ZOLOTAREV’S THEOREM ON THE LEGENDRE SYMBOL

J. L. BRENNER
ZOLOTAREV'S THEOREM ON THE LEGENDRE SYMBOL

J. L. BRENNER

Dedicated to Professor D. H. Lehmer

Matrix-theoretic proof that \((a/p) = \text{sign of the permutation} \ i \mod p \rightarrow ia \mod p\) of the residue classes \(\mod p\).

In [5], Zolotarev proved the quadratic reciprocity law on the basis of the above-stated result. Here is a short proof of that result; it uses matrix theory, together with a well-known result in number theory.

DEFINITION 1. An \(a\)-circulant is an \(n \times n\) matrix such that each row (except the first) is obtained from the preceding by shifting each element \(a\) positions to the right.

DEFINITION 2. \(P = (p_{ij})\) denotes the \(n \times n\) permutation matrix that corresponds to the permutation \(i \rightarrow i + 1 \mod n\), i.e., \(p_{ij} = 1\) if \(j = i \mod n\), \(p_{ij} = 0\) otherwise.

Note that \(P^a\), the \(a\)th power of \(P\), is an \(a\)-circulant.

DEFINITION 3. \(A(a)\) denotes the \(a\)-circulant, the first row of which has 1 in the \(a\)th column and zeros elsewhere.

Note that \(PA(a) = A(a)P^a\).

THEOREM 4. \(\det A(a) = \text{sign of the permutation} \ i \mod n \rightarrow ia \mod n\).

This follows from one of the usual definitions of the determinant function.

LEMMA 5. If the first row of \(A(a_i)\) is multiplied by the matrix \(A(a_2)\), the product is: the row that has all zeros except for 1 in the position \(a_ia_2 \mod n\). [Obvious.]

THEOREM 6. The product of an \(a_i\)-circulant by an \(a_2\)-circulant is an \(a_ia_2\)-circulant.

Proof. \(PA(a_i)A(a_2) = A(a_i)A(a_2)P^e\), \(e = a_ia_2\).

COROLLARY 7. \(A(a_i)A(a_2) = A(a_ia_2)\);

\[\det A(a_i) \det A(a_2) = \det A(a_ia_2).\]

COROLLARY 8. For \((a, n) = 1\), the determinant of the set \(\{A(a)\}\) is a character \(\mod n\).
**LEMMA 9.** If \( a = g \) is a primitive root of the odd prime number \( p = n \), then \( \det A(g) = -1 \).

*Proof.* The corresponding permutation is an \((n - 1)\)-cycle; its sign is \(-1\).

**THEOREM 10.** If \( n \) is an odd prime \( p \), then \( \det A(a) = (a/p) \), the Legendre symbol.

*Proof.* The Legendre symbol is the only real character modulo a prime that actually assumes the value \(-1\).

**COROLLARY 11.** [Zolotarev]. \( (a/p) = \text{sign of the permutation} \)

\[ i \pmod{p} \longrightarrow ia \pmod{p}, \text{where } p \text{ is a prime}. \]

*Remark.* The result \( \det A(a) = (a/n) \) does hold in general [4]. When \( n \) is an odd prime power, this is obvious since \( n \) has a primitive root. For other odd \( n \), it seems less obvious. See [2, 3] for proof.

**Concluding remark.** As Zolotarev showed, the argument of this article furnishes yet another proof, and the first matrix-theoretic one, of the quadratic reciprocity law.

**Acknowledgment.** I thank Professor D. H. Lehmer for asking whether the methods developed in [1] could be used to prove that \( \det A(a) = (a/p) \).

**REFERENCES**


Received February 2, 1972. Supported by NSF Grant GP-32527.

UNIVERSITY OF VICTORIA, CANADA

AND

COLLEGE OF NOTRE DAME, BELMONT, CALIFORNIA
PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON
Stanford University
Stanford, California 94305

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

C. R. HOBBY
University of Washington
Seattle, Washington 98105

RICHARD ARENS
University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH
B. H. NEUMANN
F. WOLF
K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
UNIVERSITY OF SOUTHERN CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
STANFORD UNIVERSITY
UNIVERSITY OF CALIFORNIA
UNIVERSITY OF TOKYO
MONTANA STATE UNIVERSITY
UNIVERSITY OF UTAH
UNIVERSITY OF NEVADA
WASHINGTON STATE UNIVERSITY
NEW MEXICO STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
OREGON STATE UNIVERSITY
*
*
*
UNIVERSITY OF OREGON
AMERICAN MATHEMATICAL SOCIETY
OSAKA UNIVERSITY
NAVAL WEAPONS CENTER

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the Pacific Journal of Mathematics should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. 39. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is issued monthly as of January 1966. Regular subscription rate: $48.00 a year (6 Vols., 12 issues). Special rate: $24.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Kenneth Paul Baclawski and Kenneth Kapp, *Induced topologies for quasigroups and loops*. 393

D. G. Bourgin, *Fixed point and min – max theorems*. 403

J. L. Brenner, *Zolotarev’s theorem on the Legendre symbol*. 413

Jospeh Atkins Childress, Jr., *Restricting isotopies of spheres*. 415

John Edward Coury, *Some results on lacunary Walsh series*. 419

James B. Derr and N. P. Mukherjee, *Generalized Sylow tower groups. II*. 427

Paul Frazier Duvall, Jr., Peter Fletcher and Robert Allen McCoy, *Isotopy Galois spaces*. 435

Mary Rodriguez Embry, *Strictly cyclic operator algebras on a Banach space*. 443

Abi (Abiadbollah) Fattahi, *On generalizations of Sylow tower groups*. 453

Burton I. Fein and Murray M. Schacher, *Maximal subfields of tensor products*. 479

Ervin Fried and J. Sichler, *Homomorphisms of commutative rings with unit element*. 485

Kenneth R. Goodearl, *Essential products of nonsingular rings*. 493

George Grätzer, Bjarni Jónsson and H. Lakser, *The amalgamation property in equational classes of modular lattices*. 507

H. Groemer, *On some mean values associated with a randomly selected simplex in a convex set*. 525

Marcel Herzog, *Central 2-Sylow intersections*. 535

Joel Saul Hillel, *On the number of type-k translation-invariant groups*. 539

Ronald Brian Kirk, *A note on the Mackey topology for \((C^b(X)^*, C^b(X))\)*. 543

J. W. Lea, *The peripherality of irreducible elements of lattice*. 555

John Stewart Locker, *Self-adjointness for multi-point differential operators*. 561

Robert Patrick Martineau, *Splitting of group representations*. 571

Robert Massagli, *On a new radical in a topological ring*. 577


Fred Richman, *The constructive theory of countable abelian p-groups*. 621

Edward Barry Saff and J. L. Walsh, *On the convergence of rational functions which interpolate in the roots of unity*. 639

Harold Eugene Schlais, *Non-aposyndesis and non-hereditary decomposability*. 643

Mark Lawrence Teply, *A class of divisible modules*. 653

Edward Joseph Tully, Jr., \(\mathfrak{H}\)-commutative semigroups in which each homomorphism is uniquely determined by its kernel*. 669

Garth William Warner, Jr., *Zeta functions on the real general linear group*. 681

Keith Yale, *Cocycles with range \(\{±1\}\)*. 693

Chi-Lin Yen, *On the rest points of a nonlinear nonexpansive semigroup*. 699