BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 3, May 1973

RESEARCH ANNOUNCEMENTS

The purpose of this department is to provide early announcement of significant new results, with some indications of proof. Although ordinarily a research announcement should be a brief summary of a paper to be published in full elsewhere, papers giving complete proofs of results of exceptional interest are also solicited. Manuscripts more than eight typewritten double spaced pages long will not be considered as acceptable. All research announcements are communicated by members of the Council of the American Mathematical Society. An author should send his paper directly to a Council member for consideration as a research announcement. A list of members of the Council for 1973 is given at the end of this issue.

SYMMETRIC MATRICES, CHARACTERISTIC POLYNOMIALS, AND HILBERT SYMBOLS OVER LOCAL NUMBER FIELDS

BY EDWARD A. BENDER AND NORMAN P. HERZBERG

Communicated by Olga Taussky Todd, November 20, 1972

Let F be a local number field. We give necessary and sufficient conditions for a monic polynomial $p(x)$ over F to be the characteristic polynomial of a symmetric matrix over F. (A matrix "over F" is a matrix whose elements lie in F.) In the process we obtain a lifting formula for the Hilbert symbol. Proofs will appear elsewhere ([**2**], [**3**], [**4**]).

Notation and terminology. We denote the transpose, determinant, and dimension of a square matrix X by X^t, $|X|$ and $\dim X$ respectively.

Let $p(x) = q_1(x)q_2(x)\cdots$ be the prime decomposition of $p(x)$ in $F[x]$. Define

$$G_i = F[x]/(q_i(x)) \quad \text{and} \quad \mathscr{A} = G_1 \oplus G_2 \oplus \cdots.$$

For $\lambda = \lambda_1 \oplus \lambda_2 \oplus \cdots \in \mathscr{A}$ define the norm by

$$N_{\mathscr{A}/F}\lambda = (N_{G_1/F}\lambda_1)(N_{G_2/F}\lambda_2)\cdots.$$

Let $\boldsymbol{\alpha}$ be a basis for G over F and for $\lambda \in G$ define the symmetric matrix $A(\lambda; G/F)$ by $a_{ij} = \operatorname{tr}_{G/F}(\lambda\alpha_i\alpha_j)$. Since $\boldsymbol{\alpha}$ is arbitrary $A(\lambda; G/F)$ is defined only up to congruence over F. (Recall that "A is congruent to B over F" means $TAT^t = B$ for some nonsingular matrix T with elements in F.) If $\lambda \in \mathscr{A}$, any matrix congruent over F to $A(\lambda; \mathscr{A}/F) = A(\lambda_1; G_1/F) \oplus A(\lambda_2; G_2/F)\cdots$ is called *a matrix from* $\mathscr{A}$ *to* F. (Here $\oplus$ denotes the direct sum of matrices.) If X is a matrix over G, let $A(X)$ be the matrix obtained by replacing x_{ij} with $A(x_{ij}; G/F)$.

AMS (MOS) subject classifications (1970). Primary 15A18, 10C05, 12B05, 15A57; Secondary 10C20, 15A63.

Let $(\cdot,\cdot)_F$ and $c_F(\cdot)$ denote the Hilbert and Hasse symbols over a local field F. See [**5**] for details.

The lifting theorem. In [**2**] we prove

THEOREM 1. *Let G be an extension of the local field F. Let X and Y be nonsingular symmetric matrices over G such that* $\dim X = \dim Y$ *and* $|X|/|Y|$ *is a square in G. Then*

$$c_G(X)c_G(Y) = c_F(A(X;G/F))c_F(A(Y;G/F)). \tag{1}$$

When

$$X = \begin{pmatrix} 1 & 0 \\ 0 & \lambda\mu \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

the theorem leads to

COROLLARY. *Let F and G be as in the theorem. If λ and μ are nonzero elements of G, then*

$$(\lambda, \mu)_G = (N_{G/F}\lambda, N_{G/F}\mu)_F C(1)C(\lambda)C(\mu)C(\lambda\mu)$$

where $C(\beta) = c_F(A(\beta;G/F))$.

Another way to state (1) is: $A(X;G/F)$ and $A(Y;G/F)$ are congruent over F if and only if X and Y are congruent over G. The "if" direction is true for any field, but the "only if" direction depends on the properties of quadratic forms over local fields.

Characteristic polynomials. Let $\boldsymbol{Q}_2$ denote the 2-adic rational numbers.

THEOREM 2. *Let F be a local number field and let $p(x)$ be a monic polynomial over F. There exists a symmetric matrix over F with characteristic polynomial $p(x)$ if and only if*

(i) *there is a $\mu \in \mathscr{A}$ such that $(-1)^{n(n-1)/2}N_{\mathscr{A}/F}\mu$ is a nonzero square in F, and*

(ii) *if $p(x)$ is an irreducible quartic over $F = \boldsymbol{Q}_2$, there is a quadratic subextension of F in $\mathscr{A} = G_1$.*

PROOF OF NECESSITY IN THEOREM 2. It is shown in [**3**] that if A and X are commuting matrices over F such that $p(x)$ is the characteristic polynomial of F, then $|X| = N_{\mathscr{A}/F}\lambda$ for some $\lambda \in \mathscr{A}$. This is used to show that (i) is necessary in Theorem 2.

In [**4**] it is shown, with the aid of a computer, that if $F = \boldsymbol{Q}_2$ and $p(x)$ is an irreducible polynomial of degree 4 such that there is no field between $\boldsymbol{Q}_2$ and $\mathscr{A} = G_1$, then there is no symmetric matrix over $\boldsymbol{Q}_2$ having $p(x)$ as its characteristic polynomial. In order to use a computer it is necessary (i) to obtain a list of all quartic extensions G of $\boldsymbol{Q}_2$ such that there is no field between G and Q_2, and (ii) to provide a test for the existence of symmetric matrices. The test is based on the fact that if the *irreducible* polynomial $p(x)$ is the characteristic polynomial of a symmetric matrix, then the identity is a matrix from G_1 to F.

Some counterexamples involving symmetric matrices over the rational integers are also discussed in [**4**].

Proof of sufficiency in Theorem 2. Sufficiency is proved in [**3**]. We use the fact that if the identity is a matrix from $\mathscr{A}$ to F, then there is a symmetric matrix with characteristic polynomial $p(x)$ [**1**, Lemma 1]. The proof of sufficiency when F is nondyadic is like that in [**1**, Lemma 2].

Dyadic fields are handled by piecing together matrices from G_i to F to get a matrix from $\mathscr{A}$ to F. The main tool is

Lemma 1. *Let G be an extension of the dyadic local number field F such that*

(i) $[G:F] > 2$,

(ii) *if* $[G:F] = 4$ *and* $F = Q_2$, *then there is a quadratic subextension of* Q_2 *in* G.

Then for every nonzero $\lambda \in G$, *there is a* $\sigma \in G$ *such that* $N_{G/F}\sigma$ *is a square in* F *and* $c_F(A(\lambda))c_F(A(\sigma\lambda)) = -1$.

The proof of Lemma 1 relies heavily on the fact that when σ does not exist

$$[G:F] \leqq 2 + 2/[F:Q_2]. \tag{2}$$

To deduce this we use the corollary of Theorem 1 to show that $(\alpha, \beta)_G = +1$ whenever $\alpha, \beta \in S = (N_{G/F})^{-1}(F^{*2})$, the elements of G with nonzero square norms. Using this observation we deduce that

$$|G^*:G^{*2}| \leqq |G^*:S|^2 \leqq |F^*:F^{*2}|^2$$

where $|\mathscr{G}:\mathscr{H}|$ denotes the index of the subgroup $\mathscr{H}$ in the group $\mathscr{G}$ and G^* is the multiplicative group of nonzero elements of G. This implies (2).

References

1. E. A. Bender, *Characteristic polynomials of symmetric matrices*, Pacific J. Math. **25** (1968), 433–441. MR **37** #5193.

2. ———, *A lifting formula for the Hilbert symbol*, Proc. Amer. Math. Soc. (to appear).

3. ———, *Characteristic polynomials of symmetric matrices.* II. *Local number fields* (to appear).

4. E. A. Bender and N. P. Herzberg, *Characteristic polynomials of symmetric matrices.* III: *Some counterexamples* (to appear).

5. O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der math. Wissenschaften, Band 117, Academic Press, New York; Springer-Verlag, Berlin, 1963. MR **27** #2485.

Communications Research Division, Institute for Defense Analyses, Princeton, New Jersey 08540