

## CHARACTERISTIC POLYNOMIALS OF SYMMETRIC MATRICES

EDWARD A. BENDER

Let  $F$  be a field and  $p$  an  $F$ -polynomial. We say that  $p$  is  $F$ -real if and only if every real closure of  $F$  contains the splitting field of  $p$  over  $F$ . Our main purpose is to prove

**THEOREM 1.** Let  $F$  be an algebraic number field and  $p$  a monic  $F$ -polynomial with an odd degree factor over  $F$ . Then  $p$  is  $F$ -real if and only if it is the characteristic polynomial of a symmetric  $F$ -matrix.

That  $p$  must be  $F$ -real follows from work of Krakowski [4, Satz 3.3]. To prove the converse we generalize results of Sapiro [6] in Lemma 1 and Theorem 3. Sapiro deals with the case in which  $p$  is a cubic. Theorem 4 considers the minimum dimension of symmetric matrices with a given root.

2. A basic lemma. In our proof we shall study congruence classes of certain symmetric matrices which are defined below. We shall denote congruence of the matrices  $A$  and  $B$  over the field  $F$  (i.e.,  $A = TBT'$  for some nonsingular  $F$ -matrix  $T$ ) by  $A \sim B(F)$ .

**DEFINITION.** Let  $G$  be a field with subfield  $F$ . If  $\lambda \in G$  is nonzero and if  $\alpha_1, \dots, \alpha_n$  form a basis for  $G$  (as a vector space) over  $F$ , define the matrices  $M = \|\alpha_i^{(j)}\|$  and  $D(\lambda) = \text{diag}(\lambda^{(1)}, \dots, \lambda^{(n)})$  where superscripts denote conjugacy over  $F$ . We call

$$A = A(\lambda) = MD(\lambda)M'$$

a matrix from  $G$  to  $F$ . Clearly

$$a_{ij} = \text{tr}_{G/F}(\lambda \alpha_i \alpha_j).$$

If  $\mathcal{A} = \Sigma \oplus G_i$  where the  $G_i$  are extension fields of  $F$ , and if  $A_i$  is a matrix from  $G_i$  to  $F$ , then any matrix congruent to  $\Sigma \oplus A_i$  over  $F$  is called a matrix from  $\mathcal{A}$  to  $F$ . Note that a different choice for the basis  $\alpha_1, \dots, \alpha_n$  would lead to a matrix congruent to  $A(\lambda)$  over  $F$ .

**LEMMA 1.** Let  $F$  be a field and  $p = q_1 \cdots q_m$  a monic  $F$ -polynomial decomposed into prime factors over  $F$ . Assume that the splitting field of  $p$  over  $F$  is a separable extension of  $F$ . If the identity is a matrix from

$$\sum_1^m \oplus F[x]/(q_i)$$

to  $F$ , then  $p$  is the characteristic polynomial of a symmetric  $F$ -matrix.

*Proof.* Let  $D = \Sigma \oplus D(\lambda_i)$  and  $M = \Sigma \oplus M_i$  where the  $i^{\text{th}}$  component refers to  $F[x]/(q_i(x))$ . We have  $TT' = MDM'$  for some  $F$ -matrix  $T$ . Let  $E = \Sigma \oplus D(\theta_i)$  where  $\theta_i$  is a zero of  $q_i$ . By separability  $M$  is nonsingular. We have  $T^{-1}MD = (M^{-1}T)'$ . Let

$$S = T^{-1}(MEM^{-1})T .$$

Then

$$\begin{aligned} S' &= (M^{-1}T)'E(T^{-1}M)' \\ &= (T^{-1}M)ED(T^{-1}M)' \\ &= (T^{-1}M)E(T^{-1}MD)' \\ &= (T^{-1}M)E(M^{-1}T) \\ &= S . \end{aligned}$$

Also  $|S - \lambda I| = |E - \lambda I| = \pm p(\lambda)$ . Finally,  $S$  is an  $F$ -matrix since  $M_i^{-1} = ||\beta_i^{(j)}||$  where  $\vec{\beta}$  is the complementary basis to  $\vec{\alpha}$  [2, p. 437].

3. The irreducible case. In this section we shall reduce the proof of Theorem 1 to a study of the prime factors of  $p$  over  $F$ . This requires the Hasse-Minkowski Theorem. The Hilbert symbol over a local field  $L$  will be written  $(a, b/L) = (a, b) = \pm 1$ . If  $A$  is a symmetric  $L$  matrix and  $A \sim \Sigma \oplus a_i(L)$ , then

$$c(A/L) = c(A) = \prod_{i \leq j} (a_i, a_j)$$

is the Hasse invariant. If  $A$  is a nonsingular symmetric matrix over an algebraic number field  $F$ , then we have  $\dim A$  and  $\det A = |A|$  as global invariants,  $c(A/F_p)$  as Hasse invariants, and  $\text{ind}^+(A/F_p)$  as real archimedean invariants where  $\text{ind}^+(A/F_p)$  is the number of positive  $a_i$  in  $A \sim \Sigma \oplus a_i(F_p)$ .

**THEOREM 2.** *Let  $F$  be an algebraic number field and  $q$  an  $F$ -real irreducible  $F$  polynomial of degree  $n$ . Let  $K = F[x]/(q(x))$  and let  $k$  be a rational integer.*

(1) *If  $n$  is odd, the identity is a matrix from  $K$  to  $F$ .*

(2) *If  $n$  is even, there is a matrix  $A$  from  $K$  to  $F$  which has the same archimedean invariants as the identity and satisfies  $c(A)(|A|, -1)^k = +1$  at all local completions of  $F$ .*

The next two sections develop the ideas needed in the proof of this theorem. We now prove Theorem 1 from Lemma 1 and Theorem 2.

Let  $p = q_1 \cdots q_s r_1 \cdots r_t$  be the prime factorization of  $p$  over  $F$  where the degree  $d_i$  of  $q_i$  is odd and the degree  $e_i$  of  $r_i$  is even. By assumption  $s \neq 0$ . Let  $A_i$  be the matrix from  $F[x]/(r_i(x))$  to  $F$  given by Theorem 2 (2) with

$$k = k(i) = \left( \sum_{j=1}^{i-1} e_j + d_1 - 1 \right) / 2 .$$

Let  $B_0$  be the  $d_1$  dimensional identity matrix—a matrix from  $F[x]/(q_1(x))$  to  $F$  by Theorem 2(1)—and let

$$B_i = | A_i | B_{i-1} \oplus A_i .$$

By induction, the Hasse-Minkowski Theorem gives  $B_i \sim I(F)$ . Thus the identity is a matrix from

$$F[x]/(q_1(x)) \oplus \sum_{i=1}^r \oplus F[x]/(r_i(x))$$

to  $F$ . By Theorem 2 (1), the identity is a matrix from  $F[x]/(q_i(x))$ , so an application of Lemma 1 proves Theorem 1.

4. **The local case.** In this section we reduce the proof of theorems having the form of Theorem 2 to local considerations.

**THEOREM 3.** *Let  $F$  be an algebraic number field and  $q$  an  $F$ -real irreducible  $F$ -polynomial. Let  $\alpha_1, \dots, \alpha_n$  be algebraic integers in  $G = F[x]/(q(x))$  which are a basis for  $G$  over  $F$ . Let  $M = || \alpha_i^{(j)} ||$  and let  $\Omega$  be the set of prime spots on  $F$  which divide  $2 |M|^2$ . Suppose that for each  $\mathfrak{p} \in \Omega$  there is given a matrix  $A(\lambda_{\mathfrak{p}})$  from  $F_{\mathfrak{p}}[x]/(q(x))$  to  $F_{\mathfrak{p}}$ . Then there is a matrix  $A = A(\lambda)$  from  $G$  to  $F$  and a local prime spot  $\mathfrak{q} \notin \Omega$  on  $F$  such that*

(1) *if  $\mathfrak{p} \in \Omega$ , then*

$$c(A/F_{\mathfrak{p}}) = c(A(\lambda_{\mathfrak{p}})/F_{\mathfrak{p}}) ,$$

and

$$| A(\lambda_{\mathfrak{p}}) | / | A | \in F_{\mathfrak{p}}^2 ,$$

the group of squares in  $F_{\mathfrak{p}}$

(2) *if  $\mathfrak{p} \notin \Omega$  is a local prime spot on  $F$  distinct from  $\mathfrak{q}$ , then  $c(A/F_{\mathfrak{p}}) = +1$  and  $| A |$  is a unit of  $F_{\mathfrak{p}}$ ;*

(3)  *$A$  has the same real archimedean invariants as the identity matrix of the same dimension.*

*Proof.* If we change the basis used in forming  $A(\lambda_{\mathfrak{p}})$  and change  $\lambda_{\mathfrak{p}}$  by a square factor, then  $c(A(\lambda_{\mathfrak{p}}))$  and  $| A(\lambda_{\mathfrak{p}}) | \cdot F_{\mathfrak{p}}^2$  will be unchanged.

Hence we may assume that  $\alpha_1, \dots, \alpha_n$  is the basis for all  $\mathfrak{p}$  and that  $\lambda_{\mathfrak{p}}$  is integral at  $\mathfrak{p}$ .

There is a sufficiently large positive rational integer  $m$  such that

$$\lambda_0 \equiv \lambda_{\mathfrak{p}} \pmod{\mathfrak{p}^m} \quad \text{for } \mathfrak{p} \in \Omega,$$

implies

$$c(A(\lambda_0)/F_{\mathfrak{p}}) = c(A(\lambda_{\mathfrak{p}})/F_{\mathfrak{p}}) \quad \text{for } \mathfrak{p} \in \Omega,$$

and

$$|A(\lambda_{\mathfrak{p}})| \mid |A(\lambda_0)| \in F_{\mathfrak{p}}^2 \quad \text{for } \mathfrak{p} \in \Omega.$$

Choose  $\lambda_0$  such that

- (i)  $\lambda_0$  is an integer of  $G$
- (ii)  $\lambda_0 \equiv \lambda_{\mathfrak{p}} \pmod{\mathfrak{p}^m}$  for  $\mathfrak{p} \in \Omega$
- (iii) if  $F$  is formally real,  $\lambda_0$  is totally positive. Let  $\mathfrak{M} = \prod_{\mathfrak{p} \in \Omega} \mathfrak{p}^m$ .

For each local prime spot  $\mathfrak{P}$  on  $G$  let  $k(\mathfrak{P})$  be the largest rational integer such that  $\mathfrak{P}^{k(\mathfrak{P})}$  divides  $\lambda_0$ . Let

$$\mathfrak{U} = \prod_{\mathfrak{P} \mid \mathfrak{p} \in \Omega} \mathfrak{P}^{k(\mathfrak{P})}.$$

Then  $\lambda_0/\mathfrak{U}$  is prime to  $\mathfrak{M}$ . By the generalized arithmetic progression theorem [1, Satz 13], there is an  $\alpha \in G$  and a prime spot  $\mathfrak{D}$  on  $G$  such that

- (i)  $(\alpha\lambda_0/\mathfrak{U}) = \mathfrak{D}$ ,
- (ii)  $\alpha \equiv 1 \pmod{\mathfrak{M}}$ ,
- (iii) if  $F$  is formally real,  $\alpha$  is totally positive.

Let  $\lambda = \alpha\lambda_0$  and let  $\mathfrak{q}$  be the prime spot on  $F$  which  $\mathfrak{D}$  divides. Since  $\lambda \equiv \lambda_0 \equiv \lambda_{\mathfrak{p}} \pmod{\mathfrak{p}^m}$ , part (1) holds. Since  $\lambda$  is totally positive if  $F$  is formally real, (3) holds. Since  $A(\lambda)$  has integral entries and  $|A(\lambda)| = N(\mathfrak{D}\mathfrak{U})|M|^2$ , a unit of  $F_{\mathfrak{p}}$  for  $\mathfrak{p} \in \Omega \cup \{\mathfrak{q}\}$ , part (2) holds by [5, 92: 1].

**5. Local lemmas.** In this section we prove a series of lemmas. They will be used together with Theorem 3 to prove Theorem 2. Throughout this section we shall let  $L$  be a local field with prime spot  $\mathfrak{p}$  and characteristic zero; further,  $K = K_1, K_2, \dots, K_m$  will be finite algebraic extensions of  $L$ .

**LEMMA 2.** *If  $\mathfrak{p}$  is prime to 2, there is a matrix  $A$  from  $\Sigma \oplus K_i$  to  $L$  with integer entries and unit determinant.*

*Proof.* It suffices to exhibit such a matrix from  $K$  to  $L$ . Let  $\alpha_1, \dots, \alpha_n$  be a free basis for the integers of  $K_i$  over the integers of  $L$ . Let  $M = \|\alpha_i^{(j)}\|$ . The matrix  $M'^{-1}$  has the form  $\|\beta_i^{(j)}\|$  where

$\beta_1, \dots, \beta_n$  is the complementary basis [2, p. 437] to  $\alpha_1, \dots, \alpha_n$ . Let  $\Pi$  be a prime of  $K$ . The ideal  $(\beta_1, \dots, \beta_n)$  equals  $(\Pi^k)$  for some rational integer  $k$ . Since  $(\alpha_1, \dots, \alpha_n) = (1)$ , there is a matrix  $A$ , whose elements are integers of  $L$  and whose determinant is an  $L$  unit, satisfying  $MD(\Pi^k) = AM'^{-1}$ .

For the remainder of this section we shall assume that  $p$  divides 2.

LEMMA 3. *If  $[K:L]$  is odd, the identity is a matrix from  $K$  to  $L$ .*

*Proof.* Let  $T$  be the inertia subextension of  $L$ . Suppose that the identity is a matrix from  $T$  to  $L$ , namely  $M_1 D_1 M'_1$ , and that the identity is a matrix from  $K$  to  $T$ , namely  $M_2 D_2 M'_2$ . Then the identity is a matrix from  $K$  to  $L$ , namely

$$(M_1 \otimes M_2)(D_1 \otimes D_2)(M_1 \otimes M_2)'$$

We first show that the identity is a matrix from  $T$  to  $L$ . Let  $M_1 = \|\alpha_i^{(j)}\|$  where  $\alpha_1, \dots, \alpha_f$  is a basis for  $T$  over  $L$ . Set  $A = M_1 M'_1$ . Since  $T$  is a cyclic extension of  $L$ , we have  $A \sim I(T)$ . Since  $[T:L]$  is odd, it follows that  $A \sim I(L)$ .

We now show that the identity is a matrix from  $K$  to  $T$ . Let  $\Pi$  be a prime of  $K$  such that  $\Pi^e = \pi$ , a prime of  $T$ , where  $e = [K:T]$  is odd. Let  $\alpha_i = \Pi^{i-1}$  and  $M_2 = \|\alpha_i^{(j)}\|$  and  $a = (e^2 - 1)/8$ . There are two cases.

- (i) If  $(-1, -1/T)^a = +1$ , let  $\lambda = 1/e$ ,
- (ii) If  $(-1, -1/T)^a = -1$ , let

$$\lambda = (1 + \Pi^{-1} + 4\Pi^{-2})/e.$$

Set  $A = |B \cdot B$  where  $B = M_2 D(\lambda) M'_2$ . In case (i) it is easily verified that  $c(A) = +1$ .

We consider case (ii). Since  $(-1, -1)^a = -1$ , it follows that  $e \equiv \pm 3 \pmod{8}$ . Also, as

$$-\left(\frac{1 - \sqrt{-3}}{2}\right)^2 - \left(\frac{1 + \sqrt{-3}}{2}\right)^2 = 1,$$

we have  $f(T(\sqrt{5})/T) = 2$  (see [5, 63:3]). Thus  $(\pi, 5) = -1$  and  $(\epsilon, 5) = +1$  for any unit  $\epsilon$  of  $T$ . When  $e = 3$  it is easily shown that  $c(A) = +1$ . Assume  $e > 3$ . The matrix  $B$  has the form shown in Figure I. We shall use the formula [3, p. 31]:

$$c(C_m) = (-1, |C_m|) \prod_{i=1}^{m-1} (|C_i|, -|C_{i+1}|),$$

if  $\Pi_{i=1}^m |C_i| \neq 0$ , where  $C_i = \|c_{st}\|$  ( $1 \leq s, t \leq i$ ).

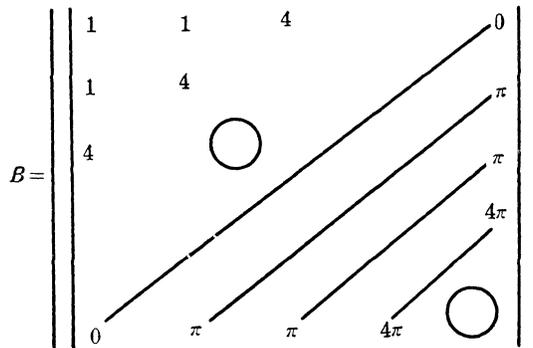


FIGURE I.

We must transform  $B$ . Let  $X$  be the  $e \times e$  matrix such that pre-multiplication by  $X$  adds  $\pi^{-1}$  times the  $(e - k + 2)^{\text{nd}}$  row to the  $k^{\text{th}}$  row for  $k = 4, 6, 8, \dots, 4[e/8] + 2$  and leaves the remaining rows unchanged. Let  $C = XBX'$ . By studying  $(X_i)^{-1}C_i(X_i)^{i-1}$ , we find that

- (i)  $|C_{2i+1}| \in (-1)^i T^2$  for  $2i + 1 < e$ ,
- (ii)  $|C_{e-1}| \in (-1)^{(e-1)/2} 5T^2$ ,
- (iii)  $|C_e| = \pi^{e-2} \varepsilon$  for some unit  $\varepsilon$  of  $T$ ,
- (iv)  $\prod_i^e |C_i| \neq 0$ .

It therefore follows that

- (i)  $(|C_{2i-1}|, -|C_{2i}|)(|C_{2i}|, -|C_{2i+1}|) = (-1)^{i-1}$  for  $2i + 1 < e$ ,
- (ii)  $(|C_{e-2}|, -|C_{e-1}|) = (-1)^{(e-3)/2}$ ,
- (iii)  $(|C_{e-1}|, -|C_e|) = (-1)^{(e+1)/2} (-1, |C_e|)^{(e-1)/2}$ .

Thus

$$\begin{aligned} c(A) &= C(B)(-1, |B_e|)^{(e+1)/2} \\ &= c(C_e)(-1, |C_e|)^{(e+1)/2} \\ &= +1 \quad \text{since } e \equiv \pm 3 \pmod{8}. \end{aligned}$$

LEMMA 4. If  $L^2 \cong N(K/L)$ , the norm group of  $K$  over  $L$ , then the identity is a matrix from  $K$  to  $L$ .

*Proof.* We make some preliminary observations. Let  $T_i$  be a subfield of  $K$  (to be specified later) such that  $N(K/T_i) \cong T_i^2$ . Let  $T_i^*$  be the multiplicative group of  $T_i$ . Let  $H$  be the maximum abelian subextension of  $T_i$  in  $K$  of type  $(2, 2, \dots, 2)$ . By the reciprocity and limitation theorems of class field theory [7, pp. 177, 180], the Galois group of  $H$  over  $T_i$  is isomorphic to

$$(T_i^*/N(K/T_i))/(T_i^*/N(K/T_i))^2.$$

Since  $N(K/T_i) \cong T_i^{*2}$ , this is isomorphic to  $T_i^*/T_i^{*2}$ . Hence  $[T_i^*: T_i^{*2}] =$

$[H: T_i]$  which divides  $[K: T_i]$ . By [5, 63: 9], 8 divides  $[T_i^*: T_i^{*2}]$ . Thus

(i)  $[K: T_i] \equiv 0 \pmod{8}$ .

Since  $N(H/T_i) \subseteq T_i^2$ , we have that  $f(H/T_i) > 1$ . Since  $[H: T_i]$  is a power of 2 and  $K \supseteq H$ , we have

(ii)  $f(K/T_i) \equiv 0 \pmod{2}$ .

Suppose  $K = T_i(\theta)$ . Let  $\alpha_i = \theta^{i-1}$  and  $M = \|\alpha_i^{(j)}\|$ . If  $\lambda \in K$  we have

$$|MD(\lambda)M'| = N_{K/T_i} \left( \lambda \prod_{i \neq 1} (\theta^{(1)} - \theta^{(i)}) \right) \in T_i^2,$$

by the formula for a van der Monde determinant and  $N(K/T_i) \subseteq T_i^2$ . Hence

(iii) if  $C$  is a matrix from  $K$  to  $T_i$ , then  $|C| \in T_i^2$ .

We now apply the above observations. Let  $T$  be the inertia subextension of  $L$ . Construct the tower

$$L = T_0 \subset T_1 \subset \dots \subset T_k \subseteq T,$$

where  $[T_j: T_{j-1}] = 2$  for  $1 \leq j \leq k$  and  $[T: T_k]$  is odd. Since  $f(K/T_k)$  is odd, we have  $N(K/T_k) \not\subseteq T_k^2$  by (ii). Hence we may choose  $i$  such that  $N(K/T_i) \subseteq T_i^2$  and  $N(K/T_{i+1}) \not\subseteq T_{i+1}^2$ . (Actually  $i = k - 1$ , but this is irrelevant.) Suppose the identity is a matrix from  $K$  to  $T_i$ . Let  $B$  be a matrix from  $T_i$  to  $L$ . Then  $A = I \otimes B$  is a matrix from  $K$  to  $L$ . By (i) we have  $\dim I \equiv 0 \pmod{4}$ . Hence  $|A| \in L^2$  and  $c(A/L) = +1$  by the formula.

(\*)  $c(X \otimes Y) = c(X)^y c(Y)^x (-1, |X|)^{y(y-1)/2} (-1, |Y|)^{x(x-1)/2} (|X|, |Y|)^{xy+1}$

where  $X, Y$  are symmetric matrices,  $x = \dim X$  and  $y = \dim Y$ . It suffices to show that the identity is a matrix from  $K$  to  $T_i$ .

Let  $C$  be a matrix from  $K$  to  $T_{i+1}$  with  $|C| \notin T_{i+1}^2$ . (This can be done since  $N(K/T_{i+1}) \not\subseteq T_{i+1}^2$ .) We have  $C \sim I \oplus -1 \oplus s \oplus t$  where  $s, t \in T_{i+1}$  by [5, 63: 17]. Let  $e \in T_i$  be such that  $T_{i+1} = T_i(\sqrt{e})$ . Let  $M = \left\| \frac{1}{\sqrt{e}} \quad \frac{1}{\sqrt{e}} \right\|$  and  $E(q) = MD(q)M'$  for  $q \in T_{i+1}$ . We have that

$$S(r) = (I \oplus -1) \otimes E(r) \oplus E(rs) \oplus E(rt)$$

is a matrix from  $K$  to  $T_i$  for nonzero  $r \in T_{i+1}$ . By (iii) we have  $|S(r)| \in T_i^2$ . Since

$$\dim(I \oplus -1) = \dim S(r)/2 - 2 \equiv 2 \pmod{4} \text{ by (i),}$$

we have

$$|(I \oplus -1) \otimes E(r)| \in T_i^2.$$

Hence  $|E(rs)| \in |E(rt)| \cdot T_i^2$ . Thus

$$c(S(r)) = c((I \oplus -1) \otimes E(r))c(E(rs))c(E(rt))(|E(rs)|, -1) \\ = (-1, -1)c(E(rs))c(E(rt))(|E(rs)|, -1) \text{ by } (*).$$

Any  $q \in T_{i+1}$  has the form  $a + b\sqrt{e}$  with  $a, b \in T_i$ . Write  $q_1 = a$ . If  $q_1 \neq 0$ , then

$$c(E(q)) = (2q_1, -|E(q)|)(-1, |E(q)|).$$

If  $(rs)_i(rt)_i \neq 0$ , we have

$$c(S(r)) = (-(rs)_i(rt)_i, -|E(rs)|).$$

We may choose  $r = s^{-1}(l + \sqrt{e})^2\sqrt{e}$  with  $l = 0, 1$ , or  $4$  such that  $(rs)_i(rt)_i \neq 0$ . Since  $-|E(rs)| \in T_i^2$ , we have  $c(S(r)) = +1$ .

**LEMMA 5.** *If  $\sum_1^m [K_i: L]$  is odd, the identity is a matrix from  $\sum_1^m \oplus K_i$  to  $L$ .*

*Proof.* By Lemmas 3 and 4 we are done unless  $[K_i: L] = d$  is even and  $N(K_i/L) \not\subseteq L^2$  for some  $i$ . Suppose that this is the case. Since  $N(K_i/L) \not\subseteq L^2$ , there is a matrix  $B$  from  $K_i$  to  $L$  such that  $(-1)^{d/2}|B| \notin L^2$ . Let  $C$  be a matrix from  $\sum_{j \neq i} \oplus K_j$  to  $L$ . Let

$$A = |B| \cdot |C| \cdot C \oplus aB$$

where  $a \in L$  is chosen so that

$$c(A) = c(|B| \cdot |C| \cdot C)(|B|, -1)c(B)(a, (-1)^{d/2}|B|) = +1.$$

**LEMMA 6.** *If  $\sum_1^m [K_i: L]$  is even,  $N(K_1/L) \not\subseteq L^2$ , and  $k$  is a rational integer, then there is a matrix  $A$  from  $\sum_1^m \oplus K_i$  to  $L$  such that  $c(A)(|A|, -1)^k = +1$ .*

*Proof.* Let  $B$  be a matrix from  $\sum_1^m \oplus K_i$  to  $L$  such that  $(-1)^n|B| \notin L^2$  where  $n = \sum_1^m [K_i: L]/2$ . Let  $A = aB$  where  $a \in L$  is chosen so that  $c(A)(|A|, -1)^k = c(B)(|B|, -1)^k(a, (-1)^n|B|) = +1$ .

**6. Proof of Theorem 2.** If  $n$  is odd, apply Lemmas 2 and 5. Let  $B$  be the matrix given by Theorem 3. Define  $A = |B| \cdot B$ . If  $n$  is even, apply Lemmas 2, 3, 4 and 6. Let  $A$  be the matrix given by Theorem 3. In both cases, behavior at the exceptional spot is handled by the Hilbert reciprocity formula [5, p. 190].

**7. Matrices with given roots.** We prove

**THEOREM 4.** *Let  $F$  be an algebraic number field. Let  $\theta$  be the root of an irreducible  $F$ -polynomial  $q$  of degree  $n$ . Then  $\theta$  is the*

characteristic root of some symmetric  $F$ -matrix if and only if  $q$  is  $F$ -real. When such a matrix exists, it may be chosen to have dimension  $n$  or  $n + 1$ , whichever is odd. This dimension is the least possible

- (1) if  $n$  is odd or  
 (2) if  $n \equiv 2 \pmod{4}$  and  $(-1) \notin N(F(\theta)/F) \cdot F^2$ .

*Proof.* Use Theorem 1 with  $p(x) = q(x)$  or  $xq(x)$ . The result is clearly best possible when  $n$  is odd. Suppose  $n \equiv 2(4)$  and  $n$  is least possible. Let  $\alpha_i = \theta^{i-1}$  and  $M = \|\alpha_i^{(j)}\|$ . By the converse of Lemma 1 when  $p$  does not have repeated roots (see [6, Lemma 1.1] for a proof), there is an  $F$ -matrix  $T$  and a  $\lambda \in F(\theta)$  such that  $MD(\lambda)M' = TT'$ . Noting that  $|MM'| = -N(p'(\theta))$ , we get

$$-1 \in N(F(\theta)/F) \cdot F^2 .$$

By class field theory, for all  $n \equiv 2(4)$  there exist  $F$  and  $\theta$  such that  $n + 1$  is the least possible dimension.

I would like to thank Drs. O. Taussky and E. C. Dade for their assistance.

#### REFERENCES

1. H. Hasse, *Bericht Über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* I, Jber. Deutsch. Math.-Verein. **35** (1926), 1-55.
2. ———, *Zahlentheorie*, 2nd ed., Akademie-Verlag, Berlin, 1963.
3. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monograph v. 10, Math. Assn. Amer., 1950.
4. F. Krakowski, *Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern*, Comment. Math. Helv. **32** (1958), 224-240.
5. O. T. O'Meara, *Introduction to quadratic forms*, Grund. Math. Wiss. v. 117, Academic Press Inc., New York, 1963.
6. A. P. Sapiro, *Characteristic polynomials of symmetric matrices* (Russian), Sibirsk. Mat. Z., **3** (1962), 280-291.
7. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

HARVARD UNIVERSITY

Received August 15, 1966. This extends a part of my doctoral dissertation written as a National Science Foundation fellow under Dr. O. Taussky at the California Institute of Technology.

