sum ([1], pp. 207-212).

Proof. We will show that $\prod_{0\le l<k<p}(e^{2i\pi k/p} - e^{2i\pi l/p}) = i^{p(p-1)/2}p^{p/2}$, and also simultaneously show that the Gauss sum $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$ equals $\sqrt{p}$ or $i\sqrt{p}$ according as to whether $p \equiv 1$ or $3 \bmod 4$. Note that this would imply the product-sum formula. As mentioned earlier, the idea is due to Schur.

Write $\zeta_p = e^{2i\pi/p}$. Consider the $p \times p$ matrix $A = (\zeta_p^{kl})_{0\le k,l<p}$. Note that

$$tr(A) = \sum_{s=0}^{p-1} \zeta_p^{s^2}$$

and

$$det(A) = \prod_{0\le l<k<p} (e^{2i\pi k/p} - e^{2i\pi l/p}).$$

The right-hand side here is the left-hand side of the asserted product-sum formula.

We first observe that the Gauss sum $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$ can also be written as the sum $S := \sum_{s=0}^{p-1} e^{2i\pi s^2/p}$. Hence, the Gauss sum

$$S = \sum_{s=0}^{p-1} \zeta_p^{s^2} = tr(A) = \sum_{r=1}^{p} \lambda_r,$$

where $\lambda_1, \cdots, \lambda_p$ are the eigenvalues of A. Now,

$$(A^2)_{u,v} = \sum_{w} \zeta_p^{(u+v)w} = b_{u+v},$$

where $b_m = \sum_w \zeta_p^{mw}$. Multiplying by ζ_p^m, we see that $b_m = p$ or 0 according as to whether $p|m$ or not. Note that

$$\sum_r \lambda_r^2 = tr(A^2) = \sum_u b_{2u} = p.$$

Also,

$$(A^4)_{uv} = \sum_w b_{u+w} b_{w+v} = p^2 \quad or \quad 0$$

according as to whether $u = v$ or not. Thus $A^4 = p^2 I$ where I is the $p \times p$ identity matrix. The characteristic polynomial $\chi_{A^4}(\lambda)$ of A^4 is $(\lambda - p^2)^p$ which means that the eigenvalues $\lambda_1^4, \cdots, \lambda_p^4$ are all equal to p^2. In particular, $\lambda_r = i^{a_r}\sqrt{p}$ where $a_r = 0, 1, 2$ or 3. For $k = 0, 1, 2, 3$ let

$$m_k = |\{a_r : a_r = k\}|.$$

Note that $m_0 + m_1 + m_2 + m_3 = p$. The Gauss sum S equals

$$\sum_r \lambda_r = \sum_r i^{a_r}\sqrt{p} = \sqrt{p}(m_0 + im_1 - m_2 - im_3)$$

and $|S|^2 = p$. We have $(m_0 - m_2)^2 + (m_1 - m_3)^2 = 1$. In other words, either $m_0 - m_2 = \pm 1$ and $m_1 = m_3$ or $m_0 = m_2$ and $m_1 - m_3 = \pm 1$. Hence $S = v\eta\sqrt{p}$ where $v = \pm 1$ and $\eta = 1$ or i. Thus, we obtain the equation

$$m_0 + im_1 - m_2 - im_3 = v\eta.$$

Taking conjugates and noting $\bar{\eta} = \eta - 1$, we have the equation

$$m_0 - im_1 - m_2 + im_3 = v\eta^{-1}.$$

Also, the equality $tr(A^2) = \sum_r \lambda_r^2 = p$ observed earlier, gives us the equation

$$m_0 - m_1 + m_2 - m_3 = 1.$$

Thus, the system of 4 linear equations can be written as a matrix equation $Bx = y$ where $B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$, $x = \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \end{pmatrix}$ and $y = \begin{pmatrix} p \\ v\eta \\ 1 \\ v\eta^{-1} \end{pmatrix}$. Inverting this matrix, we get $x = B^{-1}y$ with $B^{-1} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}$.

In particular, since $m_2 = \frac{p+1-v(\eta+\eta^{-1})}{4}$ is an integer, we have that $\eta = 1$ or i according as to whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. Further,

$$det(A) = \prod_r \lambda_r = p^{p/2} i^{m_1 + 2m_2 - m_3} = p^{p/2} i^{3(p-1)/2} v = p^{p/2} i^{p(p-1)/2} v.$$

To obtain this, we have substituted the value of $m_1 + 2m_2 - m_3$ gotten from $x = B^{-1}y$, namely, $m_1 + 2m_2 - m_3 = \frac{p+1}{2} - v$ or $\frac{p+1}{2} + v$ according as to whether $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. We have also written iv instead of i^v (as we may) above. Finally, we show that $v = 1$ as follows which will prove both the sign of trA) and of $det(A)$, thereby, determining the sign of the Gauss sum also, and proving our product-sum formula. To show $v = 1$, observe that

$$det(A) = \prod_{0 \le l < k < p} (e^{2i\pi k/p} - e^{2i\pi l/p}) = \prod_{l<k} e^{i\pi(k+l)/p}(e^{i\pi(k-l)/p} - e^{i\pi(l-k)/p}).$$

As $\sum_{0 \le l < k < p}(k + l) = p(p-1)^2/2$, we have

$$\prod_{l<k} e^{i\pi(k+l)/p} = e^{i\pi(p-1)^2/2} = i^{(p-1)^2} = 1.$$

Hence

$$\begin{aligned} det(A) &= \prod_{l<k}(e^{i\pi(k-l)/p} - e^{i\pi(l-k)/p}) \\ &= \prod_{l<k}(2i \sin \frac{\pi(k-l)}{p}) = i^{p(p-1)/2} \prod_{l<k}(2 \sin \frac{\pi(k-l)}{p}). \end{aligned}$$

As the last mentioned product is positive, the two expressions

$$det(A) = p^{p/2} i^{p(p-1)/2} v = i^{p(p-1)/2} \prod_{l<k}(2 \sin \frac{\pi(k-l)}{p})$$

imply that $v > 0$ and is, therefore, equal to 1. This completes the proof that $det(A) = p^{p/2} i^{p(p-1)/2}$, and hence, the main theorem is proved. □

Acknowledgment. It is a pleasure to thank the referee for some constructive suggestions that improved the exposition.

References

[1] E. Landau, *Elementary Number Theory, Translated by Jacob E. Goodman*, Chelsea Publishing Company, New York, 1958.