J. Austral. Math. Soc. (Series A) 25 (1978), 503–506

FROM CYCLIC ALGEBRAS OF QUADRATIC FIELDS TO CENTRAL POLYNOMIALS

OLGA TAUSSKY

To K. Mahler on his 75th birthday

(Received 27 December 1977)

Communicated by J. H. Coates

Abstract

A link between norms from quadratic fields and $-\det(AB-BA)$ for 2×2 matrices is reformulated via central polynomials and thereby generalized.

Subject classification (*Amer. Math. Soc.* (*MOS*) 1970): 12 A 99, 15 A 15, A 36.

This paper is concerned with three elaborations, I, II, III, of a theorem found earlier by this author (1974). It concerns the following fact.

(1) *Let* $A=(a_{ik})$ *be a* 2×2 *matrix with integral* (*or rational*) *elements and irrational characteristic root* α *and* $B=(b_{ik})$ *any integral* 2×2 *matrix then*

$$-\det(AB-BA)=\operatorname{norm}\lambda$$

where $\lambda\in Q(\alpha)$.

An earlier result (Taussky (1962)) is connected with this.

(2) *Let* $A=(a_{ik})$ *be a matrix as in* (1) *and S an integral matrix such that*

$$S^{-1}AS=A' \quad \text{(the transpose)}$$

then

$$-\det S=\operatorname{norm}\mu$$

where $\mu\in Q(\alpha)$.

I.

THEOREM 1. (1) *follows from* (2).

Assume $\operatorname{tr} A = 0$. This is no restriction when studying $AB-BA$. In Taussky (1976) it is shown that for A with irrational characteristic roots the commutator $C = AB-BA$ is 0 or non-singular. This follows by an easy computation via the companion matrix of C.

Assuming A in companion matrix form $\begin{pmatrix} 0 & 1 \\ -\det A & 0 \end{pmatrix}$ it follows that

$$C^{-1}AC = -A.$$

Apply then a similarity via $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ to both sides of this equation and obtain

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} C^{-1}AC \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = A'.$$

Hence $\det C\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \det C$ is a negative norm from $Q(\alpha)$ in virtue of (2).

II. Discussion of one of the proofs of (1)

A number of proofs were suggested. One of the treatments by Zassenhaus (1977) uses cyclic algebras. A version of this is used here. It is linked with a proof by Kisilevsky and this author; see Taussky (1976).

A cyclic algebra is determined by a cyclic extension of the ground field of degree, say n, with automorphism σ. The algebra has as basis elements the basis of the cyclic field and a set of elements corresponding to the powers of σ. The element corresponding to σ^n is contained in the ground field. Associativity follows then.

The algebra is isomorphic with the full ring of $n \times n$ matrices if and only if the element corresponding to σ^n is a norm from the cyclic extension. This algebra contains the four linearly independent elements I, A, B, $AB-BA$ under our assumptions as long as $AB-BA \neq 0$. Hence, by the theorem characterizing cyclic algebras which form the whole matrix algebra we have $(AB-BA)^2$ equal to a norm from $Q(\alpha)$ times I. But, by the central polynomial property of $(AB-BA)^2$ it is a scalar matrix, namely the scalar matrix $-\det(AB-BA)I$.

III. Link with the central polynomial

The fact that the case $n = 2$ is connected with the central polynomial for $n = 2$ suggested the idea of generalizing (1) via the higher dimensional central polynomials.

The polynomials found by Formanek (1972) particularly stressed the case of a pair of matrices A, B, where A is in diagonal form. Hence, again, as in (1), A is assumed integral and with irreducible characteristic polynomial and characteristic roots $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$, while $B = (b_{ik})$ is an arbitrary integral matrix. In order to use Formanek's method we transform A to diagonal form via a similarity S and apply the same similarity to B, obtaining a matrix $\tilde{B}$ whose elements lie in the normal closure of $Q(\alpha)$.

Restricting to the case $n = 3$ the central polynomial consists of the sum of certain monomials

$$cA^{i_0} \quad BA^{i_1} \quad BA^{i_2} \quad BA^{i_3},$$

where $i_0 + i_1 + i_2 + i_3 = 6$ and $c = \pm 1$ or -2.

Assuming A already in diagonal form the central polynomial applied to A, $\tilde{B}$ works out as $(\tilde{b}_{12}\tilde{b}_{23}\tilde{b}_{31} + \tilde{b}_{21}\tilde{b}_{13}\tilde{b}_{32})\prod_{1 \leqslant i < j \leqslant 3}(\alpha^{(i)} - \alpha^{(j)})^2$. This can be obtained by direct computation of the element (1,1) of the resulting scalar matrix or by using Formanek's result for diagonal A and for three matrices B_1, B_2, B_3 appearing in the monomials instead of $\tilde{B}$, taking them as matrix units and then using the linearity in the B_i's and finally replacing the B_i's by $\tilde{B}$. What remains in the scalar from $\tilde{B}$ are only full cycles $\tilde{b}_{i_1 j_1}\tilde{b}_{j_1 j_2}\tilde{b}_{j_2 i_1}$.

Comparing with the $n = 2$ case: the result there is $\tilde{b}_{12}\tilde{b}_{21}$.

We now discuss the similarity S to obtain the full generalization of (1). Again, only $n = 3$ is treated. However, while what was obtained for general n in the preceding paragraphs can be modelled in $n = 3$, this is not completely the case here from now on.

THEOREM 2. *Let A, B be a pair of 3×3 integral matrices, A with irreducible characteristic polynomial $f(x)$ and characteristic roots $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$, B an arbitrary integral matrix. Then the Formanek central polynomial $G_n(A, B, B, B)$ is equal to the scalar matrix gI where g is equal to the product of the discriminant d of the polynomial $f(x)$ times the trace from $Q(\sqrt{d})$ of a relative norm from $Q(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)})$ to $Q(\sqrt{d})$.*

PROOF. In view of what was explained earlier it is sufficient to show that $\tilde{b}_{12}, \tilde{b}_{23}, \tilde{b}_{31}$ are conjugate elements in the extension $Q(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)})$ with respect to $Q(\sqrt{d})$ and that $\tilde{b}_{12}\tilde{b}_{23}\tilde{b}_{31}$, $\tilde{b}_{21}\tilde{b}_{13}\tilde{b}_{32}$ are conjugate elements of $Q(\sqrt{d})$ with respect to Q.

The matrix S which transforms B into $\tilde{B}$ can be chosen to consist of 3 column vectors which are the characteristic vectors of A with respect to $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$ and hence are conjugate. We denote them correspondingly as $\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}$; $\alpha_1^{(2)}, \alpha_2^{(2)}, \alpha_3^{(2)}$; $\alpha_1^{(3)}, \alpha_2^{(3)}, \alpha_3^{(3)}$. (Each of these vectors forms a Z-basis for an ideal in its corresponding field via the correspondence between ideal classes and matrix classes).

To the vector $\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}$ corresponds a dual or complementary vector $\beta_1^{(1)}, \beta_2^{(1)}, \beta_3^{(1)}$ satisfying trace $\alpha_i^{(1)} \beta_k^{(1)} = \delta_{ik}$. This shows that the matrix with rows $\beta_1^{(1)}, \beta_2^{(1)}, \beta_3^{(1)}$ and its conjugates is the inverse of the matrix with columns $\alpha_1^{(i)}, \alpha_2^{(i)}, \alpha_3^{(i)}$ $(i = 1, 2, 3)$.

Hence, we have the following form for $\tilde{B} = (b_{ik})$:

$$\tilde{b}_{ik} = \sum_{r,s} \beta_r^{(i)} b_{rs} \alpha_s^{(k)}.$$

Hence

$$\tilde{b}_{12} = \sum \beta_r^{(1)} b_{rs} \alpha_s^{(2)}; \quad \tilde{b}_{23} = \sum \beta_r^{(2)} b_{rs} \alpha_s^{(3)}; \quad \tilde{b}_{31} = \sum \beta_r^{(3)} b_{rs} \alpha_s^{(1)};$$

and similarly for $\tilde{b}_{21}, \tilde{b}_{13}, \tilde{b}_{32}$.

This proves the assertion.

The idea of using the complementary basis was used by Bender when reproving the author's original theorem (1) in a less computational way. At that time Bender also observed that his method yields that for $n = 3$ the additive commutator of $\operatorname{diag}(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)})$ and $\tilde{B}$ goes over into

$$\begin{pmatrix} 0 & \tilde{b}_{12} & \tilde{b}_{13} \\ \tilde{b}_{21} & 0 & \tilde{b}_{23} \\ \tilde{b}_{31} & \tilde{b}_{32} & 0 \end{pmatrix}.$$

Hence it appears that for $n = 3$ the central polynomial scalar and the determinant of the commutator differ merely by $\prod_{1 \leqslant i < j \leqslant 3} (\alpha^{(i)} - \alpha^{(j)})^2$.

References

E. Bender, private communication.

E. Formanek (1972), "Central polynomials for matrix rings", *J. Algebra* **23**, 129–132.

O. Taussky (1962), "Ideal matrices I", *Arch. Math.* **13**, 275–282.

O. Taussky (1974), "Additive commutators between 2×2 integral matrix representations of orders in identical or different quadratic number fields", *Bull. Amer. Math. Soc.* **80**, 885–887.

O. Taussky (1976), *Two Facts concerning Rational* 2×2 *Matrices leading to Integral Ternary Forms representing Zero*. (Seminar Notes Calif. Inst. Tech.)

H. Zassenhaus (1977), "Cyclic orders", *Number Theory and Algebra*, edited by H. Zassenhaus, (Academic Press, New York), 363–393.

Mathematics Department 253–37
California Institute of Technology
Pasadena, CA 91125
USA