Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern.

Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern

von FRED KRAKOWSKI

Einleitung

Es ist bekannt, daß jedes über einem kommutativen[1]) Körper K algebraische Element λ Eigenwert einer Matrix mit Elementen aus K – kurz einer K-Matrix – ist. Bei Beschränkung auf symmetrische Matrizen gilt dies nicht allgemein: die Eigenwerte einer reellen symmetrischen Matrix sind reell, und somit ist zum Beispiel $i = \sqrt{-1}$ kein solcher Eigenwert. Die Frage nach einer Charakterisierung derjenigen Elemente der algebraischen, algebraisch-abgeschlossenen Erweiterung Ω eines Körpers K, welche als Eigenwerte symmetrischer K-Matrizen auftreten, bildet den Ausgangspunkt der vorliegenden Arbeit.

Für einen beliebigen Körper K bilden nun die Eigenwerte symmetrischer K-Matrizen ihrerseits wieder einen Körper Λ. Dieser ist in dem Sinne abgeschlossen, daß er auch alle Eigenwerte symmetrischer Λ-Matrizen enthält. Auf Grund dieser beiden in Paragraph 2 bewiesenen Sätze gelingt es durch Induktion nach dem Grad von λ über K, die gestellte Frage vollständig zu beantworten: Ist K formal-reell (das heißt -1 keine Quadratsumme), so ist ein Element λ aus Ω genau dann Eigenwert einer symmetrischen K-Matrix, wenn es zu allen reell-abgeschlossenen Erweiterungskörpern in Ω gehört (das heißt total-reell ist); ist dagegen K nicht formal-reell, so ist überhaupt jedes Element von Ω ein solcher Eigenwert. Insbesondere ist somit eine algebraische Zahl genau dann Eigenwert einer rationalzahligen symmetrischen Matrix, wenn sie und alle ihre Konjugierten reell sind.

In Verallgemeinerung dieser Sätze werden für Körper der Charakteristik $p \neq 2$ auch die Polynome charakterisiert, welche als Minimalpolynome symmetrischer Matrizen auftreten. Im Falle eines formal-reellen Körpers sind es die Polynome mit lauter einfachen, total-reellen Nullstellen, und im nicht formal-reellen Fall sind es alle Polynome ohne Ausnahme. Das zweite trifft hingegen nicht zu, wenn die Charakteristik 2 ist.

Unter Benützung dieser Resultate können wir auch die analogen Fragen für schiefsymmetrische und orthogonale Matrizen beantworten.

Ob in ähnlicher Weise auch die Eigenwerte von symmetrischen Matrizen mit ganzzahligen Elementen durch die Eigenschaft ganz-algebraisch und

[1]) Es werden in dieser Arbeit durchwegs nur kommutative Körper betrachtet.

total-reell zu sein, charakterisiert sind, ist mir außer für den Grad $n = 2$ unbekannt. Ebenfalls ungelöst ist das entsprechende Problem für die Minimalpolynome von höherem als 2. Grad.

Herrn Professor E. SPECKER, der diese Arbeit angeregt hat, danke ich herzlich für vielfältige Ratschläge und Ermunterung.

§ 1. Die Körpereigenschaften der Eigenwerte symmetrischer Matrizen

K sei ein beliebiger Körper, A eine symmetrische Matrix mit Elementen aus K – kurz eine symmetrische K-Matrix – und λ ein Eigenwert von A.

Satz 1.1. *Jedes Element von $L = K(\lambda)$ ist Eigenwert einer symmetrischen K-Matrix.*

Beweis. Ist n der Grad von L über K, so gibt es zu jedem $\mu \in L$ eine Darstellung $\mu = \sum_{k=0}^{n-1} c_k \lambda^k$, $c_k \in K$. Nun ist aber $\sum_{k=0}^{n-1} c_k \lambda^k$ Eigenwert der K-Matrix $B = \sum_{k=0}^{n-1} c_k A^k$, und wenn A symmetrisch ist, so ist es auch B.

Satz 1.2. *Die Menge Λ derjenigen Elemente einer algebraisch-abgeschlossenen Erweiterung Ω von K, welche Eigenwerte symmetrischer K-Matrizen sind, ist ein Körper.*

Beweis. Nach 1.1 ist mit λ auch λ^{-1} Eigenwert einer symmetrischen K-Matrix. Sind λ und μ Eigenwerte der r- bzw. s-reihigen symmetrischen K-Matrizen A und B, so ist $\lambda\mu$ Eigenwert des Kroneckerproduktes $P = A \times B$ (vgl. [4], S. 84), und $\lambda + \mu$ ist Eigenwert von $S = A \times E_s + E_r \times B$, wenn E_r und E_s die r- bzw. s-reihigen Einheitsmatrizen sind. Sind A und B symmetrisch, so sind es auch P und S.

Da Λ ein Unterkörper von Ω ist, ist es sinnvoll, nach denjenigen Elementen von Ω zu fragen, welche Eigenwerte symmetrischer Λ-Matrizen sind. Nach 1.2 bilden diese wiederum einen Körper Λ', der Λ enthält. Es zeigt sich aber, daß Λ gegenüber der Operation der Bildung von Eigenwerten symmetrischer Matrizen abgeschlossen ist, denn es gilt:

Satz 1.3. *Der Körper Λ' der Eigenwerte symmetrischer Λ-Matrizen stimmt mit Λ überein.*

Beweis. Seien $L = ((\lambda_{ik}))$ eine symmetrische Λ-Matrix und $\tilde{K}$ der endliche Erweiterungskörper, welcher aus K durch Adjunktion sämtlicher Elemente λ_{ik} von L entsteht. K ist Endglied einer Kette

$$K = K_0 \subset K_1 \subset \cdots \subset K_p = \tilde{K}$$

von sukzessiven einfachen Erweiterungen, wobei K_l aus K_{l-1} für $l = 1, \ldots, p$ durch Adjunktion eines Eigenwertes einer symmetrischen K_{l-1}-Matrix hervorgeht. Unser Satz wird bewiesen sein, wenn wir gezeigt haben, daß ein Eigenwert einer symmetrischen K_l-Matrix auch schon Eigenwert einer symmetrischen K_{l-1}-Matrix ist.

Es sei also $K_l = K_{l-1}(\alpha)$, wo α Eigenwert einer s-reihigen symmetrischen K_{l-1}-Matrix A ist, und λ sei ein Eigenwert der r-reihigen symmetrischen K_l-Matrix $B = ((\alpha_{ik}))$. Wir konstruieren nun eine rs-reihige K_{l-1}-Matrix S, welche λ als Eigenwert hat.

Da $\alpha_{ik} \in K_{l-1}(\alpha)$, gibt es eine Darstellung

$$\alpha_{ik} = \sum_{\nu=0}^{n-1} c_{ik}^{(\nu)} \alpha^\nu \quad , \qquad c_{ik}^{(\nu)} \in K_{l-1} \ ,$$

und α_{ik} ist daher Eigenwert der symmetrischen K_{l-1}-Matrix

$$A_{ik} = \sum_{\nu=0}^{n-1} c_{ik}^{(\nu)} A^\nu \ .$$

$V_1^s, \ldots, V_r^s$ seien r isomorphe Exemplare eines s-dimensionalen Vektorraumes V^s (mit K_l als Koeffizientenbereich), und J_j sei ein Isomorphismus von V^s auf V_j^s, $j = 1, \ldots, r$. Wir deuten A als Matrix einer Abbildung $\mathfrak{A}$ von V^s in sich bezüglich einer Basis $(\mathfrak{e}_i)$ von V^s, und es sei

$$\mathfrak{A}_{ik} = \sum_{\nu=0}^{n-1} c_{ik}^{(\nu)} \mathfrak{A}^\nu \ .$$

Ferner sei $\mathfrak{x} \in V^s$ ein zum Eigenwert α gehöriger Eigenvektor von $\mathfrak{A}$ und $\mathfrak{x}_i \in V_i^s$ das J_i-Bild von $\mathfrak{x}$.

Wir betrachten nun die direkte Summe W^{rs} der Vektorräume $V_1^s, \ldots, V_r^s$ und definieren auf folgende Weise eine Abbildung $\mathfrak{S}$ von W^{rs} in sich:

Ist $\mathfrak{w}$ ein Vektor aus W^{rs} und $\mathfrak{w} = \mathfrak{v}_1 + \mathfrak{v}_2 + \cdots + \mathfrak{v}_r$, $\mathfrak{v}_j \in V_j^s$, seine Zerlegung in direkte Summanden, so sei:

$$\mathfrak{S}(\mathfrak{w}) = \sum_{i,k} J_i \mathfrak{A}_{ik} J_k^{-1}(\mathfrak{v}_k) \ .$$

In der Basis

$$(J_1\mathfrak{e}_1, \ldots, J_1\mathfrak{e}_s, J_2\mathfrak{e}_1, \ldots, J_2\mathfrak{e}_s, \ldots, J_r\mathfrak{e}_1, \ldots, J_r\mathfrak{e}_s)$$

des Raumes W^{rs} hat die rs-reihige Matrix S dieser Abbildung folgende Gestalt:

$$S = \begin{pmatrix} A_{11} & A_{12} \ldots A_{1r} \\ A_{21} & A_{22} \ldots A_{2r} \\ \vdots & \\ A_{r1} & A_{r2} \ldots A_{rr} \end{pmatrix}$$

S entsteht also aus B, wenn man an Stelle der Elemente α_{ik} die symmetrischen «Kästchen» A_{ik} einsetzt. Da auch $A_{ik} = A_{ki}$ ist, so folgt, daß S eine symmetrische K-Matrix ist. Diese Matrix S hat nun λ als Eigenwert. Es ist nämlich:

$$\begin{aligned}\mathfrak{S}(\mathfrak{x}_k) &= \sum_i J_i \mathfrak{A}_{ik} J_k^{-1}(\mathfrak{x}_k) = \sum_i J_i \mathfrak{A}_{ik}(\mathfrak{x}) \\ &= \sum_i J_i(\alpha_{ik}\mathfrak{x}) = \sum_i \alpha_{ik} J_i(\mathfrak{x}) = \sum_i \alpha_{ik}\mathfrak{x}_i \ .\end{aligned}$$

Das bedeutet aber, daß der von $\mathfrak{x}_1, \ldots, \mathfrak{x}_r$ als Basisvektoren aufgespannte Unterraum X^r durch $\mathfrak{S}$ in sich abgebildet wird, und, wenn wir mit $\mathfrak{B}$ die von $\mathfrak{S}$ in X^r induzierte Abbildung bezeichnen, daß die Matrix von $\mathfrak{B}$ bezüglich der Basis $(\mathfrak{x}_1, \ldots, \mathfrak{x}_r)$ gerade $B = ((\alpha_{ik}))$ ist. Ist nun $\mathfrak{y} \in X^r$ ein zum Eigenwert λ gehöriger Eigenvektor von $\mathfrak{B}$, so ist er natürlich auch Eigenvektor von $\mathfrak{S}$ mit demselben Eigenwert λ. Damit ist alles bewiesen.

§ 2. Quadratische Polynome und Irrationalitäten

Wir betrachten quadratische Polynome mit Koeffizienten aus einem Körper K, und zwar beliebige, wenn die Charakteristik $p \neq 2$, nur reinquadratische Polynome, wenn $p = 2$ ist. Solche Polynome können in der Form $f(x) = x^2 + 2ax + b$ angeschrieben werden. Wir fragen nun nach der notwendigen und hinreichenden Bedingung dafür, daß $f(x)$ Minimalpolynom einer symmetrischen K-Matrix ist.

Satz 2.1. *Ein quadratisches Polynom $f(x) = x^2 + 2ax + b$ ist dann und nur dann Minimalpolynom einer symmetrischen K-Matrix, wenn seine Diskriminante $a^2 - b$ Quadratsumme (von nicht-verschwindenden Körperelementen) ist.*

Beweis. Da $x^2 + 2ax + b = (x + a)^2 - (a^2 - b)$ ist, so genügt es, den Satz für reinquadratische Polynome $x^2 - c$ zu beweisen.

1. Die Bedingung ist notwendig.

Seien a_{ik} die Elemente von A; $i, k = 1, \ldots, n$. Ist $x^2 - c$ das Minimalpolynom von A, so ist $A^2 = cE$ (E Einheitsmatrix). Das Element in der i-ten Zeile und i-ten Kolonne von A^2 ist $a_{i1}^2 + a_{i2}^2 + \cdots + a_{in}^2 = c$; c ist also Quadratsumme in K von Elementen, die nicht alle $= 0$ sind.

2. Die Bedingung ist hinreichend.

Sei $c = u_1^2 + u_2^2 + \cdots + u_r^2$, $u_j \in K$, $u_j \neq 0$, $j = 1, \ldots, r$.
Ist die Charakteristik des Körpers 2, so ist $c = u_1^2 + \ldots + u_r^2 = (u_1^2 + \ldots + u_r)^2 = u^2$, und die zweireihige Matrix $\begin{pmatrix} 0 & u \\ u & 0 \end{pmatrix}$ hat die gewünschte Eigenschaft. Ist

die Charakteristik von K aber von 2 verschieden, so beweisen wir die Behauptung durch Induktion nach r. Für $r = 1, c = u_1^2$ hat die zweireihige Matrix

$$A_1 = \begin{pmatrix} u_1 & 0 \\ 0 & -u_1 \end{pmatrix}$$

das Minimalpolynom $x^2 - c$. Die Behauptung sei bewiesen für $r - 1$. Es seien $c' = u_1^2 + \ldots + u_{r-1}^2$ und A_{r-1} eine symmetrische s-reihige K-Matrix mit $A_{r-1}^2 = c'E'$ (E' s-reihige Einheitsmatrix). Wir bilden nun die $2s$-reihige symmetrische K-Matrix

$$A_r = \begin{pmatrix} u_r E' & A_{r-1} \\ A_{r-1} & -u_r E' \end{pmatrix} .$$

Es ist

$$A_r^2 = \begin{pmatrix} u_r^2 E' + A_{r-1}^2 & 0 \\ 0 & u_r^2 E' + A_{r-1}^2 \end{pmatrix}$$

$$= \begin{pmatrix} (u_1^2 + \ldots + u_{r-1}^2 + u_r^2)\, E' & 0 \\ 0 & (u_1^2 + \ldots + u_{r-1}^2 + u_r^2)\, E' \end{pmatrix} = cE .$$

A_r erfüllt daher die Gleichung $x^2 - c = 0$. Anderseits kommen in der Hauptdiagonalen von A_r die Elemente u_r und $-u_r$ vor, welche voneinander verschieden sind. Daher kann A_r nicht einer Gleichung $x - d = 0$ genügen; $x^2 - c$ ist also das Minimalpolynom von A_r.

Da die Wurzeln des Minimalpolynoms einer Matrix A die Eigenwerte von A sind, so folgt aus 2.1 unter Anwendung von 1.1:

Satz 2.2. *Ist $p \neq 2$, so ist jedes Element einer quadratischen Erweiterung L von K, deren Diskriminante Quadratsumme in K ist, Eigenwert einer symmetrischen K-Matrix.*

In nicht formal-reellen Körpern (d. h. -1 ist Quadratsumme) der Charak teristik $p \neq 2$ ist jedes Element Quadratsumme. Demnach ist in ihnen jedes quadratische Polynom Minimalpolynom einer symmetrischen Matrix. Ist $p = 2$, so ist jede Quadratsumme selbst ein Quadrat. Es kann aber Elemente geben, die keine Quadrate sind, wie z. B. das Element t im Körper $P_2(t)$, wo P_2 der Primkörper mod 2 und t eine Unbestimmte sind. Dementsprechend tritt auch nicht jedes quadratische Polynom als Minimalpolynom einer symmetrischen $P_2(t)$-Matrix auf. Dagegen gilt noch:

Satz 2.21. *Ist $p = 2$, so ist jede Quadratwurzel Eigenwert einer symmetrischen K-Matrix.*

Beweis. Ist $\gamma^2 = c$, so ist γ Eigenwert von

$$C = \begin{pmatrix} 0 & c & 1 \\ c & c & c+1 \\ 1 & c+1 & 1 \end{pmatrix} ,$$

denn das charakteristische Polynom von C ist $\chi(x) = (x^2 + c)(x + c + 1)$, und C ist symmetrisch.

Bemerkung. Für den Körper der rationalen Zahlen kann man auf Grund des von Legendre bewiesenen Satzes, wonach jede natürliche Zahl $\not\equiv 0, 4, 7 \pmod 8$ Summe von 3 Quadraten ist (vgl. [5]), zeigen:

2.3 Jede reelle algebraische (ganz-algebraische) Zahl zweiten Grades ist Eigenwert einer 3-reihigen rationalzahligen (ganzzahligen) symmetrischen Matrix, und jedes quadratische Polynom mit rationalen (ganz-rationalen) Koeffizienten und positiver Diskriminante ist Minimalpolynom einer 4-reihigen rationalzahligen (ganzzahligen) symmetrischen Matrix. Im allgemeinen kommt man aber mit weniger Reihen als eben angegeben nicht aus.

§3. Charakterisierung der Eigenwerte und Minimalpolynome beliebigen Grades

Wir geben in diesem Abschnitt die in der Einleitung angekündigte Charakterisierung der Eigenwerte und Minimalpolynome symmetrischer Matrizen mit Elementen aus einem beliebigen Körper. Vorerst beweisen wir zwei Hilfssätze.

Hilfssatz 3.1.

Es seien:

K *ein Körper;*

Ω *eine algebraisch-abgeschlossene Erweiterung von* K*;*

$f(x) = x^n + a_1 x^{n-1} + \dots$ *ein Polynom* n*-ten Grades aus* $K[x]$ *mit den Wurzeln* $\alpha_1, \dots, \alpha_n$*;*

$g(x) = x^{n-1} + b_1 x^{n-1} + \dots$ *ein Polynom* $(n-1)$*-ten Grades aus* $K[x]$ *mit lauter einfachen Wurzeln* $\beta_1, \dots, \beta_{n-1}$*;*

$$c_j = -\frac{f(\beta_j)}{\prod\limits_{k \neq j}^{n-1} (\beta_j - \beta_k)} \quad \textit{und} \quad \gamma_j^2 = c_j\,;$$

$f(x) = (x - a)\,g(x) + r(x)$, *wobei* $a \in K$ *und* $r(x)$ *ein Polynom von höchstens* $(n-2)$*-tem Grad ist.*

Dann hat die symmetrische Matrix

$$M = \begin{pmatrix} a & \gamma_1 & \cdot & \cdot & \cdot & \gamma_{n-1} \\ \gamma_1 & \beta_1 & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & & \cdot & \cdot \\ \vdots & \vdots & & \vdots & \cdot & 0 \\ \gamma_{n-1} & 0 & & \cdot & 0 & \beta_{n-1} \end{pmatrix}$$

das charakteristische Polynom $\chi_M(x) = (-1)^n f(x)$.

Zusatz. *Ist* $\beta_j \neq \alpha_k$ *für alle* j, k, *dann ist* $\chi_M(x)$ *zugleich das Minimalpolynom von* M.

Beweis. Es ist

$$\chi_M(x) = (a - x)(\beta_1 - x)\ldots(\beta_{n-1} - x) - \sum_{i=1}^{n-1} c_i \prod_{k\neq i}^{n-1} (\beta_k - x) =$$
$$(-1)^n (x - a)\, g(x) - (-1)^{n-2} \sum_{i=1}^{n-1} c_i \prod_{k\neq i}^{n-1} (x - \beta_k) =$$
$$(-1)^n \Big[(x - a)\, g(x) - \sum_{i=1}^{n-1} c_i \prod_{k\neq i}^{n-1} (x - \beta_k)\Big] . \qquad (1)$$

Sei

$$h(x) = - \sum_{i=1}^{n-1} c_i \prod_{k\neq i}^{n-1} (x - \beta_k) .$$

Es ist dann

$$h(\beta_j) = - c_j \prod_{k\neq j}^{n-1} (\beta_j - \beta_k) = f(\beta_j); \quad j = 1, \ldots, n-1 .$$

Da auch

$$f(\beta_j) = r(\beta_j); \quad j = 1, \ldots, n-1$$

und $r(x)$ höchstens vom Grade $n-2$ ist, so folgt, daß $h(x) = r(x)$, und daher stimmt das Polynom in den eckigen Klammern von (1) überein mit $f(x)$.

Zum Beweise des Zusatzes haben wir zu zeigen, daß der größte gemeinsame Teiler aller $(n-1)$-reihigen Unterdeterminanten der charakteristischen Matrix $M - xE$ gleich 1 ist (vgl. [4], S. 20). Sei $D_k(x)$ diejenige $(n-1)$-reihige Unterdeterminante von $M - xE$, welche aus dieser durch Streichen der ersten Zeile und der $(k+1)$-ten Kolonne hervorgeht. Es ist:

$$D_k(x) = \pm \gamma_k (\beta_1 - x)(\beta_2 - x)\ldots(\beta_{k-1} - x)(\beta_{k+1} - x)\ldots(\beta_{n-1} - x) .$$

Weil $\beta_k \neq \alpha_i$ für $i = 1, \ldots, n$, so ist $f(\beta_k) \neq 0$ und daher auch $\gamma_k \neq 0$. Da auch $\beta_j \neq \beta_k$ für $j \neq k$, so ist $D_k(x)$ nicht teilbar durch $\beta_k - x$. Mithin ist der größte gemeinsame Teiler von $D_1(x), \ldots, D_{n-1}(x)$ und daher auch aller $(n-1)$-reihigen Unterdeterminanten von $M - xE$ gleich 1.

Für die im folgenden verwendeten Begriffe und Sätze aus der Theorie der formal-reellen Körper verweisen wir auf [1] und [2] oder auch [3].

Hilfssatz 3.2.

Es seien:

K ein formal-reeller Körper;

Ω eine algebraisch-abgeschlossene Erweiterung von K;

Δ der Körper der total-reellen Elemente von Ω[2]*;*

$f(x) = x^n + a_1 x^{n-1} + \ldots$ ein Polynom aus $K[x]$ mit lauter verschiedenen und total-reellen Wurzeln $\alpha_1, \ldots, \alpha_n$;

$f'(x)$ die Ableitung von $f(x)$ und $\beta_1, \ldots, \beta_{n-1}$ ihre Wurzeln;

$$L = K(\beta_1, \ldots, \beta_{n-1}) \quad \textit{und} \quad c_j = - \frac{f(\beta_j)}{\prod_{k\neq j}^{n-1} (\beta_j - \beta_k)} .$$

---

[2]) Das heißt, Δ ist der Durchschnitt aller reell-abgeschlossenen Erweiterungen von K.

Dann ist L formal-reell, $L \subset \Delta$, und die $n-1$ Größen $c_j \in L$ sind total-positiv.

Beweis. Nach dem Rolleschen Theorem liegen $\beta_1, \ldots, \beta_{n-1}$ in Δ. L ist daher in Δ enthalten und mithin auch formal-reell. Wir haben noch zu beweisen, daß c_j in jeder Anordnung von L positiv ist. Da jede Anordnung von L Anlaß zu einer angeordneten reell-abgeschlossenen Erweiterung gibt, welche Δ enthält und deren Anordnung diejenige von L fortsetzt, so wird die Behauptung bewiesen sein, wenn wir gezeigt haben, daß c_j in jeder Anordnung von Δ positiv ist.

Da eine Änderung der Numerierung der Größen α_i und β_j nur eine Permutation der Größen c_j unter sich bewirkt, so können wir ohne Einschränkung der Allgemeinheit annehmen, daß in der betrachteten Anordnung von Δ gilt:

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \ldots < \alpha_{n-1} < \beta_{n-1} < \alpha_n \ .$$

Es ist

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$$

und somit

$$f(\beta_j) = (\beta_j - \alpha_1)(\beta_j - \alpha_2) \ldots (\beta_j - \alpha_n) \ .$$

Da

$$\beta_j < \alpha_k \quad \text{für} \quad k > j \quad \text{und} \quad \beta_j > \alpha_k \quad \text{für} \quad k \leqslant j \ ,$$

ist

$$sg f(\beta_j) = sg\,(\beta_j - \alpha_{j+1}) \ldots (\beta_j - \alpha_n) = (-1)^{n-j} \ .$$

Ebenso

$$sg \prod_{k \neq j}^{n-1} (\beta_j - \beta_k) = sg(\beta_j - \beta_{j+1}) \ldots (\beta_j - \beta_{n-1}) = (-1)^{n-1-j}$$

Daher ist $sg c_j = +1$ und somit $c_j > 0$ in jeder Anordnung von Δ.

Wir sind nun imstande, unser Problem für die Eigenwerte symmetrischer K-Matrizen zu lösen.

Satz 3.3. *Sei Ω die algebraische, algebraisch-abgeschlossene Erweiterung des Körpers K. Ist K formal-reell, so ist $\lambda \in \Omega$ dann und nur dann Eigenwert einer symmetrischen K-Matrix, wenn λ total-reell ist; ist aber K nicht formal-reell, so ist jedes Element von Ω Eigenwert einer symmetrischen K-Matrix.*

Das bedeutet, daß der Körper aller Eigenwerte symmetrischer K-Matrizen im nicht formal-reellen Fall algebraisch-abgeschlossen ist und im formal-reellen Fall mit dem Durchschnitt aller reell-abgeschlossenen Erweiterungen von K übereinstimmt.

Beweis. Ist L ein formal-reeller Körper und liegen die Eigenwerte der symmetrischen L-Matrix A in $L(i)$, $i = \sqrt{-1}$, so liegen sie, wie bekannt, auch schon in L. Ist L Unterkörper von Ω und reell-abgeschlossen, so ist $L(i) = \Omega$.

Somit gehören die Eigenwerte jeder symmetrischen K-Matrix, wenn K formal-reell ist, zu allen reell-abgeschlossenen Erweiterungskörpern von K in Ω. Die Bedingung ist daher notwendig.

Den Beweis der Umkehrung führen wir durch Induktion nach dem Grad n von λ über K. Für $n = 1$ ist die Behauptung trivial. Sie sei bewiesen für $n - 1$. Ist $f(x)$ das irreduzible Polynom, von welchem λ eine Nullstelle ist, so betrachten wir die Matrix

$$M = \begin{pmatrix} a & \gamma_1 & \cdots & \gamma_{n-1} \\ \gamma_1 & \beta_1 & 0 \, . \, . & 0 \\ . & 0 & . \; . & . \\ \vdots & \vdots & \vdots \; . & 0 \\ \gamma_{n-1} & 0 & . \, . \; 0 & \beta_{n-1} \end{pmatrix}.$$

Die Größen $a, \beta_1, \ldots, \beta_{n-1}$ und $\gamma_1, \ldots, \gamma_{n-1}$ sollen dabei dieselbe Bedeutung haben wie in den Hilfssätzen 3.1 und 3.2. Im formal-reellen Fall sind $\beta_1, \ldots, \beta_{n-1}$ die Wurzeln der Ableitung $f'(x)$ und sind total-reell, a ist in K und $\gamma_1, \ldots, \gamma_{n-1}$ sind nach 3.2 Quadratwurzeln aus total-positiven Elementen von $K(\beta_1, \ldots, \beta_{n-1})$. Ist K nicht formal-reell, so sind $\beta_1, \ldots, \beta_{n-1}$ die (lauter einfachen) Wurzeln irgendeines Polynoms $(n - 1)$-ten Grades, und $\gamma_1, \ldots, \gamma_{n-1}$ sind Quadratwurzeln aus Elementen von $K(\beta_1, \ldots, \beta_{n-1})$. In einem formal-reellen Körper sind die total-positiven und in einem nicht formal-reellen Körper der Charakteristik $p \neq 2$ alle Elemente Quadratsummen (vgl. [2], S. 103; [3], S. 248); demnach sind nach 2.2 und für die Charakteristik 2 nach 2.21 sämtliche γ_i Eigenwerte symmetrischer $K(\beta_1, \ldots, \beta_{n-1})$-Matrizen. Da $\pm f(x)$ nach 3.1 das charakteristische Polynom von M ist, so ist λ Eigenwert von M. M ist symmetrisch, und seine Elemente sind Eigenwerte symmetrischer $K(\beta_1, \ldots, \beta_{n-1})$-Matrizen. Mithin ist auch λ nach 1.3 Eigenwert einer symmetrischen $K(\beta_1, \ldots, \beta_{n-1})$-Matrix. Da $\beta_1, \ldots, \beta_{n-1}$ über K höchstens den Grad $n - 1$ haben, so sind die Elemente dieser Matrix nach Induktionsvoraussetzung Eigenwerte symmetrischer K-Matrizen; nach 1.3 ist daher auch λ ein solcher Eigenwert. Damit ist der Satz bewiesen.

Bemerkung. Ist K der Körper der rationalen Zahlen, so läßt sich der Beweis infolge der Eigenschaft, daß sich die reellen Wurzeln eines Polynoms durch rationale Zahlen voneinander trennen lassen, vereinfachen. Es genügt nämlich, um reelle $\gamma_1, \ldots, \gamma_{n-1}$ zu erhalten, welche dann Eigenwerte symmetrischer rationaler Matrizen sind, für $\beta_1, \ldots, \beta_{n-1}$ rationale Zahlen zu nehmen, welche zwischen je zwei Wurzeln von $f(x)$ liegen. Die Induktion fällt weg, und eine einmalige Anwendung von 1.3 liefert das Gewünschte. Dieser Schluß versagt hingegen in allgemeinen formal-reellen Körpern, wo es nicht immer möglich ist, die in einer rell-abgeschlossenen Erweiterung liegenden Wurzeln eines Polynoms durch Elemente aus dem Grundkörper zu trennen (vgl. [1], S. 99).

Der folgende Satz erlaubt die Beantwortung der Frage nach der Charakterisierung der Minimalpolynome symmetrischer K-Matrizen. Wir betrachten dabei endliche Erweiterungen $K(\alpha_1, \ldots, \alpha_r)$ von K und fragen nach den Bedingungen, unter denen der Körper $K(\alpha_1, \ldots, \alpha_r)$ eine Darstellung durch symmetrische K-Matrizen, kurz, eine symmetrische K-Darstellung, besitzt. Eine solche Darstellung besteht aus einem Matrixring $K[A_1, \ldots, A_r]$, wo $A_1, \ldots, A_r$ symmetrische K-Matrizen sind, und einem Homomorphismus von $K(\alpha_1, \ldots, \alpha_r)$ auf $K[A_1, \ldots, A_r]$, welcher, da $K(\alpha_1, \ldots, \alpha_r)$ ein Körper ist, zu einem Isomorphismus wird.

Satz 3.4. *Ist K formal-reell, so gibt es dann und nur dann eine symmetrische K-Darstellung der endlichen Erweiterung $K(\alpha_1, \ldots, \alpha_r)$, wenn die r adjungierten Elemente $\alpha_1, \ldots, \alpha_r$ total-reell sind; ist K nicht formal-reell, seine Charakteristik aber von 2 verschieden, so besitzt jede endliche Erweiterung $K(\alpha_1, \ldots, \alpha_r)$ eine symmetrische K-Darstellung.*

Beweis. Daß, im formal-reellen Fall, die Bedingung notwendig ist, folgt sofort aus 3.3; denn ist A_i die dem Element α_i in der Darstellung entsprechende Matrix, so ist α_i Eigenwert von A_i, nach 3.3 also total-reell.

Den Beweis des Satzes in der umgekehrten Richtung zerlegen wir in drei Schritte. Wir zeigen der Reihe nach:

1. Ist der Satz richtig für eine einfache Erweiterung vom Grade $\leqslant n$, so ist er auch richtig für jede endliche Erweiterung, vorausgesetzt, daß der Grad sämtlicher adjungierter Elemente über K nicht größer als n ist.

2. Der Satz ist richtig, wenn die adjungierten Elemente Quadratwurzeln sind.

3. Der Satz ist richtig für eine einfache Erweiterung.

Zu 1. Wir führen den Beweis des ersten Schrittes durch Induktion nach r. $\alpha_1, \ldots, \alpha_r$ seien algebraische Elemente, welche unsere Voraussetzungen erfüllen und deren Grade über K nicht größer sind als n. Für $r = 1$ ist die Behauptung trivial. Sie sei bewiesen für $r - 1$, d. h. wir nehmen an, es existieren $r - 1$ symmetrische K-Matrizen $\bar{A}_1, \ldots, \bar{A}_{r-1}$ und ein Isomorphismus J von $K(\alpha_1, \ldots, \alpha_{r-1})$ auf $K[\bar{A}_1, \ldots, \bar{A}_{r-1}]$. Der Grad g von α_r über $L = K(\alpha_1, \ldots, \alpha_{r-1})$ ist nicht größer als der Grad von α_r über K. Mithin ist $g \leqslant n$. Ist K formal-reell, so ist es auch L. Da der Satz für einfache Erweiterungen vom Grade $\leqslant n$ richtig sein soll, so gibt es eine symmetrische L-Matrix $\tilde{A}_r = ((\alpha_{ik}))$, derart, daß $L(\alpha_r) \cong L[\tilde{A}_r]$ ist. $\tilde{A}_r$ habe m-Reihen, und es sei $J(\alpha_{ik}) = \bar{A}_{ik}$. Die Matrix

$$A_r = \begin{pmatrix} \bar{A}_{11} & \dots & \bar{A}_{1m} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \bar{\cdot} & & \bar{\cdot} \\ \bar{A}_{1m} & \dots & \bar{A}_{mm} \end{pmatrix}$$

ist eine symmetrische $K[\bar{A}_1, \dots, \bar{A}_{r-1}]$-Matrix, und es gilt

$$L[\tilde{A}_r] \cong K[\bar{A}_1, \dots, \bar{A}_{r-1}][A_r] .$$

Ist E die m-reihige $K[\bar{A}_1, \dots, \bar{A}_{r-1}]$-Einheitsmatrix, so sei

$$A_j = \bar{A}_j E \quad \text{für} \quad j = 1, \dots, r-1 .$$

Da die Elemente von $A_1, \dots, A_r$ symmetrische K-Matrizen sind, so können auch $A_1, \dots, A_r$ selbst als symmetrische K-Matrizen betrachtet werden.

Es ist dann

$$K[\bar{A}_1, \dots, \bar{A}_{r-1}][A_r] \cong K[A_1, \dots, A_{r-1}, A_r] ,$$

also

$$K(\alpha_1, \dots, \alpha_{r-1}, \alpha_r) = L(\alpha_r) \cong L[\tilde{A}_r] \cong K[A_1, \dots, A_{r-1}, A_r] .$$

Damit ist unsere Behauptung bewiesen.

Zu 2. Sind K formal-reell, $c \in K$, γ total-reell und $\gamma^2 = c$, so ist c total-positiv und somit Quadratsumme in K. Ist K nicht formal-reell, seine Charakteristik aber $\neq 2$, so ist jedes Element $c \in K$ Quadratsumme. Nach 2.1 gibt es in beiden Fällen eine symmetrische K-Matrix C mit $x^2 - c$ als Minimalpolynom. Infolgedessen ist $K(\gamma) \cong K[C]$. Sind nun $c_1, \dots, c_r \in K$, $\gamma_1^2 = c_1, \dots, \gamma_r^2 = c_r$ und $\gamma_1, \dots, \gamma_r$ total-reell, wenn K formal-reell ist, so gibt es, nach dem unter 1. bewiesenen angewendet für $n = 2$, r symmetrische K-Matrizen $C_1, \dots, C_r$, so daß $K(\gamma_1, \dots, \gamma_r) \cong K[C_1, \dots, C_r]$, was zu beweisen war.

Zu 3. Sei α algebraisch über K vom Grade n und total-reell, wenn K formal-reell ist. $f(x) = 0$ sei die irreduzible Gleichung, welcher α genügt. Wir haben nachzuweisen, daß eine symmetrische Matrix A existiert, derart, daß $K(\alpha) \cong K[A]$ oder, was auf dasselbe herauskommt, daß $f(x)$ das Minimalpolynom von A ist.

Für $n = 1$, d. h. wenn α in K liegt, ist die Behauptung trivial. Sie sei bewiesen für alle algebraischen Elemente, deren Grade über K kleiner als n sind. Wir betrachten nun wieder die mit Hilfe von $f(x)$ konstruierte symmetrische Matrix

$$M = \begin{pmatrix} a & \gamma_1 & \dots & \gamma_{n-1} \\ \gamma_1 & \beta_1 & 0 \, . \, . & 0 \\ . & 0 & . \quad . & . \\ \vdots & \vdots & \vdots \quad . & 0 \\ \gamma_{n-1} & 0 & . \, . \, 0 & \beta_{n-1} \end{pmatrix},$$

wo $a, \gamma_1, \ldots, \gamma_{n-1}, \beta_1, \ldots, \beta_{n-1}$ dieselbe Bedeutung haben sollen wie im Beweis von Satz 3.3. Ist $L = K(\beta_1, \ldots, \beta_{n-1})$, so gibt es nach dem unter 2. bewiesenen $n-1$ symmetrische L-Matrizen $C_1, \ldots, C_{n-1}$, so daß $L(\gamma_1, \ldots, \gamma_{n-1}) \cong L[C_1, \ldots, C_{n-1}]$.

Ersetzen wir in M die Matrixelemente durch die ihnen in $L[C_1, \ldots, C_{n-1}]$ entsprechenden symmetrischen L-Matrizen, so erhalten wir eine symmetrische Matrix:

$$M_L = \begin{pmatrix} \alpha E & C_1 & \ldots & C_{n-1} \\ C_1 & \beta_1 E & 0 \,.\,. & 0 \\ . & 0 & & . \\ \vdots & \vdots & & 0 \\ C_{n-1} & 0 & \,.\,.\, 0 & \beta_{n-1} E \end{pmatrix},$$

deren Elemente nun in L liegen. E ist dabei die Einheitsmatrix in $L[C_1, \ldots, C_{n-1}]$. Da $L(\gamma_1, \ldots, \gamma_{n-1}) \cong L[C_1, \ldots, C_{n-1}]$, ist das Minimalpolynom von M_L dasselbe wie dasjenige von M; dieses ist aber $f(x)$, denn $f(x)$ ist irreduzibel und charakteristisches Polynom von M.

Nun haben die Elemente $\beta_1, \ldots, \beta_{n-1}$ über K höchstens den Grad $n-1$, und sie erfüllen die Voraussetzungen von Satz 3.4. Nach Induktionsvoraussetzung besitzt eine einfache Erweiterung von K, deren Grad $n-1$ ist, eine symmetrische K-Darstellung. Mithin gibt es nach dem unter 1. bewiesenen auch eine symmetrische K-Darstellung $K[B_1, \ldots, B_{n-1}]$ von $K(\beta_1, \ldots, \beta_{n-1})$.

Ersetzen wir nun in gleicher Weise wie oben die Elemente von M_L durch die ihnen in $K[B_1, \ldots, B_{n-1}]$ entsprechenden symmetrischen K-Matrizen, so erhalten wir eine neue symmetrische Matrix M_K, deren Elemente aus K stammen. Weil $K(\beta_1, \ldots, \beta_{n-1}) \cong K[B_1, \ldots, B_{n-1}]$ ist, so haben M_K und M_L das gleiche Minimalpolynom. Damit ist aber eine symmetrische K-Matrix, nämlich M_K gefunden, deren Minimalpolynom $f(x)$ ist, so daß alles bewiesen ist.

Es folgt nun ohne weiteres der

Satz 3.5. *Ist K formal-reell, so ist ein Polynom dann und nur dann Minimalpolynom einer symmetrischen K-Matrix, wenn seine Wurzeln einfach und totalreell sind; ist K nicht formal-reell und seine Charakteristik $p \neq 2$, so ist jedes Polynom Minimalpolynom einer symmetrischen K-Matrix.*

Beweis. Für irreduzible Polynome ergibt sich der Satz sofort aus 3.4. Er bleibt daher nur noch für reduzible Polynome zu beweisen.

Da eine symmetrische Matrix mit Elementen aus einem formal-reellen Körper K innerhalb jeder rell-abgeschlossenen Erweiterung von K auf Diagonalform transformiert werden kann, so ist die Bedingung notwendig.

Für die Umkehrung beachten wir, daß sich in nicht formal-reellen Körpern der Charakteristik $p \neq 2$ zu jedem Polynom $f(x)$ ein Polynom $g(x)$ finden läßt, welches die Voraussetzungen von Hilfssatz 3.1 und seinem Zusatz erfüllt. Ist K formal-reell, so sei $g(x) = f'(x)$. In beiden Fällen hat die nach 2.1 mit Hilfe von $f(x)$ und $g(x)$ konstruierte symmetrische Matrix M das Minimalpolynom $f(x)$. Die Elemente von M erfüllen die Voraussetzungen von Satz 3.4. Somit besitzt der aus K durch Adjunktion dieser Elemente entstehende Erweiterungskörper L eine symmetrische K-Darstellung D. Da $L \cong D$, hat die der symmetrischen L-Matrix M entsprechende symmetrische D-Matrix $\bar{M}$ dasselbe Minimalpolynom wie M, also $f(x)$. Jede symmetrische D-Matrix kann aber auch als symmetrische K-Matrix aufgefaßt werden. Damit ist der Satz bewiesen.

Bemerkungen:

3.51. Wie wir schon in § 2 gesehen haben, ist Satz 3.5 ohne die Voraussetzung $p \neq 2$ nicht richtig.

3.52. Im Körper der rationalen Zahlen gelten auf Grund von 2.3 die folgenden Abschätzungen:

Ist r die Zeilenzahl der kleinsten symmetrischen Matrix, von welcher λ ein Eigenwert ist, und ist n der Grad von λ, so ist $r \leqslant n \cdot 3^{n-1}$.

Ist s die Zeilenzahl der kleinsten symmetrischen Matrix, von der $f(x)$ Minimalpolynom ist, und ist n der Grad von $f(x)$, so ist $s \leqslant n \cdot 4^{n-1}$.

§ 4. Schiefsymmetrische und orthogonale Matrizen

Auf Grund der Ergebnisse des vorhergehenden Abschnittes sind wir nun imstande, die entsprechenden Fragen für schiefsymmetrische und orthogonale Matrizen zu beantworten. Im folgenden sei die Charakteristik der betrachteten Körper, ohne ausdrückliche Nennung, als $\neq 2$ vorausgesetzt. Wir behandeln zuerst den Fall der schiefsymmetrischen Matrizen.

Diejenigen Polynome $f(x)$ aus $K[x]$, welche als Minimalpolynome schiefsymmetrischer K-Matrizen auftreten können, haben entweder die Gestalt $f(x) = g(x^2)$ oder $f(x) = xg(x^2)$. Ist nämlich $f(x)$ das Minimalpolynom der schiefsymmetrischen K-Matrix S, so ist $f(S)^* = f(S^*) = f(-S) = 0$, wenn mit A^* die Transponierte einer Matrix A bezeichnet wird. Bedeutet n den Grad von $f(x)$, so ist $f(S) + (-1)^{n-1} f(-S) = 0$. Da der Grad von $f(x) + (-1)^{n-1} f(-x)$ kleiner als n, anderseits $f(x)$ das Minimalpolynom von S ist, so muß $f(x) + (-1)^{n-1} f(-x)$ identisch verschwinden. Somit ist, wenn n gerade ist, $f(-x) = f(x)$, also $f(x) = g(x^2)$ und anderseits, wenn n ungerade ist, $f(-x) = -f(x)$, also $f(x) = xg(x^2)$.

Ist K formal-reell und Δ der Körper der total-reellen Elemente der algebraischen, algebraisch-abgeschlossenen Erweiterung Ω von K, so sei $\Gamma = \Delta(i)$

der aus Δ durch Adjunktion einer Wurzel von $x^2 + 1 = 0$ erhaltene Erweiterungskörper. Jedes Element λ von Γ läßt sich in der Form $\lambda = \alpha + \beta i$, $\alpha, \beta \in \Delta$, darstellen. Ist $\alpha = 0$, so soll λ total-imaginär heißen.

Bezeichnen wir mit $s(x)$ ein Polynom aus $K[x]$, welches sich entweder in der Form $g(x^2)$ oder in der Form $xg(x^2)$ schreiben läßt, so lautet nun der 3.5 entsprechende Satz für schiefsymmetrische Matrizen:

Satz 4.1. *Ist K formal-reell, so ist ein Polynom $s(x)$ dann und nur dann Minimalpolynom einer schiefsymmetrischen K-Matrix, wenn seine Wurzeln einfach und total-imaginär sind; ist K nicht formal-reell, so ist jedes Polynom $s(x)$ Minimalpolynom einer solchen Matrix.*

Beweis.

1. Die Bedingung ist notwendig im Falle eines formal-reellen Körpers. Sei $s(x)$ das Minimalpolynom der schiefsymmetrischen K-Matrix S und sei $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Das Kroneckerprodukt $T = J \times S$ ist symmetrisch und $T^2 = (J \times S)^2 = E \times (-S^2)$ (E Einheitsmatrix). Für das Minimalpolynom $t(x)$ von T gilt daher $t(x) = g(-x^2)$ oder $t(x) = xg(-x^2)$, je nachdem $s(x) = g(x^2)$ oder $s(x) = xg(x^2)$ ist. Ist β Wurzel von $t(x)$, so ist βi Wurzel von $s(x)$ und umgekehrt. Da die Wurzeln von $t(x)$ total-reell und einfach sind, so sind die Wurzeln von $s(x)$ total-imaginär und ebenfalls einfach.

2. Die Bedingung ist hinreichend. Da $s(x)$ im formal-reellen Fall lauter verschiedene und total-imaginäre Wurzeln haben soll, so sind die Wurzeln von $g(-x^2)$ bzw. $xg(-x^2)$ total-reell und ebenfalls einfach. Nach 3.5 gibt es in beiden Fällen eine symmetrische K-Matrix A, deren Minimalpolynom $g(-x^2)$ bzw. $xg(-x^2)$ ist. Nun ist $S = J \times A$ schiefsymmetrisch, und das Minimalpolynom von S ist $s(x)$.

Wenn K nicht formal-reell ist, so tritt jedes Element von Ω als Wurzel eines Polynoms $s(x)$ auf. Daher:

Satz 4.2. *Ist K formal-reell, so sind die total-imaginären Elemente von Ω, und nur diese, Eigenwerte schiefsymmetrischer K-Matrizen; ist K nicht formal-reell, so ist jedes Element von Ω Eigenwert einer solchen Matrix.*

Wir betrachten nun noch orthogonale K-Matrizen. Als Minimalpolynome können in diesem Fall nur solche Polynome auftreten, welche sich in der Gestalt $q(x) = x^m (x+1)^\delta (x-1)^\varepsilon g\left(x + \frac{1}{x}\right)$, wo δ, ε entweder 0 oder 1 sind, schreiben lassen. Ist nämlich Q eine orthogonale K-Matrix mit dem Minimalpolynom $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_n = 1$, so gilt: $\sum_{k=0}^{n} a_k Q^k = 0$ und $\sum_{k=0}^{n} a_k Q^{*k} = \sum_{k=0}^{n} a_k Q^{-k} = 0$. Die Multiplikation der letzten Gleichung mit Q^n ergibt:

$\sum\limits_{k=0}^{n} a_k Q^{n-k} = 0$ oder, nach Änderung des Summationsindexes: $\sum\limits_{k=0}^{n} a_{n-k} Q_k = 0$. Daher ist: $\sum\limits_{k=0}^{n} (a_k - a_{n-k})\, Q^k = 0$. Da $\sum\limits_{k=0}^{n} a_k x^k$ das Minimalpolynom von Q ist, so folgt: $a_k - a_{n-k} = \mu a_k$ für $k = 0, 1, \ldots, n$ und daraus $a_k(1-\mu) = a_{n-k}$ und $a_{n-k}(1-\mu) = a_k$, also $a_{n-k}(1-\mu)^2 = a_{n-k}$. Für $k = 0$ ergibt sich: $(1-\mu)^2 = 1$, also $\mu = 0$ oder $\mu = 2$, mithin $a_k = a_{n-k}$ oder $a_k = -a_{n-k}$. Ein Polynom, dessen Koeffizienten diese Eigenschaften haben, läßt sich aber immer in der Form $q(x)$ schreiben.

Es gilt nun:

Satz 4.3. *Ist K formal-reell, so ist ein Polynom $q(x)$ dann und nur dann Minimalpolynom einer orthogonalen K-Matrix, wenn seine Wurzeln in Γ liegen, einfach sind und über Δ die Norm 1 haben; ist K nicht formal-reell, so ist jedes Polynom $q(x)$ Minimalpolynom einer solchen Matrix.*

Beweis.

1. Die Bedingung ist im formal-reellen Fall notwendig. Ist $q(x)$ das Minimalpolynom der orthogonalen K-Matrix Q und λ eine Wurzel von $q(x)$, so ist λ Eigenwert von Q. Die Matrix $Q + Q^*$ ist symmetrisch, und $\lambda + \lambda^{-1}$ ist wegen $Q^* = Q^{-1}$ Eigenwert von $Q + Q^*$. Ebenso ist $\lambda - \lambda^{-1}$ Eigenwert der schiefsymmetrischen K-Matrix $Q - Q^*$. Setzen wir $2\alpha = \lambda + \lambda^{-1}$ und $2\beta i = \lambda - \lambda^{-1}$, so sind α und β nach 3.3 und 4.2 total-reell. Da $\lambda = \alpha + \beta i$ und $\lambda^{-1} = \alpha - \beta i$ wird, so ist $\alpha^2 + \beta^2 = 1$; mithin ist $\lambda \in \Gamma$, und seine Norm über Δ ist 1. Da des weiteren Q innerhalb Ω auf Diagonalform transformiert werden kann, sind die Wurzeln von $q(x)$ einfach.

2. Die Bedingung ist hinreichend.

Sei K vorerst formal-reell. Wir unterscheiden 2 Fälle:

a) $q(x)$ ist irreduzibel. Hat $q(x)$ den Grad $n = 1$, so ist die Behauptung trivial. Ist $n \geqslant 2$, so ist $q(x) = x^m g\left(x + \frac{1}{x}\right)$, wobei $g(y)$ vom Grade $m = \frac{n}{2}$, irreduzibel ist und lauter total-reelle Wurzeln hat. Ist $\lambda = \alpha + \beta i$ Wurzel von $q(x)$, so ist 2α Wurzel von $g(y)$. Da α und β total-reell sind, gibt es nach 3.4 eine Darstellung des Körpers $K(\alpha, \beta)$ durch symmetrische K-Matrizen. In dieser seien $\bar{A}$ und $\bar{B}$ die den Elementen α und β entsprechenden symmetrischen K-Matrizen. Da nach Voraussetzung $\alpha^2 + \beta^2 = 1$, so ist $\bar{A}^2 + \bar{B}^2 = \bar{E}$ ($\bar{E}$ Einheitsmatrix). Seien $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $A = E_2 \times \bar{A}$ und $B = J \times \bar{B}$. Da $\bar{A}\bar{B} = \bar{B}\bar{A}$, so ist $AB = BA$. Die K-Matrix $Q = A + B$ ist orthogonal, denn A ist symmetrisch, B schiefsymmetrisch und $QQ^* = (A + B)(A - B) = A^2 - B^2 = E$. Da $g(2A) = 0$ ist, ist

$$q(Q) = Q^m g\,(Q + Q^{-1}) = Q^m g\,(Q + Q^*) = Q^m g(2A) = 0\ .$$

Somit ist $q(x)$ das Minimalpolynom von Q.

b) $q(x)$ ist reduzibel. Sei $q(x) = q_1(x) \ldots q_r(x)$, wo $q_i(x) = x^{m_i} g_i\left(x + \frac{1}{x}\right)$ oder $= x \pm 1$, seine Zerlegung in lauter verschiedene irreduzible Faktoren. Zu jedem $q_i(x)$ gibt es nach a) ein orthogonales Q_i, welches $q_i(x)$ als Minimalpolynom hat. Dann ist $q(x)$ das Minimalpolynom der direkten Summe

$$Q = Q_1 \dot{+} Q_2 \dot{+} \cdots \dot{+} Q_r \,.$$

Sei nun K nicht formal-reell. Wir unterscheiden 3 Fälle:

a) $q(x)$ habe keine Wurzeln $+1$ oder -1. Dann ist $q(x) = x^m g\left(x + \frac{1}{x}\right)$. Nach 3.5 gibt es symmetrische K-Matrizen $\bar{A}$ und I derart, daß $g(y)$ Minimalpolynom von $2\bar{A}$ und $y^2 + 1$ Minimalpolynom von I ist. Dabei können $\bar{A}$ und I als vertauschbar angenommen werden. Es seien nun $\bar{B} = \begin{pmatrix} \bar{E} & I\bar{A} \\ I\bar{A} & -\bar{E} \end{pmatrix}$, $\bar{E}$ Einheitsmatrix, $B = J \times \bar{B}$ und $A = \bar{A} \dot{+} \bar{A} \dot{+} \bar{A} \dot{+} \bar{A}$. Dann ist $Q = A + B$ orthogonal, und man bestätigt leicht, daß $q(x)$ das Minimalpolynom von Q ist.

b) Sei $q(x) = (x-1)^r$. Ist $r = 2s$, bzw. $r = 2s + 1$, so sei

$$h_s(x) = \sum_{k=0}^{s} \binom{\frac{1}{2}}{k} x^k$$

der Anfang der Entwicklung von $(1 + x)^{\frac{1}{2}}$ in eine formale Potenzreihe. Es ist dann $(h_s(x))^2 \equiv 1 + x$, $\bmod x^{s+1}$. B sei eine schiefsymmetrische K-Matrix mit dem Minimalpolynom x^r. Dann ist $A = h_s(B^2)$ symmetrisch und $Q = A + B$ wegen $QQ^* = (h_s(B^2))^2 - B^2 = E + B^2 - B^2 = E$ orthogonal. Da $B^r = (\frac{1}{2}(Q - Q^{-1}))^r = \frac{1}{2^r} Q^{-r} (Q + E)^r (Q - E)^r = 0$ und sowohl Q als auch $Q + E$ nicht singulär sind, so ist $(Q - E)^r = 0$. Anderseits ist $(Q - E)^{r-1} \neq 0$, also ist $(x-1)^r$ das Minimalpolynom von Q.

Eine analoge Betrachtung zeigt, daß auch $(x + 1)^r$ Minimalpolynom einer orthogonalen K-Matrix ist.

c) $q(x)$ habe neben anderen Wurzeln auch die Wurzeln $+1$ und -1.

Dann ist: $q(x) = (x-1)^{r_1} (x+1)^{r_2} \bar{q}(x)$ wo $\bar{q}(x)$ keine Wurzeln $+1$ und -1 mehr besitzt. Zu jedem dieser drei teilerfremden Faktoren gibt es nach dem eben bewiesenen eine orthogonale K-Matrix, welche diesen Faktor als Minimalpolynom hat. Somit gibt es auch eine orthogonale K-Matrix, nämlich die direkte Summe dieser drei Matrizen, deren Minimalpolynom $q(x)$ ist. Damit ist der Satz bewiesen.

Da jedes Element $\neq 0$ von Ω, wenn K nicht formal-reell ist, Wurzel eines Polynoms der Gestalt $q(x)$ ist, so folgt unmittelbar:

Satz 4.4. *Ist K formal-reell, so ist $\lambda \in \Omega$ dann und nur dann Eigenwert einer orthogonalen K-Matrix, wenn $\lambda \in \Delta(i)$ und über Δ die Norm 1 hat*[3]*; ist K nicht formal-reell, so ist jedes von 0 verschiedene Element von Ω Eigenwert einer orthogonalen K-Matrix.*

Für Körper der Charakteristik $p = 2$ ist Satz 4.4 falsch.

Gegenbeispiel: $q(x) = x^2 + x + 1$. Wäre Q eine orthogonale K-Matrix mit $q(x)$ als Minimalpolynom, so müßte $Q^2 + Q + E = O$, also $Q + Q^* + E = O$ sein. Aber in der Hauptdiagonalen von $Q + Q^*$ stehen lauter Nullen.

LITERATUR

[1] E. ARTIN und O. SCHREIER, *Algebraische Konstruktion reeller Körper*, Abh. math. Sem. Hamburg 5 (1926) S. 85–99.
[2] E. ARTIN, *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. math. Sem. Hamburg 5 (1926) S. 100–115.
[3] B. L. VAN DER WAERDEN, *Algebra*, Bd. 1, 4. Aufl., Verlag Springer, Berlin 1955, S. 219–246.
[4] C. C. MACDUFFEE, *The theory of matrices*, Ergeb. Math. Grenzgeb. II, 5. Verlag Springer, Berlin 1933.
[5] A. M. LEGENDRE, *Théorie des nombres*, Ed. 3, art. 317, 319.

(Eingegangen den 6. Juli 1957)

[3]) Das heißt für den Körper der rationalen Zahlen, wenn λ und alle seine Konjugierten den absoluten Betrag 1 haben.