EXTERIOR ALGEBRAS AND THE QUADRATIC RECIPROCITY LAW

Autor(en): **Rousseau, G.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **36 (1990)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-57910

L'Enseignement Mathématique, t. 36 (1990), p. 303-308

EXTERIOR ALGEBRAS AND THE QUADRATIC RECIPROCITY LAW

by G. Rousseau

Abstract. As is known, the theory of exterior algebras can be used to derive the properties of determinants and of the signature of permutations (cf. Chevalley, "Fundamental Concepts of Algebra", N.Y., 1956). We show that the properties of the Jacobi symbol, including reciprocity, can also be derived easily from this source.

In this note we consider the connection between a certain identity for exterior algebras and the quadratic reciprocity law.

It is easily shown that if M is a module then, in the exterior algebra of M,

$$\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{n} a_{i,j} = (-1)^{\binom{m}{2}\binom{n}{2}} \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{m} a_{i,j} \tag{1}$$

for all $a_{i,j} \in M$. However it is also easily shown that this identity is equivalent, in case m and n are odd and relatively prime, to the reciprocity law for the Jacobi symbol

$$(n \mid m) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} (m \mid n) . \tag{2}$$

This provides a very simple and transparent treatment of quadratic reciprocity. Apart from the formulation in terms of exterior algebras, which though convenient is not essential, this approach is substantially that of Zolotarev (cf. [9], [1], [7]). It is curious that it is so little known considering the attention given in the literature to Zolotarev's Theorem (which appears in [9] as a preliminary to the proof of the reciprocity law).

After definitions and preliminaries in 1, we prove (1), and the equivalence of (1) and (2), in 2. Other formulas such as the two supplementary laws and the second multiplicativity formula are considered briefly in 3, together with

Zolotarev's Theorem. Finally in 4 we show how the main propositions can be formulated in terms of operations on ordered sets rather than in the framework of exterior algebras.

1. The exterior algebra $\Lambda(M)$ of a module M (see, for example, [6]) satisfies the skew-commutative property $a \wedge b = -b \wedge a$ $(a, b \in M)$. It follows that for any permutation σ of $1, 2, \ldots, m$,

$$\Lambda_{i=1}^{m} a_{\sigma(i)} = \operatorname{sgn}(\sigma) \Lambda_{i=1}^{m} a_i .$$

If a_i $(i = 1, \ldots, m)$ and b_j $(j = 1, \ldots, n)$ are module elements then

$$\Lambda_{i=1}^{m} a_i \wedge \Lambda_{j=1}^{n} b_j = (-1)^{mn} \Lambda_{j=1}^{n} b_j \wedge \Lambda_{i=1}^{m} a_i . \tag{3}$$

Also it is clear that

$$\text{if} \quad \Lambda_{i=1}^{m} \Lambda_{j=1}^{n} a_{i,j} = \Lambda_{i=1}^{m} \Lambda_{j=1}^{n} b_{i,j} \text{ then } \Lambda_{j=1}^{n} \Lambda_{i=1}^{m} a_{i,j} = \Lambda_{j=1}^{n} \Lambda_{i=1}^{m} b_{i,j} ,$$

while

$$\text{if} \quad \Lambda_{i=1}^{m} \Lambda_{j=1}^{n} a_{i,j} = \Lambda_{j=1}^{n} \Lambda_{i=1}^{m} b_{i,j} \text{ then } \Lambda_{j=1}^{n} \Lambda_{i=1}^{m} a_{i,j} = \Lambda_{i=1}^{m} \Lambda_{j=1}^{n} b_{i,j} .$$

In the first case, in passing from the antecedent equation to the consequent equation the permutation undergone by the elements on the left is equal to that undergone by the elements on the right; in the second case it is inverse.

The Jacobi symbol may be defined independently of the notion of quadratic residue as follows ([9], [5], [3]). If n is an integer which is relatively prime to the odd positive integer m, then the mapping

$$\pi_{nm}(i) = ni \bmod m \qquad (i = 0, 1, 2, \ldots, m-1)$$

is a permutation of the set $\{0, 1, 2, \ldots, m-1\}$; we define the symbol $(n|m)$ to be the signature of this permutation,

$$(n|m) = \operatorname{sgn}(\pi_{nm}) . \tag{4}$$

It follows from the definition that

$$\text{if} \quad n \equiv n' \pmod{m} \quad \text{then} \quad (n|m) = (n'|m) . \tag{5}$$

Also, since $\pi_{nn'm} = \pi_{nm} \pi_{n'm}$, we have

$$(nn'|m) = (n|m)\,(n'|m) . \tag{6}$$

Using (3) and the fact that m is odd, we see that since the permutation $i \to i + r \bmod m$ interchanges the first r of the numbers $0, 1, \ldots, m-1$ with the last $m - r$ it has signature $(-1)^{r(m-r)} = 1$. It follows that each linear permutation $i \to ni + r \bmod m$ has signature $(n|m)$.

2. To prove that (1) and (2) are equivalent when m and n are odd and relatively prime, we consider permutations μ_j and ν_i defined by

$$\mu_j(i) = ni + j \bmod m \quad (i = 0, \ldots, m-1; j = 0, \ldots, n-1),$$
$$\nu_i(j) = i + mj \bmod n \quad (j = 0, \ldots, n-1; i = 0, \ldots, m-1).$$

We have

$$\bigwedge_{i=0}^{m-1} \bigwedge_{j=0}^{n-1} a_{\mu_j(i),j} = \bigwedge_{j=0}^{n-1} \bigwedge_{i=0}^{m-1} a_{i,\nu_i(j)}$$

because both sides are equal to $\bigwedge_{k=0}^{mn-1} a_{k \bmod m, k \bmod n}$. It follows that

$$\bigwedge_{j=0}^{n-1} \bigwedge_{i=0}^{m-1} a_{\mu_j(i),j} = \bigwedge_{i=0}^{m-1} \bigwedge_{j=0}^{n-1} a_{i,\nu_i(j)}.$$

The left side is

$$\bigwedge_{j=0}^{n-1} (n|m) \bigwedge_{i=0}^{m-1} a_{i,j} = (n|m)^n \bigwedge_{j=0}^{n-1} \bigwedge_{i=0}^{m-1} a_{i,j},$$

while the right side is

$$\bigwedge_{i=0}^{m-1} (m|n) \bigwedge_{j=0}^{n-1} a_{i,j} = (m|n)^m \bigwedge_{i=0}^{m-1} \bigwedge_{j=0}^{n-1} a_{i,j}.$$

Thus

$$(n|m)^n \bigwedge_{j=0}^{n-1} \bigwedge_{i=0}^{m-1} a_{i,j} = (m|n)^m \bigwedge_{i=0}^{m-1} \bigwedge_{j=0}^{n-1} a_{i,j}.$$

From this it is clear that (2) implies (1), and the converse implication is obtained if the $a_{i,j}$ are taken to be basis elements of a free module.

Formula (1) may easily be proved by induction using (3), or even more simply by observing that the permutation which transforms the pairs (i, j) from lexicographic (row) order to dual-lexicographic (column) order inverts the order in which (i, j) and (i', j') appear just when both

(i) $i < i'$ or $(i = i'$ and $j < j')$, and

(ii) $j > j'$ or $(j = j'$ and $i > i')$;

since this condition is equivalent to $i < i'$ and $j > j'$, the number of inversions is $\binom{m}{2}\binom{n}{2}$, as required.

3. The permutation π_{-1m} leaves 0 fixed and transforms the numbers $1, \ldots, m-1$ to reverse order, so in view of the evident formula

(7) $$\bigwedge_{i=1}^{n} a_i = (-1)^{\binom{n}{2}} \bigwedge_{i=n}^{1} a_i$$

we have (on putting $n = m - 1$) the first supplementary law,

$$(8) \qquad (-1|m) = (-1)^{\frac{m-1}{2}} .$$

As is well known, formulas (2), (5), (6) and (8) suffice for the calculation of the Jacobi symbol, and the other standard properties can be deduced easily from them (cf. [3], [2]). However they may also be proved directly by the present methods by suitably adapting the arguments in [2] and [4]. One can also readily establish by the present methods Schur's generalisation of the Zolotarev-Frobenius-Lerch Theorem, according to which, for odd m, a k-dimensional integral linear transformation A, considered as a transformation of the k-tuples of residues modulo m, has signature $(\det(A)|m)$ (cf. [8], [4], [2]).

In 1 we defined the Jacobi symbol independently of the notion of quadratic residue. The crucial connection is established by Zolotarev's Theorem [9]:

$$(9) \qquad nRp \quad \text{iff} \quad (n|p) = 1 \qquad (2 \nmid p \nmid n) .$$

To prove this we may use the formula

$$(n|p) = \operatorname{sgn}(\pi_{np}) = \prod\nolimits_{i>i'} \frac{\pi_{np}(i) - \pi_{np}(i')}{i - i'} .$$

Calculating modulo p, we have

$$(n|p) \equiv \prod\nolimits_{i>i'} (ni - ni')/(i - i') = \prod\nolimits_{i>i'} n$$
$$= n^{p(p-1)/2} \equiv n^{(p-1)/2} \pmod{p} ,$$

and so (9) follows by Euler's criterion.

4. We have seen that the theory of quadratic residues may be deduced from three propositions of exterior algebra, namely (1), (3) and (7). These essentially combinatorial propositions may also be formulated in terms of ordered sets.

If E and F are linearly ordered sets (supposed disjoint) then as is known there are two sums, $E + F$ and $F + E$, defined on the union, and two products, $E . F$ and $F . E$, defined on the Cartesian product; also one considers the dual or opposite, E^*, defined on the same base set as E. If E and F are finite then $E + F \cong F + E$, $E . F \cong F . E$ and $E^* \cong E$, but in each case one may ask what is the signature of the (uniquely determined) isomorphism, considered as a permutation of the base set. The answers are contained in the following three propositions, which correspond to (7), (3) and (1) respectively.

PROPOSITION 1. *If E is a linearly ordered set with m elements, where m is an arbitrary positive integer, then the permutation of E which transforms the elements to reverse order has signature $(-1)^{\binom{m}{2}}$.*

PROPOSITION 2. *If E and F are disjoint linearly ordered sets with m and n elements respectively, where m and n are arbitrary positive integers, then the permutation of $E \cup F$ which transforms the elements from the order in which all elements of E precede all elements of F to the order in which all elements of F precede all elements of E has signature $(-1)^{mn}$.*

PROPOSITION 3. *If E and F are linearly ordered sets with m and n elements respectively, where m and n are arbitrary positive integers, then the permutation of $E \times F$ which transforms the elements from lexicographic (row) order to dual-lexicographic (column) order has signature $(-1)^{\binom{m}{2}\binom{n}{2}}$.*

The simplest method of proof in each case is to count the number of inversions. From the foregoing we see that Proposition 1 is substantially the first supplementary law, Proposition 2 plays a certain auxiliary role in regard to the definition of the Jacobi symbol, and Proposition 3 may be viewed as comprising the combinatorial kernel of the reciprocity law.

REFERENCES

[1] BACHMANN, P. *Niedere Zahlentheorie* I. Teubner, Leipzig, 1902, reprinted Chelsea, New York, 1968.

[2] CARTIER, P. Sur une généralisation des symboles de Legendre-Jacobi. *L'Ens. Math. 16* (1970), 31-48.

[3] FROBENIUS, F.G. Über das quadratische Reziprozitätsgesetz I. *Sitzungsber. Akad. Wiss. Berlin* (1914), 335-349.

[4] LEHMER, D.H. The characters of linear permutations. *Lin. and Multilin. Alg. 4* (1976), 1-16.

[5] LERCH, M. Sur un théorème arithmétique de Zolotarev. *Česka Akad., Prague, Bull. Int. Cl. Math. 3* (1986), 34-37.

[6] MAC LANE, S. and G. BIRKHOFF. *Algebra,* Macmillan, 1967.
[7] ROUSSEAU, G. On the Jacobi symbol. (In preparation.)
[8] SCHUR, I. Über die Gaußschen Summen. *Nachrichten K. Gesell. Wiss. Göttingen, math.-phys. Kl.* (1921), 147-153.
[9] ZOLOTAREV, G. Nouvelle démonstration de la loi de réciprocité de Legendre. *Nouv. Ann. de Math. (2) 11* (1872), 354-362.

(Reçu le 8 décembre 1989)

G. Rousseau
The University
Leicester, LE1 7RH
(England)