Journal of Pure and Applied Algebra 38 (1985) 91–102
North-Holland



# SPECTRAL DECOMPOSITION THEOREM FOR REAL SYMMETRIC MATRICES IN TOPOI AND APPLICATIONS

Christiane ROUSSEAU
*Université de Montréal, Case postale 6128, Succ. "A", Montréal P.Q., H3C 3J7 Canada*

Communicated by P.J. Freyd
Received January 1981
Revised February 1985

## Introduction

In this paper we give the constructive version (in the topos-theoretic sense) of the spectral decomposition theorem for real symmetric (resp. hermitian) matrices. We interpret the theorem in spatial topoi. The interpretation gives us the following results:

(1) If a real symmetric matrix depends continuously on parameters, then its eigenvalues depend continuously on the same parameters.

(2) We get a normal form for real symmetric matrices depending continuously (resp. differentiably) on parameters.

(3) We get a versal deformation of any real symmetric matrix, i.e. a deformation that induces all other deformations up to similarity.

Classically Arnold gave a method in [1] to compute minimal versal deformations of matrices, i.e. deformations which involve the minimal number of parameters. With the same techniques we calculate here the minimal versal deformation of a real symmetric matrix. We notice that it is exactly the deformation obtained by interpreting our spectral decomposition theorem in topoi. This gives us that the spectral decomposition theorem we got in topoi is the best we can hope to get constructively.

It was in the author's thesis that the connection was first developped between constructive arguments in a topos and arguments involving parameters. There [3] she proved a one variable division theorem which has an interpretation in $\mathrm{Sh}(\mathbb{C}^{n-1})$ as the classical $n$-variable division theorem. Fourman worked in the same direction: He proved that, in a topos, any complex separable polynomial splits into linear factors. We use here his result, which can be interpreted as: If the coefficients of a complex separable polynomial depend continuously (resp. holomorphically) on parameters, then its roots depend continuously (resp. holomorphically) on the same parameters.

The paper is divided into three parts. In the first section we sketch the proof of the spectral decomposition theorem. We postpone the proof of the technical lemmas until the last section. We interpret the theorem in the second section. We also com-

pute the minimal versal deformation of a real symmetric matrix by classical methods and we compare it with our results. Finally in the last section we give the proof of the technical lemmas. We also give a proof of Fourman's theorem mentioned above.

**Remark.** Everything that is done here for real symmetric matrices works for complex hermitian matrices. In the proofs, orthogonal matrices are replaced by unitary matrices. Since both theorems and proofs are similar in all points we do not mention the hermitian case more explicitly.

## 1. Spectral decomposition theorem in a topos:

It is known that if a real symmetric matrix depends continuously on parameters, then its eigenvalues depend continuously on the same parameters, but the following example shows that continuous eigenvectors do not necessarily exist.

**Example.** We consider $\mathrm{Sh}(\mathbb{R}^2)$, the topos of sheaves over $\mathbb{R}^2$. In this topos the object of Dedekind real numbers is the sheaf of germs of continuous real-valued functions on $\mathbb{R}^2$. Let

$$A=\begin{pmatrix} x & y \\ y & 2x \end{pmatrix}.$$

$|\lambda I-A|=\lambda^2-3\lambda x+2x^2-y^2=0$ iff $\lambda=(3x\pm\sqrt{x^2+4y^2})/2$. In any neighborhood of $(0,0)$ there are no eigenvectors depending continuously on $x$ and $y$.

Moreover, in this example the eigenvalues are not differentiable. Thus there is no hope for a generalization of the theorem below to other 'real number objects', such as the sheaf of germs of $C^\infty$ real-valued functions on $\mathbb{R}^2$ (see [4] for the notion of 'real number object').

We first prove that in a topos eigenvalues exist.

**Theorem 1.** *Let $\mathscr{E}$ be a topos with a natural number object and $\mathbb{R}$ denote the object of Dedekind real numbers (cf.* [2]*). Any real symmetric matrix has n real eigenvalues, i.e. its characteristic polynomial splits into linear factors.*

**Proof.** Let $A=(a_{ij})$ be a real symmetric $n\times n$ matrix. The eigenvalues of $A$ are obtained as the extrema of the quadratic form associated with $A$: $Q(x)=xAx^{\mathrm{t}}$, $x\in\mathbb{R}^n$.

Let

$$\lambda_k=\min_{\{(x_1,\ldots,x_k)\mid x_i\cdot x_j=\delta_{ij}\}}\ \max_{\{x=a_1x_1+\cdots+a_kx_k\mid |x|=1\}} xAx^{\mathrm{t}}.$$

The following lemmas prove the existence of $\lambda_k$.

**Lemma 1.** *Given orthonormal vectors $x_1,\ldots,x_k$, the set*

$$S^{k-1}\langle x_1, \ldots, x_k\rangle = \{x = a_1 x_1 + \cdots + a_k x_k \mid |x| = 1\}$$

*is totally bounded, i.e.,* $\forall \varepsilon > 0\ \exists y_1, \ldots, y_m \in S^{k-1}\langle x_1, \ldots, x_k\rangle$ *such that* $\forall x \in S^{k-1}\langle x_1, \ldots, x_k\rangle\ \exists i \ni x \in B(y_i, \varepsilon)$.

**Lemma 2.** $S_k = \{(x_1, \ldots, x_k) \mid x_i \cdot x_j = \delta_{ij}\}$ *is totally bounded.*

**Lemma 3.** *The function* $\max_{x \in S^{k-1}\langle x_1, \ldots, x_k\rangle} xAx^t$ *is uniformly continuous on* $S_k$.

We must now show that the $\lambda_k$'s are roots of the polynomial $|\lambda I - A|$. André Joyal gave us the following idea: the $\lambda_k$'s depend continuously on $A$. It is therefore enough to show that $|\lambda_k I - A| = 0$ for rational matrices $A$. These matrices can be diagonalized by the usual method, i.e. we use the fact that the real algebraic numbers form a totally ordered field. The roots of the characteristic polynomial are then precisely the extrema of the associated quadratic form. The details of this proof are given in the following lemmas:

**Lemma 4.** *The* $\lambda_k$*'s depend continuously on* $A$.

**Lemma 5.** *Any polynomial in* $\mathbb{Q}[x]$ *splits into linear factors in* $\mathbb{C}[x]$.

**Lemma 6.** *The algebraic numbers are a geometric subfield of* $\mathbb{C}$, *i.e. a subring in which* $\forall x$ ($x = 0$ *or* $x$ *is invertible*).

*In particular the algebraic real numbers form a totally ordered geometric subfield of* $\mathbb{R}$, *i.e.,* $\forall x$ ($x = 0$ *or* $x > 0$ *or* $x < 0$).

**Lemma 7.** *Any rational symmetric matrix* $A$ *is diagonalizable, i.e.* $A$ *has* $n$ *orthonormal eigenvectors.*

$$A = S\begin{pmatrix} \mu_1 & & 0 \\ & \ddots & \\ 0 & & \mu_n \end{pmatrix} S^{-1},$$

$S$ *orthogonal. Moreover, if* $\mu_1 \leq \cdots \leq \mu_n$, *then* $\mu_k = \lambda_k$, *where* $\lambda_k$ *was defined as the* $k$*th extremum of* $Q(x) = xAx^t$.

The results on algebraic numbers (Lemmas 5 and 6) are from André Joyal. The proofs are sketched in Section 3.

We now give the tools for our spectral decomposition theorem: these tools are classical. We omit the proofs when the classical proofs are valid in our context.

**Proposition 1** (Cayley-Hamilton theorem). *Let* $A$ *be an* $n \times n$ (*real or complex*) *matrix, and* $p(\lambda) = |\lambda I - A|$ *be its characteristic polynomial. Then* $p(A) = 0$.

**Proposition 2.** *Let* $A$ *be a real* $n \times n$ *matrix and* $S$ *an orthogonal matrix* ($SS^t = I$). *Then* $A$ *is symmetric iff* $S^{-1}AS$ *is symmetric.*

**Proposition 3.** *Let $A$ be a real symmetric $n\times n$ matrix, and $p(\lambda)$ be its characteristic polynomial. If $p(\lambda)=p_1(\lambda)p_2(\lambda)$, with $(p_1,p_2)=1$, i.e. $\exists q_1(\lambda)$, $q_2(\lambda)$ such that $p_1q_1+p_2q_2=1$, then $\mathbb{R}^n=\mathrm{Ann}(p_1)\oplus\mathrm{Ann}(p_2)$, where $\mathrm{Ann}(p_i)=\{x\in\mathbb{R}^n \mid p_i(A)(x)=0\}$. Moreover $\mathrm{Ann}(p_1)$ is orthogonal to $\mathrm{Ann}(p_2)$.*

**Proof.** We just prove the last fact. Let $x\in\mathrm{Ann}(p_1)$. Then

$$x=p_1q_1(A)(x)+p_2q_2(A)(x)=p_2q_2(A)(x).$$

Let $y\in\mathrm{Ann}(p_2)$. Then

$$(x,y)=(p_2q_2(A)(x),y)=(x,p_2q_2(A)(y))=0.$$

**Definition.** $(f_1,\ldots,f_n)$ is a basis of $\mathbb{R}^n$ iff

(1) $f_1,\ldots,f_n$ generate $\mathbb{R}^n$, i.e., $\forall x\in\mathbb{R}^n\ \exists a_1,\ldots,a_n$ such that $x=a_1f_1+\cdots+a_nf_n$.

(2) $f_1,\ldots,f_n$ are linearly independant, i.e., $\forall a_1,\ldots,a_n\in\mathbb{R}\ \exists i\ a_i\neq 0\Rightarrow\sum a_jf_j\neq 0$.

**Theorem 2** (Spectral decomposition theorem for symmetric matrices). *Let $A$ be a real symmetric matrix. Then $\forall\varepsilon>0$ there exists an orthonormal basis $f_1,\ldots,f_n$, in which $A$ has the form:*

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}$$

*where each block $A_i$ is of order $n_i$. $n_1$ is such that $|\lambda_1-\lambda_i|<\varepsilon$ for $i\leq n_1$ and $\lambda_i\neq\lambda_1$ for $i>n_1$; $n_2$ is such that $|\lambda_{n_1+1}-\lambda_{n_1+i}|<\varepsilon$ for $1\leq i\leq n_2$, and $\lambda_{n_1+i}\neq\lambda_{n_1+1}$ for $i>n_2$, etc. ($\lambda_1\leq\lambda_2\leq\cdots\leq\lambda_n$ are the eigenvalues of $A$.)*

**Proof.**

$$|\lambda I-A|=(\lambda-\lambda_1)\cdots(\lambda-\lambda_n),\quad \lambda_1\leq\lambda_2\leq\cdots\leq\lambda_n,$$

$$\bigwedge_{i=1}^{n}(|\lambda_1-\lambda_i|<\varepsilon\vee\lambda_1\neq\lambda_i).$$

We finally have:

$$|\lambda_1-\lambda_i|<\varepsilon,\quad \forall i\leq n_1\wedge\lambda_i\neq\lambda_1,\quad i>n_1.$$

We take $p_1=(\lambda-\lambda_1)\cdots(\lambda-\lambda_{n_1})$ and $p_2=\prod_{i>n_1}(\lambda-\lambda_i)$. Let $\mathrm{Res}(p_1,p_2)$ be the resultant of the two polynomials $p_1,p_2$ (cf. [5]). $\mathrm{Res}(p_1,p_2)$ is invertible (classical proof). By the classical method we find $q_1,q_2$ such that $p_1q_1+p_2q_2=1$. Let $W_i=\mathrm{Ann}(p_i)$. By Proposition 3, $\mathbb{R}^n=W_1\oplus W_2$ and $W_1\perp W_2$. We need to find a basis for $W_1$ and $W_2$. Let $e_1,\ldots,e_n$ be the standard basis of $\mathbb{R}^n$. We consider the vectors $p_iq_i(A)(e_j)$. These $2n$ vectors generate $\mathbb{R}^n$, since $x=p_1q_1(A)(x)+p_2q_2(A)(x)$. We call them $f_1,\ldots,f_{2n}$. $f_j=\sum b_{ij}e_i$. $B=(b_{ij})$ is a $n\times 2n$ matrix. We also have $e_j=\sum c_{ij}f_i$. $C=(c_{ij})$ is a $2n\times n$ matrix.

$$BC = I_n \cdot \mathrm{Det}(BC) = \sum_{i_1 \cdots i_n} |B_{i_1 \cdots i_n}| \, |C^{i_1 \cdots i_n}| = 1,$$

where $B_{i_1 \cdots i_n}$ (resp. $C^{i_1 \cdots i_n}$) is the $n \times n$ submatrix of $B$ (resp. $C$) obtained by taking the columns (resp. the rows) $i_1, \ldots, i_n$. $\exists i_1, \ldots, i_n \, |B_{i_1 \cdots i_n}| \neq 0$. Then $f_{i_1}, \ldots, f_{i_n}$ generate $\mathbb{R}^n$. Moreover $f_{i_j} \in W_1$ or $f_{i_j} \in W_2$. We can suppose $f_{i_j} \in W_1$ for $j \leq k$, and $f_{i_j} \in W_2$ for $j > k$. This basis can be orthogonalized by the Gram-Schmidt process and we stay inside the $W_i$'s.

We now have to prove that $k = n_1$. If $A$ is rational it follows from the fact that $A$ is diagonalizable. We show that the $W_i$'s depend continuously on $A$ and that dimension is preserved. (One can remark that the argument used above can be repeated to prove that all basis have the same number of elements, so dimension is well defined). The rest of the proof is given in the following two lemmas.

**Lemma 8.** *The $W_i$'s depend continuously on $A$. By this we mean the following: Let $A = (a_{ij})$ and $A' = (a'_{ij})$.*

$$|\lambda I - A| = p(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n) = p_1 p_2, \qquad \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n,$$

$$|\lambda I - A'| = p'(\lambda) = (\lambda - \lambda'_1) \cdots (\lambda - \lambda'_n) = p'_1 p'_2, \quad \lambda'_1 \leq \lambda'_2 \leq \cdots \leq \lambda'_n$$

*where $p_1 = (\lambda - \lambda_1) \cdots (\lambda - \lambda_{n_1})$ (same for $p'_1$).*

*Let $W_i = \mathrm{Ann}(p_i)$ and $W'_i = \mathrm{Ann}(p'_i)$. Then $\forall \varepsilon > 0 \; \exists \delta > 0$ such that*

$$\sum_{i,j} |a_{ij} - a'_{ij}| < \delta \;\Rightarrow\; (\forall x \in W_i \;\; |x| = 1 \;\Rightarrow\; \exists x' \in W'_i \;\; |x - x'| < \varepsilon)$$

*and*

$$\forall x' \in W'_i \;\; |x'| = 1 \;\Rightarrow\; \exists x \in W_i \;\; |x' - x| < \varepsilon.$$

**Proof.** Let $\varepsilon > 0$ and $x' \in W'_1$. $p_1(A)(x) = 0$ iff $x = p_2 q_2(A)(x)$ iff $q_1 p_1(A)(x) = 0$. $\exists \delta > 0$ such that $|A - A'| < \delta$ implies $(p'_1, p'_2) = 1$ and $|q_1 p_1(A) - q_1 p'_1(A')| < \varepsilon$ (since the $\lambda_i$'s depend continuously on $A$ by Lemma 4). Then, if we suppose $|x'| = 1$,

$$|q_1 p_1(A)(x') - q_1 p'_1(A')(x')| = |q_1 p_1(A)(x')| < \varepsilon.$$

But $x' = x_1 + x_2$ with $x_i \in W_i$ and $x_2 = q_1 p_1(A)(x')$. So $|x' - x_1| = |x_2| < \varepsilon$.

**Lemma 9.** *If $W_i$ and $W'_i$ are defined as above and $\varepsilon$ is sufficiently small, then $W_i$ and $W'_i$ have the same dimension.*

**Proof.** Let $W_1$ be generated by orthonormal vectors $e_1, \ldots, e_k$. Let $e'_i \in W'_i$ be given by Lemma 8 such that $|e'_i - e_i| < \varepsilon$. We show that the $e'_i$'s are linearly independant. This shows $\dim W'_1 < \dim W_1$. We suppose $n\varepsilon < 1$. Let $x_1, \ldots, x_k$ be given with one $x_j \neq 0$. Without loss of generality we can suppose $|x_j| > n\varepsilon$, and $\forall i \;\; |x_i| < 1$.

$$|\textstyle\sum x_i e'_i| \geq |\sum x_i e_i| - |\sum x_i (e'_i - e_i)|.$$

$\sum x_i e_i$ has norm

$$\sqrt{\sum x_i^2} \geq \sqrt{x_j^2} > n\varepsilon. \qquad |\sum x_i(e_i' - e_i)| \leq \sum |x_i|\,|e_i' - e_i| < n\varepsilon.$$

Then $|\sum x_i e_i'| > n\varepsilon - n\varepsilon > 0$. So $\sum x_i e_i' \neq 0$.

**Remark.** We specialize here to the topos Sh($M$), where $M$ is a $C^\infty$ manifold. In this topos we have several 'objects of real numbers', i.e., suitable objects for real analysis (cf. [4] for the notion of real number object), of which we mention two:

$\mathbb{R}_M$, the sheaf of germs of continuous real-valued functions on $M$ (the Dedekind real number object).

$\mathbb{R}_\infty$, the sheaf of germs of $C^\infty$ real-valued functions. The example at the beginning of Section 1 shows that Theorem 1 is not valid if we replace $\mathbb{R}_M$ by $\mathbb{R}_\infty$. However Theorem 2 is valid when 'real numbers' mean elements of $\mathbb{R}_\infty$. It is enough to notice that if $p(x) \in \mathbb{R}_\infty[x]$ splits as $p = p_1 p_2$, with $p_i \in \mathbb{R}_M[x]$ and $(p_1, p_2) = 1$, then $p_1, p_2 \in \mathbb{R}_\infty[x]$.

## 2. Symmetric real matrices depending on parameters

Here we interpret Theorems 1 and 2 of Section 1. Theorem 1 is interpreted as Theorem 1′.

**Theorem 1′.** *If a real symmetric matrix depends continuously on parameters, then its eigenvalues depend continuously on the same parameters.*

**Proof.** A matrix depending continuously on parameters $\alpha_1, \ldots, \alpha_m$ can be thought of as a matrix in Sh($\mathbb{R}^m$), with coefficients in the Dedekind real numbers. Then the eigenvalues are Dedekind real numbers in Sh($\mathbb{R}^m$), i.e. depend continuously on the $\alpha_i$'s.

Theorem 2 interprets as Theorem 2′.

**Theorem 2′.** *Let $A(\beta)$ be a real symmetric matrix depending continuously (resp. differentiably) on parameters $\beta_1, \ldots, \beta_m$, and let $A(0) = A_0$ be similar to:*

$$A_0' = \begin{pmatrix} \lambda_1 I_{n_1} & & \\ & \ddots & \\ & & \lambda_r I_{n_r} \end{pmatrix} \quad \text{with } \lambda_i \neq \lambda_j \text{ for } i \neq j.$$

*Then there exists a matrix $C(\beta)$ depending continuously (resp. differentiably) on the $\beta_i$'s, and continuous (resp. differentiable) $\alpha_{jk}^i(\beta)$, $1 \leq j$, $k \leq n_i$, defined in a neighborhood of 0, such that $C(\beta)^{-1} A(\beta) C(\beta) = A_0' + B$ with*

$$B = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_r \end{pmatrix}.$$

*$B_i$ is symmetric:*

$$B_i = \begin{pmatrix} \alpha^i_{11} & \cdots & \alpha^i_{1n_i} \\ \vdots & & \vdots \\ \alpha^i_{1n_i} & \cdots & \alpha^i_{n_i n_i} \end{pmatrix}.$$

*Moreover, if $A_0 = A_0'$, i.e. $A_0$ is already in Jordan normal form, we can take $C(0) = I$.*

**Proof.** We consider $A(\beta)$ as a real matrix in $\mathrm{Sh}(\mathbb{R}^m)$, and we take $\varepsilon < \min(\lambda_i - \lambda_j)$. We apply Theorem 2 to the matrix $A$. The columns of the matrix $C(\beta)$ are the orthonormal vectors $f_1, \ldots, f_n$. Each $A_j$ can be written as $\lambda_j I_{i_j} + B_j$, for a $B_j$. Now suppose $A_0 = A_0'$. We replace $C(\beta)$ by $C(\beta)C(0)^{-1}$. Since $C(0)$ has the same diagonal block shape as $A_0'$,

$$(C(0)C(\beta)^{-1})A(\beta)(C(\beta)C(0)^{-1}) = A_0' + B',$$

where $B'$ has the same structure as $B$.

We now introduce the language of deformations in the present context. The definition of versal deformation was first given by Douady. It means a deformation that induces all possible deformations. In the present context, since we want deformation up to similarity, it takes the following form given by Arnold:

**Definition** (Arnold). $A(\alpha)$ is a *deformation* of $A_0$ iff $A(0) = A_0$. $A(\alpha)$ is versal iff for any deformation $B(\beta)$ of $A_0$, there exists a $C^\infty$ map $\varphi$ from a neighborhood of 0 in the parameter space of $B(\beta)$ to the parameter space of $A(\alpha)$, and a deformation $C(\beta)$ of $I_n$, defined on the same neighborhood such that $\varphi(0) = 0$ and $B(\beta) = C(\beta)A(\varphi(\beta))C^{-1}(\beta)$, with $C(\beta)$ orthogonal.

In terms of versal deformations our Theorem 2′ can be reformulated as:

**Theorem 2″.** *Let*

$$A_0 = \begin{pmatrix} \lambda_1 I_{n_1} & & \\ & \ddots & \\ & & \lambda_r I_{n_r} \end{pmatrix} \quad \text{with } \lambda_i \neq \lambda_j \text{ for } i \neq j.$$

*We define*

$$A(\alpha) = A_0 + \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_r \end{pmatrix} \quad \text{where } B_i = \begin{pmatrix} \alpha^i_{11} & \cdots & \alpha^i_{1n_i} \\ \vdots & & \vdots \\ \alpha^i_{1n_i} & \cdots & \alpha^i_{n_i n_i} \end{pmatrix}$$

*($B_i$ symmetric). Then $A(\alpha)$ is a versal deformation of $A_0$.*

We now compute the deformation of a real symmetric matrix with classical methods and compare with Theorem 2″. In particular we want to know what is the minimal number of parameters in a versal deformation of a real symmetric matrix. The following lemma is well known and gives the technique to find minimal versal deformations (cf. [1]).

**Lemma.** *$A(\alpha)$ is versal iff $A$ is transversal to* $\mathrm{Orb}(A_0)$, *where* $\mathrm{Orb}(A_0) = \{CA_0C^{-1} \mid CC^{\mathrm{t}} = I\}$. *So the minimal number of parameters is the codimension of* $\mathrm{Orb}(A_0)$.

In the context of real symmetric matrices, let $\mathrm{S}(n)$ be the set of real symmetric matrices, $\mathrm{O}(n)$ the orthogonal group. We have

$$\gamma : \mathrm{O}(n) \to \mathrm{S}(n): \quad C \mapsto CA_0C^{-1}.$$

The tangent map at the identity is $\gamma^* : T_I\mathrm{O}(n) \to T_{A_0}\mathrm{S}(n)$. $T_I\mathrm{O}(n)$ is the set of antisymmetric matrices: we denote it by $\mathrm{A}(n)$.

$$\gamma^* : \mathrm{A}(n) \to \mathrm{S}(n): \quad C \mapsto [C, A_0] = CA_0 - A_0C.$$

The image of $\gamma$ is $\mathrm{Orb}(A_0)$ and the tangent plane to $\mathrm{Orb}(A_0)$ at $A_0$ is the set of $[C, A_0]$, $C \in A(n)$. We compute this set when $A_0$ is a diagonal matrix

$$A_0 = \begin{pmatrix} \lambda_1 I_{n_1} & & \\ & \ddots & \\ & & \lambda_r I_{n_r} \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1r} \\ \vdots & & \vdots \\ C_{r1} & \cdots & C_{rr} \end{pmatrix}, \quad C \in A(n).$$

Then

$$[C, A_0] = \begin{pmatrix} D_{11} & \cdots & D_{1r} \\ \vdots & & \vdots \\ D_{r1} & \cdots & D_{rr} \end{pmatrix} \quad \text{where } D_{ij} = (\lambda_j - \lambda_i)C_{ij}.$$

In order to take $A(\alpha)$ transversal to $\mathrm{orb}(A_0)$ and minimal we take:

$$A(\alpha) = A_0 + \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_r \end{pmatrix} \quad \textit{with } B_i = \begin{pmatrix} \alpha^i_{11} & \cdots & \alpha^i_{1n_i} \\ \vdots & & \vdots \\ \alpha^i_{1n_i} & \cdots & \alpha^i_{n_in_i} \end{pmatrix}.$$

The number of independant parameters is $\sum_{i=1}^{r} n_i(n_i+1)/2$.

We have shown theorem 3:

**Theorem 3.** *The versal deformation described in Theorem 2″ is minimal. The number of independant parameters is* $\sum_{i=1}^{r} n_i(n_i+1)/2$.

Using Theorem 3 we can strengthen our Theorem 2 in topoi:

**Theorem 4.** *Theorem 2 is the best spectral decomposition theorem we can get in topoi. We mean the following: By Theorem 2 any symmetric matrix A is similar to a matrix*

$$\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix}$$

*where the $A_i$'s are symmetric square blocks. There is no hope, in the general case to show that the $A_i$'s have some zero entries.*

## 3. Proof of the lemmas

**Proof of Lemma 1.** Let $x=\sum_{i=1}^{k} x_i a_i$. Then $|x|=1$ iff $\sum_{i=1}^{k} a_i^2=1$ iff $(a_1,\ldots,a_k)\in S^{k-1}$. We consider the cube $C$ in $\mathbb{R}^k$ given by

$$C=\bigcup_{i=1}^{k} [-1,1]^{i-1}\times\{-1,1\}\times[-1,1]^{k-i}.$$

$C$ is totally bounded. Therefore, given $\varepsilon>0$, $\exists y_1,\ldots,y_m$, such that $C\subset\bigcup_{i=1}^{m} B(y_i,\varepsilon)$. Then $S^{k-1}\subset\bigcup_{i=1}^{m} B(y_i/|y_i|,\varepsilon)$. If $y_i=(a_{i1},\ldots,a_{ik})$, we have

$$S^{k-1}\langle x_1,\ldots,x_k\rangle\subset\bigcup_{i=1}^{m} B\Big(\sum_{j=1}^{k} a_{ij}x_j,\varepsilon\Big).$$

**Proof of Lemma 2.** Induction on $k$. The case $k=1$ follows from Lemma 1. We now suppose the lemma true for $k$ and we consider $S_{k+1}=\{(x_1,\ldots,x_{k+1})\,|\,x_i\cdot x_j=\delta_{ij}\}$. Let $\varepsilon>0\cdot S_k$ is totally bounded. Therefore $\exists\overline{y_1},\ldots,\overline{y_m}\in\mathbb{R}^{nk}$ such $S_k\subset\bigcup_{i=1}^{m} B(\overline{y_i},\varepsilon)$ (with the norm on $\mathbb{R}^{nk}$). Let $\overline{y_h}=(x_{h1},\ldots,x_{hk})$, $h=1,\ldots,m$, $x_{hi}\in\mathbb{R}^n$. We consider the system of linear equations $x_{h,k+1}\cdot x_{h,j}=0$, $j=1,\ldots,k$. The $k\times n$ matrix of the system is

$$B=\begin{pmatrix} x_{h,1} \\ \vdots \\ x_{h,k} \end{pmatrix} \quad\text{and}\quad BB^{t}=I_k.$$

Then

$$|I_k|=1=\sum_{i_1<\cdots<i_k}|B_{i_1\cdots i_k}|^2,$$

where $B_{i_1\cdots i_k}$ is the $k\times k$ submatrix of $B$ defined by the columns $i_1,\ldots,i_k$. So $\exists i_1,\ldots,i_k$ such that $1/\sqrt{\binom{n}{k}}\le|B_{i_1\cdots i_k}|\le 1$. Using this submatrix we can find $n-k$ linearly independent solutions $x_{h,k+1,1},\ldots,x_{h,k+1,n-k}$, of the system. These can be orthonormalized, using the Gram-Schmidt process. By Lemma 1, we can find linear combinations $y_{h,1},\ldots,y_{h,p_h}$ of these vectors such that $\forall y$ if $y\cdot x_{h,j}=0$ for

$j=1,\ldots,k$, then $\exists r \ni |y-y_{h,r}|<\varepsilon$. We consider the vectors $(x_{h,1},\ldots,x_{h,k},y_{h,k+1,j})\in S^{k+1}$, $h=1,\ldots,m$, $j=1,\ldots,p_h$. These vectors are denoted by $\bar{\bar{y}}_1,\ldots,\bar{\bar{y}}_s$. Then, for any $\bar{\bar{x}}=(x_1,\ldots,x_{k+1})\in S_{k+1}$, $\exists h \ni \bar{x}=(x_1,\ldots,x_k)\in B(\bar{y}_h,\varepsilon)$, and we have $x_{k+1}\cdot x_{h,i}=\varepsilon_i$ with $|\varepsilon_i|<\varepsilon$ for $i=1,\ldots,k$. We consider the system: $x_{k+1}\cdot x_{h,i}=\varepsilon_i$, $i=1,\ldots,k$, $|\varepsilon_i|<\varepsilon$. Since $|B_{i_1\ldots i_k}|\geq 1/\sqrt{\binom{n}{k}}$, the solutions $x_{k+1}$ are not more distant than $\varepsilon\sqrt{\binom{n}{k}}$ from those of the system: $x_{k+1}\cdot x_{h,i}=0$, $i=1,\ldots,k$.

**Proof of Lemma 3.** Let $\varepsilon>0$ and $(x_1,\ldots,x_k)$, $(y_1,\ldots,y_k)\in S_k$ with $|x_i-y_i|<\varepsilon/n$. Suppose $x=\sum_{i=1}^k a_i x_i$ and $y=\sum_{i=1}^k a_i y_i$ with $\sum_{i=1}^k a_i^2=1$. Then $|x-y|<\varepsilon$ and $|x|=|y|=1$. Further,

$$\begin{aligned}|xAx^t-yAy^t| &\leq |xAx^t-yAx^t|+|yAx^t-yAy^t|\\ &\leq |x^t|\,|(x-y)A|+|y|\,|A(x^t-y^t)|=2|(x-y)A|\\ &\leq 2C_A|x-y|, \quad \text{where } C_A=\left(\sum_{i=1}^n\sum_{j=1}^n a_{ij}^2\right)^{1/2}.\end{aligned}$$

**Proof of Lemma 4.** Let $A=(a_{ij})$ and $A'=(a'_{ij})$ be such that $\sum_{i,j}(a_{ij}-a'_{ij})^2<\varepsilon$. Let $S=S^{k-1}\langle x_1,\ldots,x_k\rangle$. Let $M=\max_{x\in S} xAx^t$ and $M'=\max_{x\in S'} xA'x^t$. $\exists x\in S$ $|M-xAx^t|<\varepsilon$. But $|xAx^t-xA'x^t|<\varepsilon$. So $M'>M-2\varepsilon$. In the same way $M>M'-2\varepsilon$. By taking the minimum of all $|M'-M|$ for all $\langle x_1,\ldots,x_k\rangle\in S_k$, we get $|\lambda_k-\lambda'_k|<2\varepsilon$.

We now give the proof of Fourman's theorem, since we use it later. It uses Newton's method in the following form.

**Lemma** (Newton's method of approximation of zeroes). *Let $f:\mathbb{C}\to\mathbb{C}$ be holomorphic and $x_0\in\mathbb{C}$. Suppose that $\exists c,\lambda$ such that: $|f(x_0)|<c/2\lambda$, and $\forall x,y\in B(x_0,c)$*

$$|f(x)-f(y)-f'(y)(x-y)|<\frac{1}{2\lambda}|x-y| \quad \textit{and} \quad |f'(x)|>\frac{1}{\lambda}.$$

*Then $\exists\xi\in B(x_0,c)$ such that $f(\xi)=0$.*

**Proof.** We define $x_{n+1}=x_n-f(x_n)(f'(x_n))^{-1}$. By induction we show $|x_n-x_{n-1}|<c/2^n$ (this implies $x_n\in B(x_0,c)$) and $|f(x_{n-1})|<c/2^n\varepsilon$ (same proof as classical proof). Then $\xi=\lim x_n$.

**Theorem** (Fourman). *Let $p(x)\in\mathbb{C}[x]$ be a monic polynomial of degree n, such that* $\mathrm{Res}(p,p')\neq 0$. *Then p splits into linear factors.*

**Proof.** $\mathrm{Res}(p,p')\neq 0 \Rightarrow \exists f,g$: $pf+p'g=1$ (same as classical proof). Let $R>0$ be such that $p(x)\neq 0$ for $|x|<R/2$. Let

$$M = \max_{x \in \overline{B(0,R)}} (f(x), g(x)) \quad \text{and} \quad \varepsilon = \frac{1}{4M}.$$

$\exists\, 0 < \delta < 1$ such that

$$\forall x, y \in \overline{B(0,R)}\ |x-y| < \delta \Rightarrow |p(x)-p(y)| < \varepsilon \text{ and}$$
$$|p(x)-p(y)-p'(y)(x-y)| < \varepsilon |x-y|.$$

We must find $x_0$ such that $|p(x_0)| \leq \delta\varepsilon = \delta/4M$.

$$\exists \eta > 0,\ \forall x, y \in \overline{B(0,R)}\ |x-y| < \eta \Rightarrow |p(x)-p(y)| < \delta\varepsilon/2.$$

$\overline{B(0,R)}$ is totally bounded: $\overline{B(0,R)} \subset \bigcup_{i=1}^{m} B(x_i, \eta/2)$. We have

$$\bigwedge_{i=1}^{m} (|p(x_i)| < \delta\varepsilon \vee |p(x_i)| > \tfrac{3}{4}\delta\varepsilon).$$

Using Liouville's theorem we see that one of the statements

$$\bigwedge_{j=1}^{k} |p(x_{i_j})| < \delta\varepsilon \wedge \bigwedge_{l \neq i_j} |p(x_l)| > \tfrac{3}{4}\delta\varepsilon$$

is valid, with at least one term $|p(x_{i_j})| < \delta\varepsilon$. We take $x_0 = x_{i_j}$. Then

$$\forall x, y \in B(x_0, \delta)\ |p'(x)g(x)| = |1 - p(x)f(x)|$$
$$\geq |1 - p(x_0)f(x)| - |f(x)(p(x)-p(x_0))|$$
$$\geq 1 - |p(x_0)|\,|f(x)| - |f(x)|\,|p(x)-p(x_0)|$$
$$\geq 1 - (\delta/4M)M - M\varepsilon \geq 1 - \tfrac{1}{4} - \tfrac{1}{4} = \tfrac{1}{2},$$

$$|p'(x)|M \geq |p'(x)g(x)| \geq \tfrac{1}{2} \Rightarrow |p'(x)| \geq 1/2M.$$

We take $\lambda = 2M$, $c = \delta$ and we apply the previous lemma.

**Proof of Lemma 5.** By induction on the degree of $p$ we show that $p(x) \in \mathbb{Q}[x]$ can be factorized as a product of separable polynomials. We then apply Fourman's theorem. Suppose the result true for any polynomial of degree $n$ and let $p(x) = x^{n+1} + a_1 x^n + \cdots + a_{n+1}$. We consider $\mathrm{Res}(p, p')$, the resultant of $p$ and $p'$.

(1) If $\mathrm{Res}(p, p') \neq 0$, then $p$ is separable.

(2) If $\mathrm{Res}(p, p') = 0$, we use Euclid's algorithm to find the GCD of $p$ and $p'$, call it $f$. Then $p = (p/f)f$, with $p/f$ separable and $\deg f \leq n$.

**Proof of Lemma 6.** The proof of Lemma 5 gives us that any algebraic real number $\bar{x}$ is the root of a separable polynomial $p(x) \in \mathbb{Q}[x] : p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$. Then ($a_n = 0$ and $a_{n-1} \neq 0$) or $a_n \neq 0$. Hence $p(\bar{x}) = 0$ implies $\bar{x} = 0$ or $\bar{x} \neq 0$.

We now show that the algebraic numbers form a field. Let $x_1, y_1$ be two algebraic real numbers, respectively roots of $p(x)$ and $q(x)$ in $\mathbb{Q}[x]$,

$$p(x)=x^n+a_1x^{n-1}+\cdots+a_n=(x-x_1)\cdots(x-x_n),$$

$$q(x)=x^m+b_1x^{m-1}+\cdots+b_m=(y-y_1)\cdots(y-y_m).$$

Then $x_1+y_1$ and $x_1y_1$ are respectively roots of

$$r(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-x_i-y_j) \quad \text{and} \quad s(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-x_iy_j).$$

$r(x)$ and $s(x)$ are symmetric in $x_1,\ldots,x_n$ on one hand, and $y_1,\ldots,y_m$ on the other. Using the symmetric function theorem, the proof of which is constructive, and thus valid in a topos, we get that $r(x)$, $s(x)\in\mathbb{Q}[x]$. Moreover, if $x_1\neq 0$ we can suppose $a_n\neq 0$ (otherwise $a_n=0$ and we consider $p/x$). Then $x^{-1}$ is a root of $t(x)=1+a_1x+a_2x^2+\cdots+a_nx^n$.

**Proof of Lemma 7.** $|\lambda I-A|=0 \Rightarrow \lambda=\mu_1,\ldots,\mu_n;\ \mu_1\leq\cdots\leq\mu_n$. The matrix $\mu_iI-A$ can be row-reduced to an echelon matrix, using that algebraic numbers are comparable and form a field. Thus we can find eigenvectors and the classical proof can be used to show that the $\mu_i$'s are real. If we orthonormalize the eigenvectors we get

$$A=S^{t}\begin{pmatrix}\mu_1 & & 0\\ & \ddots & \\ 0 & & \mu_n\end{pmatrix}S,$$

with $S$ orthogonal. Then $Q(x)=xAx^{t}=\sum_{i=1}^{n}\mu_iy_i^2$. Using this final equality to calculate the $\lambda_i$'s we get $\mu_i=\lambda_i$.

## References

[1] V.I. Arnold, On matrices depending on parameters, Russian Math. Surveys 26 (1971).

[2] C.J. Mulvey, Intuitionistic algebra and representation of rings, Mem. AMS 148 (1974).

[3] C. Rousseau, Topos theory and complex analysis, Thesis, Lecture Notes in Math. 753 (Springer, Berlin, 1979).

[4] C. Rousseau, Nombres réels et complexes dans les topos spatiaux, Ann. Sc. Math. Québec 3 (1) (1979).

[5] B.L. van der Waerden, Modern Algebra (Springer, Berlin, 1931).