# STATES IN SEPARABLE ALGEBRAS

by

Bronislaw Czarnocha

Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in the Belfer Graduate School of Science
Yeshiva University
New York

September 1976

The committee for this doctoral dissertation consisted of:

Aage Petersen, Ph.D., Chairman

David Finkelstein, Ph.D.

Arthur Komar, Ph.D.

# ACKNOWLEDGMENTS

Aage... I hope you know how grateful I am for all you've done for me.

Manuela, Malgosia, Teresa... without you, this work would never have been finished.

TABLE OF CONTENTS

ABSTRACT

The classification of composable, finite dimensional, quantal simple two product algebras yields many different types only one of which seems to occur in nature. This suggest the following question: is there a conceptually instructive way of characterizing the quantum mechanical two product algebra in relation to all other two product algebra obtained through the classification? The thesis provides a positive answer to this question through the introduction of the set $\mathcal{S}$ of states as partially defined morphisms from the algebra onto an underlying it algebraic field. ( $\mathcal{S} = \{ Hom(\mathcal{O}, F) \mid \mathcal{O} \in \mathcal{F}$ – a family of domains $\}$ ).

It is shown that:

(·) Transitivity of the automorphism group of the algebra on the set $\mathcal{S}$ is the property of the two product algebra defined, over a real closed field, by a nonisotropic involution which distinguishes it from all other algebras obtained through the classification.

(··) The condition of transitivity of the automorphism group on the set $\mathcal{S}$ is equivalent to the following separability condition:

$\mathcal{O} \in \mathcal{F}$ is separable if for any $f_1, f_2 \in \mathcal{O}$ such that $f_1 \neq f_2$ there is $\vartheta \in Hom(\mathcal{O}, P)$ with $\vartheta(f_1) \neq \vartheta(f_2)$

An algebra is separable iff every $\mathcal{O} \in \mathcal{F}$ is separable.

# INTRODUCTION

## 1. Background and Motivation

This thesis is based on the algebraic analysis of classical and quantum mechanics undertaken by Grgin and Petersen[1)2)] Their study centered on the interplay between two concepts which were abstracted from the algebraic structures present in both mechanics. These concepts are:

1. A two product algebra over a field F:

where $\sigma$ is an unspecified product and $\alpha$ is Lie i.e.

$$f \alpha g = - g \alpha f$$

$$0 \equiv f \alpha (g \alpha h) + g \alpha (h \alpha f) + h \alpha (f \alpha g)$$

The two products are related to each other through the "distribution" property of $\alpha$ with respect to $\sigma$ :

$$f \alpha (g \sigma h) = (f \alpha g) \sigma h + g \sigma (f \alpha h)$$

In other words the operator $f \alpha$ is a derivation with respect to $\sigma$ . In Classical Mechanics $\sigma$ is the commutative, associative product and $\alpha$ is the Poisson bracket in the set of differentiable real valued functions on the phase space; in Quantum Mechanics $\sigma$ is the anti-

---

1) E. Grgin and A. Petersen, "Duality of Observable and Generators in Classical and Quantum Mechanics," J. of Math. Phys., 15(6), 764-9 (June 1974).

2) E. Grgin and A. Petersen, Algebraic Implications of Composability of Physical Systems. (To be published in Communications in Mathematical Physics.)

commutator divided by 2 and $\alpha$ is the commutator divided by 2i in the algebra of hermitian operators on the Hilbert space.

2. A <u>composition class $\mathcal{T}$</u> of two product algebras - a set of two product algebras equipped with a product $\circ : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ with properties:

a. If $A_1, A_2 \in \mathcal{T}$ and $A_{12} := A_1 \circ A_2$ then $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ i.e. the underlying linear space of the product algebra $A_{12}$ is the tensor product of the underlying linear spaces of the component algebras.

b. $A_1 \circ (A_2 \circ A_3) = (A_1 \circ A_2) \circ A_3$

c. The field $F$ (considered as an algebra $(F, \sigma, \alpha)$ with $\sigma$ being the product in F and $\alpha = 0$) belongs to $\mathcal{T}$ and acts as a unit in it. i.e.

$$F \circ A = A \circ F = A$$

The composition class satisfying those properties is a semigroup with a unit.

The authors investigated restrictions which the semigroup structure imposes on the algebraic structure of the two product objects belonging to the class. They showed that:

1. All composition classes of two product algebras over the field F are obtained from a family labelled by a parameter $\alpha \in \dot{F}/\dot{F}^2 \cup \{0\}$ (where $\dot{F} := F - \{0\}$, $\dot{F}^2 = \dot{F} \cdot \dot{F}$).

2. If $\mathcal{T}_a \ni A_i = (\mathcal{H}_{i|F}, \sigma_i, \alpha_i)$, $i = 1,2$ then

$$A_{12} = A_1 \circ A_2 = (\mathcal{H}_1 \otimes \mathcal{H}_2, \sigma_{12} = \sigma_1 \otimes \sigma_2 - a\,\alpha_1 \otimes \alpha_2, \alpha_{12} = \sigma_1 \otimes \alpha_2 + \alpha_1 \otimes \sigma_2)$$

3. For every $(\mathcal{H}, \sigma, \alpha)$ in $\mathcal{T}_a$

$$f \sigma g = g \sigma f$$

$$[f, g, h]_\sigma = a[f, g, h]_\alpha \quad ^{3)}$$

If a = 0 then $\sigma$ is associative and commutative and we call the algebra $(\mathcal{H}_{|F}, \sigma, \alpha, a = 0)$ a <u>classical</u> two product algebra; if $a \neq 0$, then $\sigma$ is special Jordan[4] and $(\mathcal{H}_{|F}, \sigma, \alpha, a \neq 0)$ is a <u>quantal</u> two product algebra.

These results show that the compatibility of the composition class structure with the structure of its members leads to the determination of all composition classes (a global concept) and to the determination of the product $\sigma$ for <u>each</u> two product algebra (a local concept). The connection between those two levels of analysis is provided by the parameter a.

Elements of the classification of all simple[5] two product algebras are contained in an unpublished

---

3) If $(A, \pi)$ is an algebra then $[f, g, h]_\pi := (f \pi g) \pi h - f \pi (g \pi h)$ is the associator of $\pi$.

4) A Jordan algebra $(A, \pi)$ is an algebra which fulfills conditions: $[x, y]_\pi = 0$, $[x, y, x^2]_\pi = 0$. A Jordan algebra $(A, \pi)$ is Special Jordan if there is a monomorphism: $(A, \pi) \to (U, [,]_\cdot)$ for some associative $U$.

5) A simple two product algebra is an algebra without simultaneous nontrivial $\sigma, \alpha$ ideals.

paper[6]:

1. There are no finite dimensional classical two product algebras over the field F of characteristic 0.

2. In a case when the field F is of characteristic $p>0$ the classification of non-commutative[7] Jordan algebras is incomplete. However, among the known cases there is a large class of nodal, Lie admissible algebras which are classical.

3. For any field F there are four series of quantal algebras

a. $(\mathcal{H}_{/F}, \sigma, \alpha, a=-1) = (M^n_{/F}, [\,,\,]_-, [\,,\,]_-)$

b. $(\mathcal{H}_{/F}, \sigma, \alpha, a=-1) = (M^n_{/\Delta(F)}, [\,,\,]_+, [\,,\,]_-)$

c. $(\mathcal{H}_{/F}, \sigma, \alpha, \sqrt{-a} \notin F) = (S_J(M^n_{/F(\theta)}), \frac{1}{2}[\,,\,]_+, \frac{1}{2\theta}[\,,\,]_-)$

d. $(\mathcal{H}_{/F}, \sigma, \alpha, \sqrt{-a} \notin F) = (S_J(M^n_{/\Delta(F(\theta))}), \frac{1}{2}[\,,\,]_+, \frac{1}{2\theta}[\,,\,]_-)$

where

(·) $M^n_{/K}$ and $M^n_{/\Delta(K)}$ are total matrix algebras over respectively, the field $K$ and a division ring $\Delta$ over the field $K$,

(··) $\theta^2 = -a$, $F(\theta)$ is the quadratic extension of which includes the root $\theta$.

(···) $J$ is an involution of the second kind in $M^n$[8]

---

[6] E. Grgin and A. Petersen, Classification of Two Product Algebras. (To be published.)

[7] The classification of classical two product algebras is achieved by analyzing a noncommutative Jordan product $\tau = \sigma + \alpha$.

[8] See Appendix 1.

(iv) $S_J(M^n)$ is the set of $J$-symmetric elements of $M^n$ with $S_J(F(\Theta)) = S_J(\Delta(F(\Theta)) = F$.

One sees that the set $\mathcal{P}$ of simple, quantal, finite dimensional two product algebras contains many different types only one of which seems to occur in nature (the algebra of the type c. for $F$ being equal to $\mathbb{R}$ and $J$ being a non-isotropic involution).

The question arises: is there a conceptually instructive way of characterizing the quantum mechanical two product algebras in relation to all other elements of the set $\mathcal{P}$?

This thesis gives a positive answer to the question by exploting the framework suggested by Grgin and Petersen in their unpublished paper.[9] Its main points are the following: First, the authors assume the existence of three objects the structure of which is unspecified:

(·) an object $Ob$ whose elements are called observables

(··) an object $\mathcal{V}$ whose elements are called values

(···) an object $\mathcal{S}$ whose elements, called states, are partially defined morphisms $(Ob \longrightarrow \mathcal{V})$ with respect to the unspecified structures.

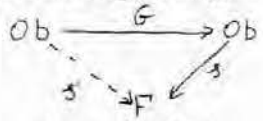
Second, they impose upon this scheme certain conditions, the role of which is to induce structures in those objects.

---

[9] Grgin and Petersen: Hamiltonian mechanics, preprint (unpublished).

The imposed conditions were as follows:

1. $Aut\ \mathcal{V} = \{id\}$
2. The group $Aut\ Ob$ can act in the set $\mathcal{S}$ through the requirement of the commutativity of the following diagram:




(For every $G \in Aut(Ob)$ and $s \in \mathcal{S}$ there exists a unique $s' \in \mathcal{S}$ which satisfies the diagram.)

The outlined program was not carried out in its full generality.

In the present paper we assume that:

($\cdot$) the set $Ob$ is an algebra $(\mathcal{H}_{|P}, 6)$ which is the substructure of a two product algebra $(\mathcal{H}_{|F}, 6, \alpha) \in \mathcal{Q}$

($\cdot\cdot$) the set $\mathcal{V}$ of values for $(\mathcal{H}_{|P}, 6)$ is the field $F$

($\cdot\cdot\cdot$) the $\mathcal{S}$ of states is equal to $\{Hom(\mathcal{O}, F) \mid \mathcal{O} \in \mathcal{F}\}$ where $\mathcal{F}$ is the family of commutative, associative subalgebras of $(\mathcal{H}_{|P}, 6)$. Each subalgebra is generated by an element $f \in \mathcal{H}$ and the unit of the algebra $(\mathcal{H}_{|P}, 6)$. (Clearly the family $\mathcal{F}$ constitutes the covering of $\mathcal{H}$.)

The choice of this family as the family of the domains of partially defined morphisms is suggested by the following remarks concerning finite dimensional Quantum Mechanics.

In the standard formulation of Quantum Mechanics an algebra of observables is an algebra $(\mathcal{H}_{/\mathbb{R}}, [,]_+)$ of hermitian operators on a Hilbert space $(V^n_{/\mathbb{C}}, \Gamma)$. Each normalized eigenvector $e_i$ of an operator A is a possible pure state of a system represented by this algebra. Moreover, if $A e_i = a_i e_i \ (a_i \in \mathbb{R})$ then $\Gamma(e_i, A e_i) = a_i$.

Let us consider now a particular operator $A \in \mathcal{H}_{/\mathbb{R}}$, the collection of its eigenvectors $\{e_i\}$, and the subalgebra $\mathcal{O}(A)$ generated over reals by the unit $I \in (\mathcal{H}_{/\mathbb{R}}, [,]_+)$ and all powers of A. As the algebra $(\mathcal{H}_{/\mathbb{R}}, [,]_+)$ is finite dimensional there are $\infty > k > 0$ linearly independent powers of A so that any element $X \in \mathcal{O}(A)$ can be uniquely written in the form:

$$X = x_0 I + x_1 A + x_2 A^2 + \ldots + x_{k-1} A^{k} + x_k A^{k}$$

Any eigenvector $e_i$ determines a map $\Gamma_{e_i} : \mathcal{O}(A) \longrightarrow \mathbb{R}$ by letting $\Gamma_{e_i}(X) := \Gamma(e_i, X e_i) = \sum_{j=1}^{k} x_j a_i^j \in \mathbb{R}$

The map $\Gamma_{e_i}$ is a homomorphism of $\mathcal{O}(A)$ onto $\mathbb{R}$ : if $Y = \sum_{m=0}^{k} y_m A^m$ then $\Gamma_{e_i}(X Y) = \Gamma_{e_i}\left(\left(\sum x_j a_i^j\right)\left(\sum y_m A^m\right)\right) =$

$$= \Gamma_{e_i}\left(\sum_{p=0}^{k} A^p \sum_{r=0}^{p} x_r y_{p-r}\right) = \Gamma\left(e_i, \left(\sum_{p=0}^{k} A^p \sum_{r=0}^{p} x_r y_{p-r}\right) e_i\right) =$$

$$= \sum_{p=0}^{k} \sum_{r=0}^{p} x_r y_{p-r}\, \Gamma(e_i, A^p e_i) = \sum_{p=0}^{k} \sum_{r=0}^{p} x_r y_{p-r}\, a_i^p = \Gamma_{e_i}(X) \cdot \Gamma_{e_i}(Y)$$

The kernel of this homomorphism $\operatorname{Ker} \Gamma_{e_i}$ is equal to the set $\{ X(A) \in \mathcal{O}(A) \mid a_i$ is a root of the equation $X(\lambda) = x_0 + x_1 \lambda + x_2 \lambda^2 + \ldots + x_k \lambda^k \}$. The normalization of eigenstates guarantees $\Gamma_{e_i}(I) = 1 \in \mathbb{R}$.

It is clear that $\Gamma_{e_i} \neq \Gamma_{e_j}$ iff $e_i, e_j$ belong to different eigenvalues. Hence, each eigenvalue

of the operator A determines a homomorphism from onto reals.[10] In a case when A is nondegenerate (i.e., when $\mathcal{O}(A)$ is a maximal, associative subalgebra on the generator A), there is a one-to-one correspondence between normalized eigenstates of A and homomorphisms $\Gamma_{e_i}$. It is important to notice that, if A is nondegenerate, the maps $\Gamma_{e_i}$ bear the homomorphic property simultaneously only on $\mathcal{O}(A)$ ; each particular $\Gamma_{e_i}$ can be extended to a larger subalgebra $\mathcal{O}_i(A) \supset \mathcal{O}(A)$ by enlarging its kernel. However, the domain on which all of them are homomorphisms is equal to $\mathcal{O}(A) = \bigcap_i \mathcal{O}_i(A)$.[11]

---

[10] In a standard approach the map $\Gamma_{e_i}$ is allowed to act on the whole algebra $(\mathcal{H}, [,]_+)$. As the algebra $(\mathcal{H}_{\mathbb{R}}, [,]_+)$ is $[,]_+$-simple no map of this type can be a homomorphism. Therefore the map $\Gamma_{e_i}$ respects only the linear structure and ignores $[,]_+$ product. - hence, a connection to the statistical interpretation of quantum mechanics.

[11] To see this more clearly one can consider the following example: Let $(V^3_{\mathbb{C}}, \Gamma(\cdot,\cdot))$ be 3 dimensional Hilbert space and the operator A has the representation $\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}$ in its eigenbasis $\{e_i\}_{i=1}^3$. $\mathcal{O}(A)$ is then the set of all diagonal matrices in this basis. Ker $\Gamma_{e_1} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & y \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ and it can be extended to $\left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & x & z \\ 0 & \bar{z} & y \end{pmatrix} \middle| z \in \mathbb{C} \right\}$ so that the domain of $\Gamma_{e_1}$ can be extended to $\mathcal{O}_1(A) = \left\{ \begin{pmatrix} w & 0 & 0 \\ 0 & x & z \\ 0 & \bar{z} & y \end{pmatrix} \middle| w, x, y \in \mathbb{R},\ z \in \mathbb{C} \right\}$. It is clear that $\Gamma_{e_1}$ is a homomorphism on $\mathcal{O}_1(A)$. Similarly, the domain of $\Gamma_{e_2}$ can be extended to the subalgebra $\mathcal{O}_2(A) = \left\{ \begin{pmatrix} x & 0 & z \\ 0 & w & 0 \\ \bar{z} & 0 & y \end{pmatrix} \middle| x, y, w \in \mathbb{R},\ z \in \mathbb{C} \right\}$ $\mathcal{O}_3(A)$ to $\left\{ \begin{pmatrix} x & z & 0 \\ \bar{z} & y & 0 \\ 0 & 0 & w \end{pmatrix} \middle| x, y, w \in \mathbb{R},\ z \in \mathbb{C} \right\}$.
The intersection of these domains is equal to $\mathcal{O}(A)$.

On the other hand any orthonormal basis $\{e_i\}$ in $(V^n_{/\mathbb{C}}, \Gamma(\,,\,))$ determines a maximal associative subalgebra $\mathcal{O}_e(A)$ which serves as a domain for the homomorphisms $\{\Gamma_{e_i}\}$. Any nondegenerate operator $A \in \mathcal{O}_e$ and $I \in \mathcal{H}_{/\mathbb{R}}$ can serve as its generators. Hence, the set $\mathcal{S} = \{Hom(\mathcal{O}, F) \mid \mathcal{O} \in \mathcal{F}$ -the family of maximal associative subalgebras$\}$ is isomorphic to the set of pure states of finite dimensional quantum mechanics.

Let now $\{\Gamma_{e_i}\}_{i=1}^{n}$ be the set of morphisms on the subalgebra $\mathcal{O}_e$ and $U$ be a unitary transformation: $e_i \longrightarrow r_i := Ue_i$, $i=1,\dots n$. Then, the maps $\Gamma_{Ue_i} := \Gamma(Ue_i \cdot Ue_i) = \Gamma(e_i, U_i^{+} Ue_i)$ are homomorphisms on the subalgebra $G_U(\mathcal{O}_e) = \{UAU^{+} \mid A \in \mathcal{O}_e\}$. We see that action induced by the subgroup of $Aut(\mathcal{H}_{/\mathbb{R}}, [\,,\,]_+)$ on the set of states is equivalent to the action of this subgroup on the family $\mathcal{F}'$ of maximal one generator subalgebras. Moreover, since any two such bases are connected by a unitary transformation, $Aut(\mathcal{H}_{/\mathbb{R}}, [\,,\,]_+)$ acts transitively on the family $\mathcal{F}'$.

The main conclusion of this thesis consists in showing:

(•) that the transitivity of $Aut(\mathcal{H}_{/\mathbb{R}}, [\,,\,]_+)$ on the family of maximal one generator subalgebras is a characteristical property of algebras $(\mathcal{H}_{/P}, \sigma)$ defined, over a real closed field, by a nonisotropic involution, which distinguishes them from other elements of the set $\mathcal{Q}$, and

(··) that this property of an algebra $(\mathcal{H},\sigma)$ is equivalent to the algebra being separable in the sense of the following definition.

$\vartheta \in \mathcal{F}$ is <u>separable</u> iff for every $f_1 \neq f_2 \in \vartheta(\ell)$ there is an $s \in \mathrm{Hom}(\vartheta, P)$ such that $s(f_1) \neq s(f_2)$

An algebra $(\mathcal{H},\sigma)$ is <u>separable</u> if every $\vartheta$ is separable.

## 2. Description of Chapters and the Results

This thesis consists of two chapters: in Chapter I we deal primarily with questions concerning the properties of a pair $(\vartheta, \mathrm{Hom}(\vartheta,F))$, while in chapter II we prove theorems concerning the family $\mathcal{F}$.

In section I.1 we construct a subalgebra $\vartheta(f)$ for any $f \in (\mathcal{P}_{[P]},\circ)$.[12] The subalgebra $\vartheta(f)$, being commutative and associative, belongs to the category $\mathcal{C}_F$ of commutative, associative algebras with unit (over the field F) on one generator. It is well known that a free object in this category is the polynomial algebra $F[\lambda]$ in one indeterminate $\lambda$, which means that if $\mathcal{A}(g) \in \mathcal{C}_F$ then there is a unique morphism $F[\lambda] \longrightarrow \mathcal{A}(g)$ which carries $\lambda$ into the generator $g$ and $1 \in F[\lambda]$ into the unit of $\mathcal{A}(g)$. This implies, that, in particular, there exists a unique

---

12) $(\mathcal{P}_{[P]},\circ)$ is a power associative algebra over the field $F$. All considerations in chapter I are in this, more general setting due to the fact that every substructure $(\mathcal{H}_{[P]},\sigma)$ is power associative.

homomorphism $\Psi_f : F[\lambda] \longrightarrow \mathcal{O}(f)$

$$\lambda \longrightarrow f$$

$$1 \longrightarrow I$$

As the subalgebra $\mathcal{O}(f)$ is finite dimensional the map $\Psi_f$ has a nontrivial kernel: Ker $\Psi_f = \{ v(\lambda) \mid \Psi_f(v(\lambda)) = 0 \}$. Ker $\Psi_f$ is an ideal in $F[\lambda]$ and as such it is generated by a unique monic polynomial $\mu_f(\lambda)$ .[13] This polynomial is called the minimal polynomial of $f$ .

The minimal polynomial $\mu_f(\lambda)$ contains most of the information concerning the structure of the pair $(\mathcal{O}(f), Hom(\mathcal{O}(f), F))$; therefore this section is devoted to its analysis. (The considerations in this and the next three sections are either based on or are reformulations (suited for our purposes) of certain properties of the well known concept of a factor algebra.[14]

In section I.2 we analyze the structure of $\mathcal{O}(f)$. If $\vartheta \in Hom(\mathcal{O}(f), F)$ then Ker $\vartheta$ is an ideal in $\mathcal{O}(f)$. Moreover, as $\mathcal{O}(f)$ is an algebra over the field F, the Ker $\vartheta$ must be a maximal ideal of codimension 1.[15] Thus the considerations in this section are focused on

---

[13] We refer here to the Principal Ideal Domain property of $F[\lambda]$ i.e., the fact that any ideal in it is generated by a unique monic polynomial.

[14] Greub, Linear Algebra, (New York: Springer Verlag, 1967).

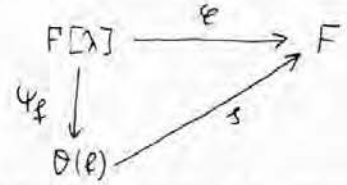
[15] For any algebra $\mathcal{A}/F$ an ideal $\mathcal{J}$ is of codimension 1 iff $\mathcal{A}/\mathcal{J}$ is a one dimensional linear space over F.

the characterization of ideals in $\theta(f)$ and relations between them. We find out that $\theta(f)$ has maximal ideals of codimension 1 iff the minimal polynomial $\mu_f(\lambda)$ has linear factors in $F[\lambda]$. (The unique factorization of $\mu_f(\lambda)$ into powers of prime factors i.e., $\mu_f(\lambda) = \pi_1^{k_1}(\lambda) \cdot \ldots \cdot \pi_s^{k_s}(\lambda)$ is discussed in section I.1.)

The next section, I.3, is devoted to the characterization of the set $Hom(\theta(f), F)$. We achieve it with the help of the set $Hom(F[\lambda], F)$. It turns out that the set $Hom(\theta(f), F)$ is isomorphic with a certain subset $Hom_{\psi_f}(F[\lambda], F)$ of the set $Hom(F[\lambda], F)$.

$Hom_{\psi_f}(F[\lambda], F) := \{ \varphi \in Hom(F[\lambda], F) \mid Ker\ \psi_f \subset Ker\ \varphi \}$

As Ker $\psi_f = (\mu_f(\lambda))$ and $(\mu_f(\lambda)) = \bigcap_i (\pi_i^{k_i}(\lambda))$ i.e., the intersection of ideals generated by powers of primes, and as Ker $\varphi = ((\lambda - \lambda_\varphi))$, the aforementioned condition Ker $\psi_f \subset$ Ker $\varphi$ is fulfilled if $(\lambda - \lambda_\varphi)$ is a factor of $\mu_f(\lambda)$. We get then the commutativity of the diagram




$s \circ \psi_f = \varphi$
$s \in Hom(\theta(f), \varphi)$

We also prove in this section (Proposition I.3) that $\theta(f)$ is separable iff $\mu_f(\lambda) = (\lambda - \lambda_1) \cdot \ldots \cdot (\lambda - \lambda_s)$ $\lambda_i \in F$

In section I.4 we introduce the idea of an abstract subalgebra $\mathcal{O}$ on one generator with the set $\mathcal{G}_\mathcal{O}$ of generators associated with it. In this new language the subalgebra $\theta(f)$ is a particular representation of the

subalgebra $\mathcal{O}$ in the basis and multiplication algorithm provided by the generator $f \in \mathcal{G}_{\mathcal{O}}$

We show (Lemma I.4) that all elements of $\mathcal{G}_{\mathcal{O}}$ have the same degrees of minimal polynomials and the same degrees, powers and splitting fields[16] E of their factors. This means that if $g, f \in \mathcal{G}_{\mathcal{O}}$ and $\mu_f(\lambda) = \pi_1^{k_1}(\lambda) \cdots \pi_s^{k_s}(\lambda)$, $\mu_g(\lambda) = \tau_1^{\ell_1}(\lambda) \cdots \tau_\nu^{\ell_\nu}(\lambda)$ then $s = \nu$ and there exists a permutation $\sigma$ of the set $\{1, \ldots, s\}$ such that $\partial(\pi_i(\lambda)) = \partial(\tau_{\sigma(i)}(\lambda))$, $k_i = \ell_{\sigma(i)}$, $E_{\pi_i} = E_{\tau_{\sigma(i)}}$.
This lemma is an important tool for proving the theorems of Chapter II.

Finally, in section I.5 we define an action induced on the family $\mathcal{F}'$ of maximal one generator subalgebras by the automorphism group of $(\mathcal{G}_{|P}, \circ)$. (The step from the family $\mathcal{F}$ to $\mathcal{F}'$ of maximal one-generator algebras is achieved by exploiting the existence of a partial ordering in $\mathcal{F}$ given by the inclusion relation and the existence of maximal elements for every chain[17] in $\mathcal{F}$.)

The content of Chapter II is the application of the framework developed in the Introduction and Chapter I to the elements of the set $\mathcal{P}$. It is important to notice that each element of the set $\mathcal{P}$ is characterized by 3 parameters: $n$, involution $J$ and the field $P$. The theorem II.1 (see below) provides the condition which stabilizes the involution and the field and places no conditions on $n$.

---

[16] The notion of a splitting field of an irreducible polynomial is introduced on the page 16.

[17] Chain in a partially ordered set is a well ordered subset of it.

Theorem II.1

The necessary and sufficient conditions for the group Aut $(\mathcal{H}_{|F})$ is be transitive (for all $n > 1$) on the family $\mathcal{F}$ associated with the algebra $(\mathcal{H}_{|F}, \sigma, \alpha, a \neq 0)$ are the following:

1. The field F has to be real closed[18] with the algebraic closure $\Omega = F(i)$

2. $(\mathcal{H}_{|F}, \sigma, \alpha, a \neq 0) = S_J(M^n_{/\Omega})$ with $J: M^n_{/\Omega} \longrightarrow M^n_{/\Omega}$ being an involution of the second kind associated with a nonisotropic hermitian form $\Gamma$.

There are essentially two real closed number fields: reals and algebraic reals P i.e., the maximum subfield of reals which does not contain transcendental numbers. (Obviously, reals and algebraic reals have different cardinalities - algebraic reals are denumerable.) Algebraically, both of them have the same properties; they differ topologically: whereas reals are complete in the topology provided by the absolute value valuation the algebraic reals are not. In the case of $F = R$ the theorem distinguishes quantum mechanical algebras, in the case of $F = P$ it suggests a new candidate to support all algebraic components of quantum mechanics.

Proposition II.13 shows that conditions 1 and 2 of the Theorem II.1 are also necessary and sufficient conditions

---

[18] See Appendix 2.

for the algebra $(\mathcal{H}_{|P}, 6, \mu)$ to be separable.

Chapter II contains another important theorem (see below) which gives the full characterization of orbits of Aut $(\mathcal{H}_{|P})$ in the family $\mathcal{F}'$ in the case of F being a real closed field and $J$ being <u>any</u> involution in $M^n_{/F(i)}$

<u>Theorem II.2</u>: Let $\mathcal{H}_{|F} = S_J(M^n_{/\Omega})$ be given where $F$ is real closed, $F(i) = \Omega$, and $J$ is an involution of the second kind, and $F = S_J(\Omega)$. Then Aut $(\mathcal{H}_{|P})$ has a finite number of orbits in $\mathcal{F}'$, uniquely described by the sets of integers $\{k_1, k_2, \ldots, k_\ell\}, \{k_{\ell+1}, \ldots, k_s\}$ which are powers of prime factors of minimal polynomials characterizing elements of a given orbit:

$$\mu(\lambda) = (\lambda - \lambda_1)^{k_1} (\lambda - \lambda_2)^{k_2} \ldots (\lambda - \lambda_\ell)^{k_\ell} \pi_{\ell+1}^{k_{\ell+1}}(\lambda) \ldots \pi_s^{k_s}(\lambda)$$

and $\pi_i(\lambda) \in F[\lambda]$ is an irreducible polynomial of the second degree. The integers $\{k_i\}_{i=1}^{s}$ fulfill the following conditions:

1. $\sum_{i=1}^{\ell} k_i + 2\sum_{i=\ell+1}^{s} k_i = n$
2. $0 \le k_i \le 2p+1$ if $i \le \ell$. $n-2p$ is a signature of the involution $J$, with $n/2 \ge p \ge 0$

   $0 \le k_i \le p$ if $i > \ell$
3. Let $\{k_{ij}\}_{1 \le i \le \ell,\ 1 \le j \le t}$ be the set of odd integers $\ge 1$ then $\sum_{j=1}^{t} k_{ij} \ge n - 2p$
4. Let $\{k_{i_1}, \ldots, k_{i_g}\} \subset \{k_1, \ldots, k_\ell\}$ where $k_{i_j} = 2b+1$, $b \ge 1$ then $\sum \frac{k_{i_j}-1}{2} + \left(\sum_{i=\ell+1}^{s} k_i\right) \le p$ and $n - \sum_{j=1}^{g}(k_{i_j}-1) + 2\sum_{i=\ell+1}^{s} k_i = g + h$ where $h$ is the number of linear primes with $k_i = 1$ in $\mu(\lambda)$

# CHAPTER I

## 1. The Minimal Polynomial

1. Let $(\mathcal{P}_F, \circ)$ be a power associative finite dimensional algebra with a unit over the field F. For any $f \in (\mathcal{P}, \circ)$ let $\mathcal{P}(f)$ be a subalgebra generated by the unit I of the algebra and the element $f$. We are interested in the set $Hom(\mathcal{P}(f), F)$. If $s \in Hom(\mathcal{P}(f), F)$ then $\ker s := \{x \in \mathcal{P}(f) \mid s(x) = 0\}$ is an ideal in $\mathcal{P}(f)$: $s(x \circ y) = s(x) \cdot s(y) = 0$ if $x \in \ker s$. By the fundamental homomorphism theorem $\mathcal{P}(f)/\ker s \simeq F$ and as $F$ is an algebraic field, and $\mathcal{P}(f)$ is a linear space over $F$ the $\ker s$ is a maximal ideal of $\mathcal{P}(f)$ of codimension 1. It follows that the existence of such ideals is a necessary condition for the set $Hom(\mathcal{P}(f), F)$ not to be empty. This fact forces one to look into the structure of the subalgebra $\mathcal{P}(f)$.

The algebra $\mathcal{P}(f)$ belongs to the category $C_F$ of commutative, associative F-algebras with an identity element on one generator. It is a well known fact that the polynomial algebra $F[\lambda]$ is a free object in this category, i.e., if $\mathcal{A}(g) \in C_F$ then there exists a unique morphism $F[\lambda] \longrightarrow \mathcal{A}(g)$

$$\lambda \longrightarrow g .$$

In particular, there exists a unique map $\psi_f : F[\lambda] \longrightarrow \mathcal{P}(f)$

$$\lambda \longrightarrow f$$
$$1 \longrightarrow I .$$

Since the subalgebra $\theta(f)$ is finite dimensional, the map $\Psi_f$ has a nontrivial kernel. $\mathrm{Ker}\,\Psi_f := \{\nu(\lambda) \in F[\lambda] \mid \Psi_f(\nu(\lambda)) = \nu(f) = 0\}$ is an ideal in $F[\lambda]$. $F[\lambda]$ is a Principal Ideal Domain: every ideal in it is generated by one element. If $\mathcal{G}_\mathcal{J}$ is the set of generators of an ideal $\mathcal{J} \subset F[\lambda]$ and if $\rho(\lambda) \in \mathcal{G}_\mathcal{J}$ then $\gamma(\lambda) \in \mathcal{G}_\mathcal{J}$ iff $\gamma(\lambda) = \alpha\,\rho(\lambda)$, $\alpha \in F$. Accordingly, there is a unique generator in $\mathcal{G}_\mathcal{J}$ which is a monic polynomial.[1] This polynomial (for $\mathcal{J} = \mathrm{Ker}\,\Psi_f$) is called the minimal polynomial of $f$; it is the monic polynomial $\mu_f(\lambda)$ of the lowest degree in $\lambda$ which vanishes when evaluated at $f$.

The minimal polynomial $\mu_f(\lambda)$ will play a fundamental role in the structure of subalgebra $\theta(f)$ and associated with it the set $\mathrm{Hom}(\theta(f), F)$; thus it is worthwhile to analyze its properties:

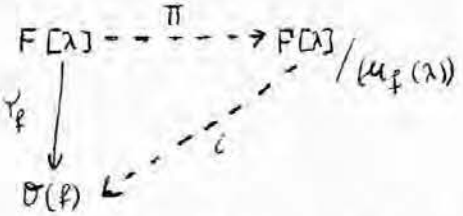
The algorithm for constructing $\mu_f(\lambda)$ is simple: if $f$ is nilpotent, i.e., if there is an integer $k>0$ with $f^k = 0$ and if $k_o$ is the smallest such integer, then $\mu_f(\lambda) = \lambda^{k_o}$. Otherwise we have $k_o$ linearly independent vectors $\{I, f, f^2, \ldots, f^{k_o-1}\}$ with $f^{k_o} \in \mathrm{Span}\{I, f, f^2, \ldots, f^{k_o-2}, f^{k_o-1}\}$. This implies that $f^{k_o} = a_0 I + a_1 f + a_2 f^2 + \ldots + a_{k-2} f^{k-2} + a_{k-1} f^{k-1}$ where not all $a_i$'s are zero; hence $\mu_f(\lambda) = \lambda^{k_o} - a_{k_o-1}\lambda^{k_o-1} - \ldots - a_1\lambda - a_0$

---

[1] A monic polynomial is a polynomial with a coefficient $a_p = 1$ if p is the highest power of $\lambda$ occurring in this polynomial.

is the polynomial of the smallest degree which vanishes when evaluated at $f$ .

The unique map $\psi_f$ factors through $F[\lambda]/(\mu_f(\lambda))$ with $\psi_f = i \circ \pi$ :




where $\pi$ is a canonical projection and $i$ is an isomorphism. The canonical map $\pi$ is defined with the help of the following <u>division algorithm</u> present in $F[\lambda]$ :

(·) there exists a map $\partial : F[\lambda] \longrightarrow \{0\} \cup N$ such that $\partial(x \cdot y) = \partial(x) + \partial(y)$

$$\partial(x+y) = \max\{\partial(x), \partial(y)\}$$

This map is called the <u>degree</u> of an element $x \in F[\lambda]$.

(··) if $x, y \in F[\lambda]$ then there exist unique polynomials $r_x, q_x \in F[\lambda]$ such that $x = y \cdot r_x + q_x$ and $\partial(q_x) < \partial(y)$ ; if $\partial(x) < \partial(y)$ then $r_x = 0$ and $q_x = x$ .

In our case, $y = \mu_f(\lambda)$ , so that for any element $x(\lambda)$ there is a unique remainder $q_{x}(\lambda)$ of this division by $\mu_f(\lambda)$ . Moreover, the division by $\mu_f(\lambda)$ defines an equivalence relation in $F[\lambda]$ : $x_1(\lambda) \sim x_2(\lambda)$ iff $q_{x_1}(\lambda) = q_{x_2}(\lambda)$ . The equivalence class of zero is an ideal $(\mu_f(\lambda))$ containing all polynomials divisible by $\mu_f(\lambda)$. Every element $x(\lambda)$ belongs to a unique coset $q_x + (\mu_f(\lambda))$

The map $\pi$ is defined now:

$$\pi : x(\lambda) \longrightarrow q_x(\lambda) + (\mu_f(\lambda))$$

The multiplication in the set of cosets is induced uniquely by $\pi$ (and therefore dependent explicitly on the minimal polynomial $\mu_f(\lambda)$ ) so as to assure the commutativity of the diagram:

$$\begin{array}{ccc} F[\lambda] \times F[\lambda] & \xrightarrow{\cdot} & F[\lambda] \\ \downarrow \pi & & \downarrow \pi \\ F[\lambda]/(\mu_f(\lambda)) \times F[\lambda]/(\mu_f(\lambda)) & \xrightarrow{\circ} & F[\lambda]/(\mu_f(\lambda)) \end{array}$$

$\cdot$ - product in $F[\lambda]$

$\circ$ - product in $F[\lambda]/(\mu_f(\lambda))$

$$\pi(x_1(\lambda) \cdot x_2(\lambda)) = \pi(x_1(\lambda)) \circ \pi(x_2(\lambda)).$$

If $\pi(x_1(\lambda)) = q_{x_1}(\lambda) + (\mu_f(\lambda))$,

$\pi(x_2(\lambda)) = q_{x_2}(\lambda) + (\mu_f(\lambda))$

then

$$\left(q_{x_1}(\lambda) + (\mu_f(\lambda))\right) \circ \left(q_{x_2}(\lambda) + (\mu_f(\lambda))\right) = \begin{cases} q_{x_1}(\lambda) \cdot q_{x_2}(\lambda) + (\mu_f(\lambda)) & \text{if } \partial(q_{x_1} q_{x_2}) < \partial(\mu_f), \\ q'(\lambda) + (\mu_f(\lambda)) & \text{if } \partial(q_{x_1} q_{x_2}) \geq \partial(\mu_f) \\ \text{where } q'(\lambda) = q_{x_1}(\lambda) \cdot q_{x_2}(\lambda) - \mu_f(\lambda) \cdot \gamma(\lambda) \\ \text{for a unique } \gamma(\lambda). \end{cases}$$

The map $i : F[\lambda]/(\mu_f(\lambda)) \longrightarrow \theta(f)$ is defined by sending $a + (\mu_f(\lambda))$ onto $a \cdot I$ for $a \in F$, $\lambda + (\mu_f(\lambda))$ onto $f$, $q(\lambda) + (\mu_f(\lambda))$ onto $q(f)$.

$i$ is an isomorphism by virtue of the fact that $\psi_f$ is a homomorphism and $i(\ker \psi_f) = i((\mu_f(\lambda))) = 0 \in \theta(f)$.

Another important property of $\mu_f(\lambda)$ is its factorization into prime factors $\mu_f(\lambda) = \pi_1^{k_1}(\lambda) \cdot \ldots \cdot \pi_s^{k_s}(\lambda)$ with $k_i > 0$ and $\sum_{i=1}^{s} \partial(\pi_i(\lambda))\, k_i = \partial(\mu_f(\lambda))$. (Prime polynomials in $F[\lambda]$ are irreducible monic polynomials.) The factorization is unique because of the Unique Factorization Domain property of $F[\lambda]$ : There are two extreme cases of this factorization:

($\cdot$) $\mu_f(\lambda) = \lambda^{k_0}$

($\cdot\cdot$) $\mu_f(\lambda)$ - irreducible in $F[\lambda]$

In the second case $F[\lambda]/(\mu_f(\lambda))$ is a field which is an algebraic extension of $F$ ; in the first case $F[\lambda]/(\mu_f(\lambda)) \simeq F \oplus \mathcal{J}$ where $\mathcal{J}$ is a nilpotent ideal generated by the coset $\lambda + (\mu_f(\lambda))$ . $\mathcal{J}$ is isomorphic to the ideal of $\mathcal{O}(f)$ generated by all F-functions of $f$ with $a_0 = 0$ . In this case $\mathcal{O}(f)$ is "furthest removed" from being an algebraic field: only elements with $a_0 \neq 0$ have inverses in $\mathcal{O}(f)$ . Generally, $a(f)$ has an inverse in $\mathcal{O}(f)$ iff $a(\lambda)$, $\mu_f(\lambda)$ are relatively prime, i.e., there are two polynomials $\chi_1(\lambda)$ , $\chi_2(\lambda) \in F[\lambda]$ such that

$$\chi_1(\lambda)\, a(\lambda) + \chi_2(\lambda)\, \mu_f(\lambda) = 1$$

In that case, we get $\chi_1(\lambda) \cdot a(\lambda) \in 1 + (\mu_f(\lambda))$ or

$\chi_1(f) \circ a(f) = I \in \mathcal{O}(f)$.

## 2. Structure of the Subalgebra $\mathcal{O}(f)$.

($\cdot$) $\mathcal{O}(f)$ is a linear space over the field $F$ of the dimension $k_0 = \partial(\mu_f(\lambda))$ . Its points are F-polynomials in $f$ of the degree $\leq k_0 - 1$ . This subalgebra is a

Principal Ideal Domain as it is a quotient object of $F[\lambda]$ and therefore all its ideals are generated by one element - some polynomial in $f$ . If $\chi(f) \in \mathcal{O}(f)$ then the necessary and sufficient condition for $\chi(f)$ to generate a proper ideal is that $\chi(f)$ have no inverse in $\mathcal{O}(f)$ . This is fulfilled iff $\chi(\lambda)$ , $\mu_f(\lambda)$ are not relatively prime, i.e., when $\chi(\lambda)$ and $\mu_f(\lambda)$ have a common factor. Hence, every ideal in $\mathcal{O}(f)$ is generated by elements

$$\pi_1^{\rho_1}(f) \cdot \cdot \cdot \pi_s^{\rho_s}(f) \quad , \quad \left(0 \le \rho_i \le k_i \quad , \quad 0 < \sum_{i=1}^{s} \rho_i < \sum_{i=1}^{s} k_i\right)$$

In particular, if $\rho_{i_0} > 1$ , we have the following inclusion relations among some of the ideals:

$$\left(\pi_{i_0}(f)\right) \supseteq \left(\pi_{i_0}^{\rho_{i_0}}(f)\right) \supseteq \left(\pi_1^{\rho_1}(f) \cdot \cdot \cdot \pi_{i_0}^{\rho_{i_0}}(f) \cdot \cdot \cdot \pi_s^{\rho_s}(f)\right)$$

The ideal $\left(\pi_{i_0}(f)\right)$ is clearly a maximal ideal since it is not contained in any other proper ideal of $\mathcal{O}(f)$ . The quotient $\mathcal{O}(f)/\left(\pi_{i_0}(f)\right)$ is therefore a field $E \supseteq F$ In particular, if $\partial(\pi_{i_0}(\lambda)) = 1$ then $\mathcal{O}(f)/\pi_{i_0}(f) \simeq F$. One can see that the canonical map

$$s' : \mathcal{O}(f) \longrightarrow \mathcal{O}(f)/\pi_{i_0}(f)$$

followed by the map $i' : \mathcal{O}(f)/\pi_{i_0}(f) \longrightarrow F$ i.e. $i' \circ s'$ is an element of $\mathrm{Hom}(\mathcal{O}(f), F)$ . Hence $\mathrm{Hom}(\mathcal{O}(f), F)$ is not empty iff $\mu_f(\lambda)$ has linear factors. (The "only if" part of this statement comes from the fact that $\ker s$ has to be the maximal ideal of codimension 1 for any $s \in \mathrm{Hom}(\mathcal{O}(f), F)$

(··) The minimal polynomial $\mu_f(\lambda)$ also serves to obtain the primary decomposition of the algebra $\mathcal{O}(f)$ .

If $\mu_f(\lambda) = \Pi_1^{k_1}(\lambda)\,\Pi_2^{k_2}(\lambda)\cdots\Pi_{s-1}^{k_{s-1}}(\lambda)\cdot\Pi_s^{k_s}(\lambda)$ let $\mu_i(\lambda) := \Pi_1^{k_1}(\lambda)\cdots\overset{\wedge}{i}\cdots\Pi_s^{k_s}(\lambda)$. The set $\{\mu_i(\lambda)\}_{i=1}^{s}$ is relatively prime which implies the existence of a set $\{\nu_i(\lambda)\}_{i=1}^{s}$ such that $\sum_{i=1}^{s}\mu_i(\lambda)\cdot\nu_i(\lambda) = 1$. This relation is mapped by the map $\Psi_f$ onto the relation $\sum_{i=1}^{s}\mu_i(f)\circ\tilde{\nu}_i(f) = I$ in the subalgebra $\mathfrak{A}(f)$, where $\tilde{\nu}_i(f) = \Psi_f(\nu(\lambda))$. It is easy to see that if $h_i(f) := \tilde{\nu}_i(f)\circ\mu_i(f)$ then $h_i(f)\circ h_j(f) = 0$ for $i \neq j$, $h_i^2(f) = h_i(f)$ and $I = \sum_{i=1}^{s} h_i(f)$. Moreover, if $f_i := f\circ h_i(f)$ then $f = \sum_{i=1}^{s} f_i$ and if $g(f)\in\mathfrak{A}(f)$ then $g(f) = \sum_i g(f_i)$ with $g(f_i)\circ g(f_j) = 0$ for $i \neq j$. This means that $\mathfrak{A}(f)$ splits into the direct sum of ideals $\mathfrak{A}_i(f_i)$ each of which is generated by $(f_i, h_i(f))$.[2]

According to our remarks in (·), for each $\mathfrak{A}_j(f_j)$ there is an element $\chi_j(f)\in\mathfrak{A}(f)$ such that $\mathfrak{A}_j(f_j) = (\chi_j(f))$. In order to find this element let us notice that for every $j$

$$\Pi_j^{k_j}(f) = \left(\Pi_j^{k_j}(f_1) + \Pi_j^{k_j}(f_2) + \cdots\overset{\wedge}{j}\cdots + \Pi_j^{k_j}(f_{s-1}) + \Pi_j^{k_j}(f_s)\right)$$

Hence, $\mu_j(f) = \prod_{i\neq j}\Pi_i^{k_i}(f) = \prod_{i\neq j}\left(\Pi_i^{k_i}(f_j) + \alpha_0^{(i)}h_j(f)\right)$ [3]

The conclusion is that $\mu_j(f)$ is the generator of $\mathfrak{A}_j(f_j)$ and $\Pi_j^{k_j}(f)$ is the generator of $\bigoplus_{i\neq j}\mathfrak{A}_i(f_i)\subset\mathfrak{A}(f)$. It is important to realize that the ideal $\mathfrak{A}_j(f_j)$ is a commutative,

---

2) The polynomial $\Pi_i^{k_i}(\lambda)$ is not the minimal polynomial of $f_i$: $\Pi_i^{k_i}(f_i) = \Pi_i^{k_i}(f\circ h_i) = \Pi_i^{k_i}(f)\circ h_i(f) + \alpha_0^{(i)}(I - h_i) = \Pi_i^{k_i}(f)\circ h_i(f) + \alpha_0^{(i)}\circ(\sum_{j\neq i}h_j(f))$ where $\alpha_0^{(i)}$ is the coefficient of zero power of $\lambda$ in the polynomial $\Pi_i^{k_i}(\lambda) = \lambda^{\ell}+\cdots+\alpha_0^{(i)}$. As $h_i(f) = \tilde{\nu}_i(f)\circ\mu_i(f)$ we get $\Pi_i^{k_i}(f_i) = \Pi_i^{k_i}(f)\circ h_i(f) + \alpha_0^{(i)}(\sum_{j\neq i}h_j(f)) = \Pi_i^{k_i}(f)\circ\tilde{\nu}_i(f)\circ\mu_i(f) + \alpha_0^{(i)}(\sum_{j\neq i}h_j(f)) = \tilde{\nu}_i(f)\circ\mu_f(f) + \alpha_0^{(i)}(\sum_{j\neq i}h_j(f)) = 0 + \alpha_0^{(i)}(\sum_{j\neq i}h_j(f))$ so that the minimal polynomial of $f_i$ is $\lambda\cdot\Pi_i^{k_i}(\lambda)$. (We have to multiply $\Pi_i^{k_i}(\lambda)$ by $\lambda$ to get the vanishing of the term $\alpha_0^{(i)}(\sum_{j\neq i}h_j)$.)

3) $\alpha_0^{(i)}$ is the coefficient of the zero power of $\lambda$ in the polynomial $\Pi_i^{k_i}(\lambda)$.

associative algebra with an identity element being $\eta_0(f)$. It is not, however, the subalgebra of $\mathcal{O}(f)$ nor of $(\mathcal{P}, \circ)$: their identity elements are different. This is the reason that $\Pi_i^{k_i}(\lambda)$ is only "almost" the minimal polynomial of $f_i$. The definition of minimal polynomial refers explicitly to the unit I of $\mathcal{O}(f)$ and not $h_i \in \mathcal{O}_i(f)$ so that $\mu_{f_i}(\lambda) = \lambda \Pi_i^{k_i}(\lambda)$.

However, if we are interested in the structure of $\mathcal{O}_i(f_i)$[4] independently of $\mathcal{O}(f)$, then $\mathcal{O}_i(f_i)$ is fully described by the map $\Psi_i : F[\lambda] \longrightarrow \mathcal{O}_i(f_i)$ with $\operatorname{Ker} \Psi_i = (\Pi_i^{k_i}(\lambda))$

$$\lambda \longrightarrow f_i$$
$$1 \longrightarrow h_i(f)$$

The algebra $\mathcal{O}_i(f_i)$ has several ideals, each of them generated by $\Pi_i^{\ell}(f_i)$, $1 \le \ell \le k_i$ and fulfilling the relations $(\Pi_i^{\ell}(f_i)) \supset (\Pi_i^{\ell+1}(f_i))$. This implies that $\Pi_i(f_i)$ generates a maximal ideal in $\mathcal{O}_i(f_i)$. As $0 \neq \Pi_i(f_i)$ is nilpotent of degree $k_i > 1$, $(\Pi_i(f_i))$ is a maximal nilpotent ideal of $\mathcal{O}_i(f_i)$. The maximality of $(\Pi_i(f_i))$ implies the existence of the map $\varphi_i : \mathcal{O}_i(f_i) \longrightarrow E \supseteq F$ where $\operatorname{Ker} \varphi_i = (\Pi_i(f_i))$ and E is an algebraic extension of . By the fundamental homomorphism theorem we have $\mathcal{O}_i(f_i) \simeq \operatorname{Ker} \varphi_i \oplus \mathcal{O}_i(f_i)/(\Pi_i(f_i))$. In the case $\Pi_i(f) = (f - \lambda_i), \lambda_i \in F$ we get $\mathcal{O}_i(f_i) \simeq (f - \lambda_i) \oplus \mathcal{O}_i(f_i)/(\Pi_i(f))$ with $\mathcal{O}_i(f_i) \ni f_i = (f_i - \lambda_i) \oplus \lambda_i$, $\nu(f_i) = \nu'(f_i) \oplus \nu(\lambda_i)$ where $\nu'(f_i) \in (f - \lambda_i)$.

We will apply now this result to the analysis of $\mathcal{O}(f)$.

4) Henceforth the subalgebra of $\mathcal{O}(f)$ generated by $(f_i, I)$ will be denoted by $\mathcal{O}(f_i)$, and the algebra generated by $(f_i, h_i)$ will be denoted by $\mathcal{O}_i(f_i)$.

Suppose again that $k_i > 1$ for some $i$ so that $(\pi_i^{k_i}(f)) = \bigoplus_{j \neq i} \mathcal{O}_j(f_j)$ is an ideal in $\mathcal{O}(f)$. It is contained in the maximal ideal $(\pi_i(f)) = \bigoplus_{j \neq i} \mathcal{O}_j(f_j) \oplus (\pi_i(f_i)) \cdot h_i$.

In the linear case, we again have the splitting $\mathcal{O}(f) = \bigoplus_{j \neq i} \mathcal{O}_j(f_j) \oplus \mathcal{O}_i(f) =$

$= \bigoplus_{j \neq i} \mathcal{O}_j(f_j) \oplus ((f - \lambda_i)) \cdot h_i \oplus \mathcal{O}_i(f_i)/(\pi_i(f_i)) \cdot h_i$

with $\mathcal{O}(f) \ni f = \sum_{j \neq i} f_j h_j + (f_i - \lambda_i) h_i + \lambda_i h_i$

$$1 = \sum_{j \neq i} h_j + h_i$$

$$v(f) = \sum_{j \neq i} v(f_j) + v'(f_i - \lambda_i) h_i + v(\lambda_i) h_i \qquad v(\lambda_i) \in F$$

and $\sum_{j \neq i} v(f_j) + v(f_i - \lambda) \in ((f - \lambda_i))$.

3. The Set $Hom(\mathcal{O}(f), F)$.

In order to characterize the set $Hom(\mathcal{O}(f), F)$ we need to investigate the relation between the ideals of $F[\lambda]$ and those of $\mathcal{O}(f)$. Let $(v(\lambda))$ be an ideal in $F[\lambda]$. This ideal can be mapped by $\psi_f$ onto:

1. all of algebra $\mathcal{O}(f)$ iff $v(\lambda)$, $\mu_f(\lambda)$ are relatively prime, for then $\tilde{v}(f) = \psi_f(v(\lambda))$ has an inverse in $\mathcal{O}(f)$;

2. zero iff $v(\lambda) \in (\mu_f(\lambda))$

3. a proper ideal of $\mathcal{O}(f)$ iff $v(\lambda)$, $\mu_f(\lambda)$ are not relatively prime. To see the latter, let $\omega(\lambda) =$ $= \text{g. c. d.} \{v(\lambda), \mu_f(\lambda)\}$ i.e., $v(\lambda) = \omega(\lambda) \cdot x_1(\lambda)$ and $\mu_f(\lambda) = \omega(\lambda) x_2(\lambda)$. This implies, of course, that $x_1(\lambda)$, $x_2(\lambda)$ are relatively prime, so that there are $y_1(\lambda)$, $y_2(\lambda)$ with

$$x_1(\lambda) y_1(\lambda) + x_2(\lambda) y_2(\lambda) = 1 \quad \text{or}$$

$$v(\lambda) y_1(\lambda) + \mu_f(\lambda) y_2(\lambda) = \omega(\lambda)$$

which is mapped by $\psi_f(\lambda)$ onto

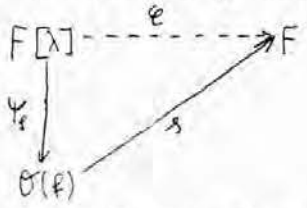
$$\tilde{v}(f) \circ \tilde{y}_1(f) = \omega(f) \in \mathcal{O}(f) \qquad (*)$$

This implies that $\tilde{\nu}(f) = (\omega(f))$, for $(\tilde{\nu}(f)) \subseteq (\omega(f))$ as homomorphic images of the ideals $(\nu(\lambda))$, $(\omega(\lambda))$ which fulfill the relation $(\nu(\lambda)) \subset (\omega(\lambda))$, and $(\hat{\nu}(f)) \supseteq (\omega(f))$ by (*). Consequently every ideal in $\mathcal{O}(f)$ is an image of several ideals in $F[\lambda]$. If $(\omega(f)) = (\pi_1^{p_1}(f) \cdot \pi_2^{p_2}(f) \cdot \ldots \cdot \pi_{s-1}^{p_{s-1}}(f) \cdot \pi_s^{p_s}(f))$, $0 \le p_i \le k_i$ is an ideal in $\mathcal{O}(f)$ and if $\mathcal{K}_{\omega(f)} := \{ \mathcal{J} \subset F[\lambda] \mid \Psi_f(\mathcal{J}) = (\omega(f)) \}$ then each element of $\mathcal{K}_{\omega(f)}$ is generated by a multiple of $\omega(\lambda)$. Hence $\mathcal{K}_{\omega(f)}$ is partially ordered by inclusion; with the maximal element being $(\omega(\lambda))$. In particular, if $\mu_f(\lambda)$ has a linear factor $(\lambda - \lambda_i)^{k_i}$ then $((f - \lambda_i)^{k_i})$ is an image of ideals $((\lambda - \lambda_i)^{\ell})$ $\ell \ge k_i$.

With the help of all those results we will now characterize the set $Hom(\mathcal{O}(f), F)$.

Lemma I.1: The set $Hom(\mathcal{O}(f), F)$ is isomorphic to the subset $Hom_{\Psi_f}(F[\lambda], F)$ of $Hom(F[\lambda], F)$ with the property:
$\varphi \in Hom_{\Psi_f}(F[\lambda], F)$ iff $\ker \Psi_f \subset \ker \varphi$.

Proof: To prove the lemma it is enough to show that for every $s \in Hom(\mathcal{O}(f), F)$ there is a unique $\varphi \in Hom(F[\lambda], F)$ satisfying the following diagram:

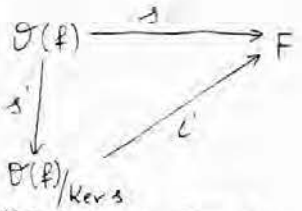



(*)

The necessary conditions for the commutativity of this diagram are: $\ker \Psi_f \subset \ker \varphi$, $\Psi(\ker \varphi) \subseteq \ker s$.

Therefore, we have to find an ideal of $F[\lambda]$ which satisfies those conditions and which can serve as a kernel of a homomorphism of $F[\lambda]$ onto $F$. If $\ker s = (\!(f-\lambda_s)\!)$ then the ideals which fulfill the second condition are elements of the set $\mathcal{J}_{(f-\lambda_s)}$. There is a unique element in $\mathcal{J}_{(f-\lambda_s)}$ which fulfills also the first condition; it is the maximal element of $\mathcal{J}_{(f-\lambda_s)}$ equal to $(\!(\lambda-\lambda_s)\!) \subset F[\lambda]$. Let then $(\!(\lambda-\lambda_s)\!)$ be the kernel of $\varphi$. Having defined the kernel of the homomorphism of $F[\lambda]$ onto $F$ we have uniquely defined also the homomorphism itself: if $\ker\varphi = (\!(\lambda-\lambda_s)\!)$ then $\varphi(v(\lambda)) = v(\lambda_s) \in F$ (by the uniqueness of the division algorithm).

On the other hand, if $\ker s = (\!(f-\lambda_s)\!) \subset \mathcal{O}(f)$ then $\ker s = \bigoplus_{i\neq s} \mathcal{O}_i(f_i) \oplus (\!(f-\lambda_s)\!)\cdot h_s$ (by the arguments in the section I.2). Hence, we get the canonical splitting of the map $s$:




with $s'(\tilde{v}(f)) = \tilde{v}(\lambda_s)\cdot h_s + \ker s$

and $i'(h_s) = 1 \in F$, $i'(\ker s) = 0$.

We now obtain $s(\tilde{v}(f)) = (i'\circ s')(\tilde{v}(f)) = i'(\tilde{v}(\lambda_s)h_s + \ker s) =$

$= i'(\tilde{v}(\lambda_s)\cdot h_s) = \tilde{v}(\lambda_s) = v(\lambda_s)$ for $v(\lambda) \in \tilde{v}(\lambda) + (\!(\lambda-\lambda_s)\!)$

which shows that the conditions above are also sufficient for the commutativity of the diagram (*).

Let now $\varphi \in Hom_{\Psi_f}(F[\lambda], F)$ be given with the kernel $((\lambda - \lambda')) \supset Ker\, \Psi_f$. This can be true iff $\lambda' = \lambda_i$ where $1 \leq i \leq \ell$, whereupon $\Psi_f(Ker\, \varphi) = Ker\, s_i$.

□

Definition I.2: A subalgebra $\mathcal{O}(f)$ is separable iff for every $f_1, f_2 \in \mathcal{O}(f)$ such that $f_i \notin F \cdot I$ there exists $s \in Hom(\mathcal{O}(f), F)$ with $s(f_1) \neq s(f_2)$. An algebra $(\mathcal{P}, \circ)$ is separable iff $\mathcal{O}(f)$ is separable for every $f \in \mathcal{P}$

Let us notice first that $\mathcal{O}(f)$ is separable iff $\bigcap_{s \in Hom(\mathcal{O}(f), F)} Ker\, s = \emptyset$ for if there is $f_1 \neq f_2 \in \mathcal{O}(f)$ such that $s(f_1) = s(f_2)$ for all $s$ then $0 \neq f_1 - f_2$ is mapped onto zero by all homomorphisms: $s(f_1 - f_2) = s(f_1) - s(f_2) = 0$

Let $\mathcal{U} \subset \mathcal{O}(f)$ be the set of elements in a nonseparable subalgebra $\mathcal{O}(f)$ such that if $x \in \mathcal{U}$ then $s_i(x) = s_j(x)$ $i \neq j$ for all $s \in Hom(\mathcal{O}(f), F)$. It is clear that $\mathcal{U}$ is a subalgebra of $\mathcal{O}(f)$ containing $F \cdot I$ and that there is an equivalence relation in $\mathcal{U}$ given by: $x_1 \sim x_2$ iff $s(x_1) = s(x_2)$. The equivalence relation defines an ideal $\mathcal{J}$ in $\mathcal{U}$ equal to $\bigcap_s Ker\, s$ and the set of cosets $\{a I + \mathcal{J} \mid a \in F\}$. The elements of each coset are "indistinguishable" by the homomorphisms. In this framework we notice an interesting role that constants play in such subalgebra: if $x_1, x_2$ are elements of one coset $\neq \mathcal{J} + 0 \cdot I$ then $ax_1, bx_2$ belong to different cosets. In other words if $x_1, x_2$ are indistinguishable then $ax_1, bx_2$ are always distinguished by homomorphisms.

The only elements which cannot be distinguished by constants are the elements of $\mathcal{J} = \bigcap_s \operatorname{Ker} s$.

Proposition I.3: $\mathcal{O}(f)$ is separable iff it is characterized by the minimal polynomial $\mu_f(\lambda) = (\lambda - \lambda_1)\cdot(\lambda - \lambda_2)\cdot\ldots\cdot(\lambda - \lambda_\sigma)$

Proof: Suppose that $\mu_f(\lambda) = (\lambda - \lambda_1)^{k_1}\cdot\ldots\cdot(\lambda - \lambda_\varrho)^{k_\varrho}\cdot\pi_{\varrho+1}^{k_{\varrho+1}}(\lambda)\cdot\ldots\cdot\pi_\sigma^{k_\sigma}(\lambda)$ where at least one power $k_{i_0}$ is $> 1$ for $1 \le i_0 \le \varrho$ and $k_{j_0} \ge 1$ for $\varrho+1 \le j_0 \le \sigma$.

Then the element $(f - \lambda_{i_0}) \in \bigcap_s \operatorname{Ker} s$, $s \in \operatorname{Hom}(\mathcal{O}(f), F)$. To see this it must be noted that $\operatorname{Ker}_{i \neq i_0} s_i = (\!(\lambda - \lambda_i)\!)$ so that

$$(f - \lambda_{i_0})\cdot h_i \in \mathcal{O}_{i_0}(f_{i_0})$$

which is contained in every $\operatorname{Ker}_{i \neq i_0} s_i$. On the other hand $\operatorname{Ker} s_{i_0} = (f - \lambda_{i_0})\circ h_{i_0} \oplus_{i \neq i_0} \mathcal{O}_i(f_i)$ so that $(f - \lambda_{i_0}) \in \operatorname{Ker} s_{i_0}$ as well. Similarly, the element $0 \neq \mu_{f_{j_0}}(f) = (f - \lambda_1)^{k_1}\cdot\ldots\cdot(f - \lambda_\varrho)^{k_\varrho}\cdot\pi_1^{k_1}(f)\cdot\ldots\cdot\hat{}\cdot\ldots\cdot\pi_s^{k_s}(f) \subset \bigcap_{i=1}^{\varrho} (\!(f - \lambda_i)\!) = \bigcap_s \operatorname{Ker} s$.

Further, let $\mu_f(\lambda) = (\lambda - \lambda_1)\cdot(\lambda - \lambda_2)\cdot\ldots\cdot(\lambda - \lambda_\sigma)$. This means that if $f = \sum_{i=1}^{\sigma} f_i$ then $\mu_{f_i}(\lambda) = (\lambda - \lambda_i)$ for $f_i \in \mathcal{O}_i(f_i)$ which means that $(f_i - \lambda_i)\circ h_i = 0$. Hence $f = \sum_i \lambda_i \cdot h_i(f)$ and for any $g(f) \in \mathcal{O}(f)$ $g(f) = \sum_i g(\lambda_i)\circ h_i(f)$. As $\operatorname{Ker} s_j = \oplus_{i \neq j} \mathcal{O}_i(f)$ we get $\bigcap_{s_i} \operatorname{Ker} s_i = \mathcal{O}$. □

4. Generators of a one-generator subalgebra.

The set of vectors $\{I, f, f^2, \ldots f^{k_0 - 1}\}$ plays a dual role in the subalgebra $\mathcal{O}(f)$. On the one hand it provides a linear basis in the underlying linear subspace; on the other, it provides, through the minimal polynomial $\mu_f(\lambda)$ an algorithm for the multiplication table in $\mathcal{O}(f)$. (See Section I.1).

In other words this basis is specially adapted for the representation of the algebra $\mathcal{O}(f)$ as an algebra on one generator (In this case, the generator $f$). There are, however, other bases in $\mathcal{O}(f)$ which have the same property; each of them is generated by different generators of the subalgebra $\mathcal{O}(f)$. This implies that the proper way of expressing our ideas is to introduce an algebra on one generator $\mathcal{O}$ with the set of generators $\mathcal{G}_{\mathcal{O}}$ attached to it. To pick a generator $h \in \mathcal{G}_{\mathcal{O}}$ is equivalent to picking the particular representation $\mathcal{O}(h)$ of the subalgebra $\mathcal{O}$ in the basis $\{I, h, h^2, \ldots, h^{k_0-1}\}$ and with the multiplication algorithm contained in $\mu_h(\lambda)$. We will show now that the change of generators in $\mathcal{O}$ is equivalent to an automorphism in $\mathcal{O}$. Later we will give a generator-invariant characterization of $\mathcal{O}$ and prove that for any two generators $f, g \in \mathcal{G}_{\mathcal{O}}$ $\mathrm{Hom}(\mathcal{O}(f), F) = \mathrm{Hom}(\mathcal{O}(g), F) \equiv \mathrm{Hom}(\mathcal{O}, F)$

Let $g, f \in \mathcal{G}_{\mathcal{O}}$. Then, in particular $g = g(f) = g_0 I + g_1 f + \ldots + g_t f^t$ with some $g_i \neq 0$. Let $\mu_f(\lambda)$, $\mu_g(\lambda)$ be their minimal polynomials. Obviously $\partial(\mu_f(\lambda)) = \partial(\mu_g(\lambda))$ since ideals generated by both of them have to have equal codimension. Let $\mu_g(\lambda) = \lambda^{k_0} + b_{k_0-1}\lambda^{k_0-1} + \ldots + b_1\lambda + b_0 I$ so that $b_0 I + b_1 g + \ldots + b_{k_0} g^{k_0} = 0$ Let $r$ be the smallest integer for which $r+1 \geq k_0$

Then

$$
\begin{aligned}
g^{k_0}(f) &= \gamma^0_{k_0}(f)\,\mu_f(f) + \gamma^1_{k_0}(f) \\
&\vdots \\
g^{r}(f) &= \gamma^0_{r}(f)\,\mu_f(f) + \gamma^1_{r}(f) \\
g^{r-1}(f) &= \gamma^1_{r-1}(f) \qquad \text{with } \partial(\gamma^1_i(\lambda)) < k_0 \\
&\vdots \\
g(f) &= \gamma^1_1(f)
\end{aligned}
$$

We get $0 \equiv b_0 I + b_1 g + \ldots + b_{k_0} g^{k_0} =$

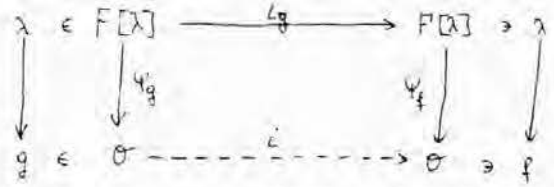
$= \mu_f(f)\left(b_0 \delta_N^0(f) + \ldots + b_{k_0} \delta_{k_0}^{k_0}(f)\right) + b_0 I + b_1 \delta_1'(f) + \ldots + b_{k_0} \delta_{k_0}'(f)$

This is satisfied iff $b_0 I + b_1 \delta_1' + \cdots + b_{k_0} \delta_{k_0}'(f) = 0$

Hence, if $\beta(\lambda) = g_0 + g_1\lambda + \cdots + g_{t-1}\lambda^{t-1} + g_t\lambda^t$ then $\mu_g(\beta) \equiv \mu_g(\beta(\lambda)) =$

$\nu(\lambda)\,\mu_f(\lambda) = \mu_g(\lambda)$ or $\mu_g(\lambda) \in (\mu_f(\lambda))$.

Let us now consider the following diagram:




where $\iota_g$ : $F[\lambda] \longrightarrow F[\lambda]$ is an injection into $F[\lambda]$

$\lambda \longrightarrow \beta(\lambda)$

$1 \longrightarrow 1$

We see that $\iota_g(\ker \psi_g) \subset \ker \psi_f$ as $i(\mu_f(\lambda)) = \mu_g(i(\lambda)) = \mu_g(\beta) =$

$= \mu_g(\lambda) \in (\mu_f(\lambda))$, and that there is a unique $i$: $\mathfrak{G} \longrightarrow \mathfrak{G}$

( $i(g) = g(f)$ , $i(I) = I$ ) which makes this diagram

commutative. $i(h_1(g) \circ h_2(g)) = (i \circ \psi_g)(h_1(\lambda) \cdot h_2(\lambda)) = (\psi_f \circ \iota_g)(h_1(\lambda)\, h_2(\lambda)) = (\psi_f \circ \iota_g)(h_1(\lambda)) \circ (\psi_f \circ \iota_g)(h_2(\lambda)) = (i \circ \psi_g)(h_1(\lambda)) \circ (i \circ \psi_g)(h_2(\lambda))$

$= i(h_1(g)) \circ i(h_2(g))$, whereby $i$ is a homomorphism; since $i(h(g)) = h'(f) = 0$ iff $h'(f) = \mu_f(f)$

$i$ is an automorphism of $\mathfrak{G}$ . The proof is symmetric with respect to the exchange of $f$ with $g$ ; of course, the direction of the arrows of $\iota_g$ , $i$ changes accordingly. In a more general case, i.e., when $f \in \mathfrak{G}_\sigma$ , $g \notin \mathfrak{G}_\sigma$ so that when $g$ generates a proper subalgebra $\mathfrak{G}'$ of $\mathfrak{G}$ , the above diagram gives us an injection of $\mathfrak{G}'$ into $\mathfrak{G}$.

We will now prove

Lemma I.4: (The generator-invariant characterization of $\mathcal{O}$). All elements of $\mathcal{G}_\mathcal{O}$ have the same degrees of minimal polynomials, the same degrees and powers of their irreducible factors and the same splitting fields;[5] i.e., if $g, f \in \mathcal{G}_\mathcal{O}$ and

$$\mu_f(\lambda) = \pi_1^{k_1}(\lambda) \cdot \ldots \cdot \pi_s^{k_s}(\lambda)$$
$$\mu_g(\lambda) = \tau_1^{\ell_1}(\lambda) \cdot \ldots \cdot \tau_r^{\ell_r}(\lambda)$$

Then $r = s$ and there exists a permutation $\sigma$ on the set $\{1, 2, 3, \ldots, s\}$ such that

$$\partial(\pi_i(\lambda)) = \partial(\tau_{\sigma(i)}(\lambda))$$
$$k_i = \ell_{\sigma(i)}$$
$$E_{\pi_i} = E_{\tau_{\sigma(i)}}$$

Proof: Let $\mathcal{O}(f) = \bigoplus_{i=1}^{s} \mathcal{O}_i(f_i)$ be the primary decomposition of the subalgebra $\mathcal{O}$ in the representation $\mathcal{O}(f)$ with $f = \sum_{i=1}^{s} f_i$, $I = \sum_{i=1}^{s} h_i(f)$. We have shown before that the minimal polynomial of $f_i$ in $\mathcal{O}_i(f_i)$ is $\pi_i^{k_i}(\lambda)$ so that

$$\mathcal{O}_i(f_i) \simeq F[\lambda]/(\pi_i^{k_i}(\lambda)) \quad \text{with} \quad \varphi_{f_i} : F[\lambda] \longrightarrow \mathcal{O}_i(f_i)$$
$$\lambda \longrightarrow f_i$$
$$1 \longrightarrow h_i(f)$$

Since $g \in \mathcal{O}$, we also have a unique decomposition: $g = \sum_{i=1}^{s} g_i$. Let $\mu_{g_i}(\lambda)$ be the minimal polynomial of $g_i \in \mathcal{O}_i(f_i)$. Then $\partial(\mu_{g_i}(\lambda)) \leq \partial(\mu_{f_i}(\lambda))$ and as $g \in \mathcal{G}_\mathcal{O}$, $\mu_g(\lambda) = \text{l. c. m.}\{\mu_{g_i}(\lambda)\}$[6] we obtain $g_i \neq g_j$ for $i \neq j$ and $\partial(\mu_{g_i}(\lambda)) = \partial(\pi_i^{k_i}(\lambda))$. Hence, what is left to prove is that for every $i = 1, 2, \ldots, s$ there is a polynomial

---

[5] A splitting field $E_\pi \supset F$ of an irreducible polynomial $\pi(\lambda) \in F[\lambda]$ is the smallest overfield of $F$ containing all roots of $\pi(\lambda)$; equivalently, it is the smallest field in which $\pi(\lambda)$ splits into powers of linear factors.

[6] N. Jacobson, Linear Algebra (New York: D. Van Nostrand Company, Inc., 1953), Chapter III.

$\tau_i(\lambda) \in F[\lambda]$ such that $\partial(\pi_i(\lambda)) = \partial(\tau_i(\lambda))$ with $E_{\pi_i} = E_{\tau_i}$. This will show, of course, that $\mu_{g_i}(\lambda) = \tau_i^{k_i}(\lambda)$

Let $\mu_{f_i}(\lambda) = \pi_i^{k_i}(\lambda)$, $\mu_{g_i}(\lambda) = \tau_i^{k_i}(\lambda)$ with $k_i > 0$ and $\tau_i(\lambda)$ unspecified. Let $F(\xi_1, \ldots, \xi_m)$ be the splitting field of $\pi_i(\lambda)$ so that $F(\xi_1 \ldots \xi_m)[\lambda] \supset F[\lambda] \ni \mu_{f_i}(\lambda) = (\lambda - \xi_1)^{a_1 k_i} \cdot \ldots \cdot (\lambda - \xi_m)^{a_m \cdot k_i}$.

Since $\partial(\mu_{f_i}(\lambda)) = \partial(\mu_{g_i}(\lambda))$ both of $f_i, g_i \in \mathcal{G}_{\sigma_i}$ and $\mathcal{O}_i(g_i) \simeq \mathcal{O}_i(f_i)$.

If

$$\begin{array}{ccc} F[\lambda] & \xrightarrow{i_{g_i}} & F[\lambda] \\ \downarrow \Psi_{g_i} & & \downarrow \Psi_{f_i} \\ \mathcal{O}_i(g_i) & \xrightarrow{\quad\iota\quad} & \mathcal{O}_i(f_i) \end{array}$$

$$\Psi_{g_i}: \begin{array}{ccc} F[\lambda] & \longrightarrow & \mathcal{O}_i(f_i) \\ \lambda & \longrightarrow & f_i \\ 1 & \longrightarrow & h_i \end{array} \qquad \Psi_{f_i}: \begin{array}{ccc} F[\lambda] & \longrightarrow & \mathcal{O}_i(g_i) \\ \lambda & \longrightarrow & g_i \\ 1 & \longrightarrow & h_i \end{array}$$

is the diagram giving the automorphism $i$, let $i_{g_i}(\lambda) = \beta_i(\lambda) = g_0 + g_1\lambda + \ldots + g_n\lambda^n$. $i(\mu_{g_i}(\lambda)) = \mu_{g_i}(i(\lambda)) = \mu_{g_i}(\lambda) = \nu(\lambda)\,\mu_{f_i}(\lambda)$.

We have

$$\beta_i(\lambda) = \beta_i(\lambda; \xi_1)(\lambda - \xi_1) + \gamma_1$$

where $\gamma_i \in F(\xi_1, \ldots, \xi_m)$ is unique by the division algorithm.

$\beta_i(\lambda; \xi_1)$ is a function of $\lambda$ and $\xi_1$.

Hence, $(\beta_i(\lambda) - \gamma_i) = \beta_i(\lambda; \xi_1)(\lambda - \xi_1)$.

$\beta_i(\lambda, \xi_1)$ might be a multiple of some other factors of $\mu_{f_i}(\lambda)$ so that generally if $I := \{1, 2, \ldots, (k_i \partial(\pi_i))\}$ we have a family of subsets $I_\omega$ of $I$ such that $I_i \cap I_j = \emptyset$ and

$$(\beta_i - \gamma_\omega) = \beta_\omega(\lambda_i; \xi_{\omega_1}, \ldots, \xi_{\omega_{p(\omega)}})(\lambda - \xi_{\omega_1})^{e_{\omega_1}} \cdot \ldots \cdot (\lambda - \xi_{\omega_{p(\omega)}})^{e_{\omega_{p(\omega)}}}$$

where $\omega_i \in I_\omega$, $e_{\omega_j} \leq a_j \cdot k_i$ and $p(\omega)$ is the cardinality of $I_\omega$. Let us take (for every $\omega$) $d_\omega := \max_j \left\{ A\left(\frac{a_j \cdot k_i}{e_{\omega_j}}\right) \right\}$

where

$$A\left(\frac{a_j \cdot k_i}{e_{\omega_j}}\right) = \begin{cases} \dfrac{a_j \cdot k_i}{e_{\omega_j}} & \text{(if it is an integer)}, \\ E\left(\dfrac{a_j \cdot k_i}{e_{\omega_j}}\right) = \text{the smallest integer} > \dfrac{a_j \cdot k_i}{e_{\omega_j}} & \\ \text{(if } \dfrac{a_j k_i}{e_{\omega_j}} \text{ is } \underline{\text{not}} \text{ an integer).} & \end{cases}$$

One notices that $A\left(\frac{a_j \cdot k_i}{e_{\omega_j}}\right) \geq a_j \cdot k_i$ with equality iff $e_{\omega_j} = 1$. It follows that $\prod_{\omega} (\beta_i(\lambda) - \zeta_\omega)^{d_\omega} = B(\lambda; \xi_1, \dots, \xi_m)\, \mu_{g_i}(\lambda)$. Obviously $\mu_{g_i}(\lambda)$ contains all factors $(\beta_i(\lambda) - \zeta_\omega)$, because $\mu'_{g_i}(\lambda) = \nu(\lambda)\, \mu_{f_i}(\lambda)$. Moreover it has to contain the powers $(\beta_i(\lambda) - \xi_\omega)^{d_\omega}$, for only then it is a multiple of $\mu_{f_i}(\lambda)$ (by construction).

On the other hand $\mu_{g_i}(\beta(\lambda))$ is the polynomial of the minimal degree which vanishes when evaluated at $g = g(f)$. Hence $\prod_{\omega} (\beta_i(\lambda) - \zeta_\omega)^{d_\omega} = \mu'_{g_i}(\lambda)$. This implies that $E_{\pi_i} \geq E_{\tau_i}$ and by symmetry with respect to $g_i, f_i$ we get $E_{\pi_i} = E_{\tau_i}$

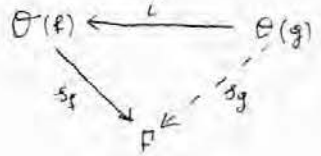
The degree of $\prod_{\omega} (\beta(\lambda) - \zeta_\omega)^{d_\omega}$ is equal to $\sum_{\omega} d_\omega =$

$$= \sum_{\omega} \max_j \left\{ A\left(\frac{a_j \cdot k_i}{e_{\omega_j}}\right) \right\} \leq \sum_{\omega} \sum_{\delta=1}^{N(\omega)} A\left(\frac{a_j \cdot k_i}{e_{\omega_j}}\right) \leq \sum_{\delta=1}^{m} a_j \cdot k_i .$$

The second inequality becomes an equality iff $e_{\omega_j} = 1$ for all $\omega_j$'s ; the first inequality becomes an equality iff $p(\omega) = 1$ for every $\omega$. Hence $\sum_{\omega} d_\omega \equiv \partial_\lambda \mu_{g_i}(\beta(\lambda)) = \partial_\lambda (\mu_{f_i}(\lambda))$ iff $d_\omega = d_j = a_j \cdot k_i$ so that $\prod_{\omega} (\beta - \zeta_\omega)^{d_\omega} = \prod_{\omega} [(\beta(\lambda) - \zeta_\omega)^{a_j}]^{k_i}$ $= \tau_i(\beta(\lambda))^{k_i}$ with $\partial_\beta(\tau_i(\beta)) = \partial_\lambda(\pi_i(\lambda))$.

□

Corollary I.5: Let $f, g \in \mathcal{G}_\theta$ and $\theta(g)$, $\theta(f)$ be the representations of the subalgebra $\theta$ in, respectively, $f, g$ generated bases. Then for every $s_f \in \mathrm{Hom}(\theta(f), F)$ there is a unique $s_g \in \mathrm{Hom}(\theta(g), F)$ such that the diagram

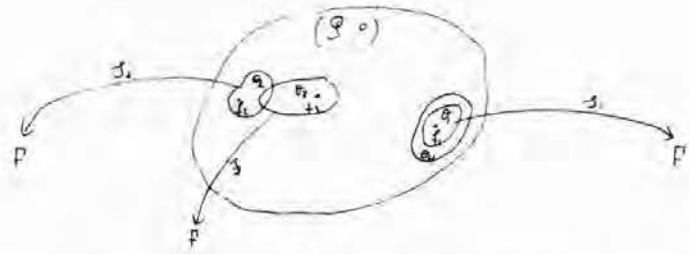



commutes.

Proof: The existence of a homomorphic map $s_g$ is trivial. $s_g := s_f \circ \iota$. Let $\mathrm{Ker}\, s_f = \langle\!\langle f - \lambda_0 \rangle\!\rangle$. Then $s_f(g(f)) = g(\lambda_0) \in F$ and $\mathrm{Ker}\, s_g := \langle\!\langle g - g(\lambda_0) \rangle\!\rangle$ which by Lemma I.4 exists and is unique. Moreover $\iota(g - g(\lambda_0)) = (\iota(g) - g(\lambda_0)) = (g(f) - g(\lambda_0)) = (g'(f)(f - \lambda_0) + g(\lambda_0) - g(\lambda_0)) = g'(f)(f - \lambda_0)$. By Lemma I.4 $g'(\lambda)$ and $\mu_f(\lambda)$ are relatively prime so that $(g'(f)(f - \lambda_0)) = (f - \lambda)$ (by point 3 in section I.3 of this chapter). □

This way one arrives at the generator-invariant characterization of a one-generator algebra $\mathcal{O}$: $\mathcal{O}$ is characterized by the degree of the minimal polynomial of any of its generators, the degrees, powers and splitting fields of its prime factors. With each algebra $\mathcal{O}$ there is associated a set $\mathrm{Hom}(\mathcal{O}, F)$ which again, does not depend on a particular generator. Every generator $f \in \mathcal{G}_{\mathcal{O}}$ defines a particular linear basis and a multiplication algorithm which is designed explicitly to exhibit $\mathcal{O}$ as an algebra $\mathcal{O}(f)$ on the generator $f$. (In other words, to choose a generator "means" to give a particular name to the algebra $\mathcal{O}$.)

The global picture we are now obtaining is that of the algebra $(\mathcal{P}_{/p}, \circ)$ completely covered by the family $\mathcal{F}$ of subalgebras on one generator. Each element $f \in \mathcal{P}$ belongs to at least one such subalgebra and it might be mapped into the field $F$ with the help of the elements of $\mathrm{Hom}(\mathcal{O}, P)$ (if this set is not empty):



$\mathcal{P} = \bigcup_{\theta \in \mathcal{F}} \theta$

$s_i \in \mathrm{Hom}(\theta_i, P)$.

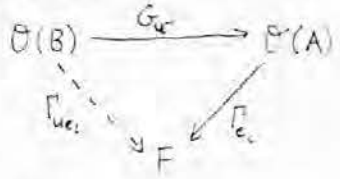
The family $\mathcal{F}$ is partially ordered by the inclusion relation: $\theta_1 \subset \theta_2$ iff there is an element $g \in \theta_1$ such that $g \in \mathcal{G}_{\theta_1}$ and $\partial(u_g^{(n)}) < \dim \theta_2$.

The finite dimensionality of the problem tells us that every chain (a well-ordered subset of $\mathcal{F}$) of $\mathcal{F}$ has a maximal element. Let $\mathcal{F}'$ be the family of maximal subalgebras in that sense; i.e., the maximal one-generator subalgebras of $(\mathcal{P}, \circ)$ . With the help of this family we will discuss now the action on $\mathcal{F}'$ induced by the $\mathrm{Aut}(\mathcal{P})$.

5. Action Induced on $\mathcal{F}'$ by the Automorphism Group Aut (P)

Given the algebra $(\mathcal{P}_{/P}, \circ)$ the set of all possible motions of an observable is given by the automorphism group. We are interested here, however, in those possible motions of the elements of the sets $\mathrm{Hom}(\theta, P)$ which are given only in terms of the already introduced concepts. Again, we can look to quantum mechanics for a hint: Let $(\mathcal{H}_{/\mathbb{R}}, \frac{1}{2}[\,,\,]_+, \frac{1}{2i}[\,,\,]_-)$-a quantum mechanical algebra be given together with its automorphism group $\mathrm{Aut}(\mathcal{H}_{/\mathbb{R}})$, and the positive definite hermitian form $\Gamma(\cdot,\cdot)$ on the space $V^n_{/\mathbb{C}}$ . Let A be a nondegenerate operator and $\{e_i\}_{i=1}^n$ be its eigenbasis. Then, as we know from the Introduction the map $\Gamma_{e_i} = \Gamma(e_i, \cdot\, e_i)$ is a homomorphism from $\mathcal{O}(A)$ onto $F$ . Let $U$ be a unitary transformation so that

$Aut(\mathcal{H}_{\mathbb{R}}) \ni G_U$ is given by $G_U(A) = U A U^+$ . The map $\Gamma_{Ue_i} := \Gamma(Ue_i \cdot Ue_i) = \Gamma(e_i, U^+ \cdot Ue_i)$ is a homomorphism of the subalgebra $\mathcal{O}(B) = \mathcal{O}(UAU^+) = G_U(\mathcal{O}(A))$ . In terms of commutative diagrams $\Gamma_{Ue_i}$ is defined by the commutativity of the diagram:




where $\Gamma_{e_i} \in Hom(\mathcal{O}(A), F)$
$\Gamma_{Ue_i} \in Hom(\mathcal{O}(B), F)$

This example shows that the motion of states understood as homomorphisms on certain domains -- subalgebras of $\mathcal{H}$ induces the movement of these very domains.

We can formulate this abstractly:

Let $\mathcal{O}_1, \mathcal{O}_2 \in \mathcal{F}$ and $G \in Aut(\mathcal{P})$ such that

$$G(\mathcal{O}_1) = \mathcal{O}_2 .$$

Let $s_2 \in Hom(\mathcal{O}_2, F)$. Then there exists a unique $s_1 \in Hom(\mathcal{O}_1, F)$ such that the following diagram commutes:


and $s_1 = s_2 \circ G$

The existence of $s_1$ is obvious. To show uniqueness let us notice that if $g \in \mathcal{G}_{\mathcal{O}_1}$ then $G(g) \in \mathcal{G}_{\mathcal{O}_2}$ because the automorphism group preserves all $\circ$-relations in the algebra $(\mathcal{P}, \circ)$ and the dimensions of its subspaces. This means that not only $\sigma(\mu_g(\lambda)) = \sigma(\mu_{G(g)}(\lambda))$, but also that $\mu_g(\lambda) = \mu_{(G(g))}(\lambda)$ . If $\ker s_2 = ((G(g) - \lambda))$ then there is

a unique ideal $((g - \lambda))$ such that $G((g - \lambda)) = ((G(g) - \lambda_0)) \in \mathcal{O}_2$ If $\mathrm{Ker}\, s_1 := ((g - \lambda_0))$ then $s_1$ is specified uniquely. We see therefore that $\mathrm{Aut}(\mathcal{P})$ generates motion in the set $\{\mathrm{Hom}(\mathcal{O}, \mathcal{P}) \mid \mathcal{O} \in \mathcal{F}'\}$ via the motion in the family $\mathcal{F}'$. Thus we can restrict our attention to the action of $\mathrm{Aut}(\mathcal{P})$ on $\mathcal{F}'$.

If $\mathcal{O} \in \mathcal{F}'$ then the subset $\{G(\mathcal{O}) \mid G \in \mathrm{Aut}(\mathcal{P})\}$ is an orbit of $\mathrm{Aut}(\mathcal{P})$ in $\mathcal{F}'$. Generally, $\mathcal{F}'$ does not constitute a single orbit; in fact the distinguishing feature of quantum algebra is transitivity of $\mathrm{Aut}(\mathcal{P})$ on $\mathcal{F}'$. All other cases we are going to investigate (except the finite dimensional algebra of hermitian operators over a real closed field) have families $\mathcal{F}'$ with the multitude of orbits.

# CHAPTER II

## 1. Proof of the Sufficient Condition for Aut$(\mathcal{H})$ to Be Transitive on the Family $\mathcal{F}$ of the Algebra $(\mathcal{H}_{/P}, \sigma, \alpha)$

**Theorem II.1**: The necessary and sufficient conditions for the group Aut $(\mathcal{H})$ to be transitive (for all $n>1$) on the set $\mathcal{F}$ which is associated with a finite dimensional algebra $(\mathcal{H}_{/P}, \sigma, \alpha, \alpha \neq 0)$ are the following:

1. $(\mathcal{H}_{/P}, \sigma, \alpha) = S_J(M^n_{/F(\theta)}, \frac{1}{2}[\ ]_+, \frac{1}{2i}[\ ]_-)$ with $J: M^n_{/F(i)} \longrightarrow M^n_{/F(i)}$ being an involution of the second kind[1] associated with a non-isotropic hermitian form.

2. $F = S_J(F(i)) = S_J(\Omega_2)$ is a real closed field[2].

Let us first consider the sufficient condition. It is the corollary to a following more general theorem.

**Theorem II.2**: Let $\mathcal{H}_{/P} = S_J(M^n_{/\Omega_2})$ be given where $P$ is real closed, $F(i) = \Omega_2$, and $J$ is an involution of the second kind, and $F = S_J(\Omega_2)$. Then Aut $(\mathcal{H}_{/P})$ has a finite number of orbits in $\mathcal{F}$, uniquely described by the sequence of integers $(k_1, \ldots, k_\ell, k_{\ell+1}, \ldots, k_s)$ which are powers of prime factors of minimal polynomials characterizing elements of a given orbit:

$$\mu(\lambda) = (\lambda - \lambda_1)^{k_1} : \ldots : (\lambda - \lambda_\ell)^{k_\ell} \cdot \pi_{\ell+1}^{k_{\ell+1}}(\lambda) : \ldots : \pi_s^{k_s}(\lambda), \quad \lambda_i \in F$$

and $\pi_i(\lambda) \in F[\lambda]$ is an irreducible polynomial of the second

---

1) See Appendix 1.

2) See Appendix 2.

degree. The integers $\{k_i\}_{i=1}^{s}$ fulfill the following conditions:

1. $\sum_{i=1}^{\ell} k_i + 2\sum_{i=\ell+1}^{s} k_i = n$

2. $0 \le k_i \le 2p+1$ if $i \le \ell$. $n-2p$ is a signature of the involution $\jmath$, with
   $0 \le k_i \le p$ if $i > \ell$ $\frac{n}{2} \ge p \ge 0$

3. Let $\{k_{i_j}\}_{\substack{i \le \ell \\ 1 \le j \le t}}$ be the set of odd integers $\ge 1$
   then $\sum_{j=1}^{t} k_{i_j} \ge n - 2p$

4. Let $(k_{i_1}, \ldots, k_{i_g}) \subset (k_1, \ldots, k_\ell)$ where $k_{i_j} = 2b+1$, $b \ge 1$
   then $\sum_{j=1}^{g} \frac{k_{i_j}-1}{2} + \left(\sum_{i=\ell+1}^{s} k_i\right) \le p$
   and $n - \left(\sum_{j=1}^{g} (k_{i_j}-1) + 2\sum_{i=\ell+1}^{s} k_i\right) = g+h$
   where $h$ is the number of linear primes with $k_i = 1$ in $\mu(\lambda)$

Corollary II.3: (The sufficient condition of the Theorem II.1) Let $\jmath$ be the nonisotropic involution of the second kind, $\mathcal{H}_{|F} = S_\jmath(M^{\circ}_{/\mathbb{R}})$, and $F$ - a real closed field be given. Then the group $Aut(\mathcal{H}_{|F})$ is transitive on the set $\mathcal{F}$.

Proof: If $\jmath$ is nonisotropic then $p=0$. Point 2 of the Theorem II.2 gives that $0 \le k_i \le 1$, $(i \le \ell)$
$k_i = 0$, $(i > \ell)$.
On the other hand, by Point 1, $\sum_{i=1}^{\ell} k_i = n$, which can be now fulfilled iff $\ell = n$ and each $k_i = 1$. So there is only one sequence of Theorem II.1, namely $(1, \ldots, 1)$. As each

sequence $(k_1, \ldots, k_s)$ characterizes an orbit uniquely (i.e., there is only one orbit for every sequence) we have proven the corollary. □

Theorem II.2 will be proven with the help of several lemmas, the main ideas of which are:

1. to show that for every sequence $(k_1, \ldots, k_s)$ there is $\mathcal{O} \in \mathcal{F}'$ the generators of which are characterized by the described type of minimal polynomial. (Due to Lemma I.4 it is enough to show that there is one $f \in \mathcal{G}_{\mathcal{O}}$ the minimal polynomial of which is characterized by $(k_1, \ldots, k_s)$ fulfilling conditions 1-4.

2. to show that all elements of $\mathcal{F}'$ are characterized this way.

3. to show that any two elements of $\mathcal{F}'$ characterized by the same sequence of integers are on the same orbit i.e. that each sequence is an invariant of elements on the orbit.

The main idea of the proof consists in establishing a relation between elements of the family $\mathcal{F}'$ and a collection of bases (in the space $V^n_{/\Omega}$) in which the form $\Gamma$ associated with a given involution $\mathcal{J}$ has a canonical representation.[3] We will show that any two subalgebras $\mathcal{O}_1, \mathcal{O}_2 \in \mathcal{F}'$ characterized by the same sequence of integers contain elements $f_i \in \mathcal{G}_{\mathcal{O}_i}$ which:

---

[3] A canonical representation of the form $\Gamma$ on the space $V^n_{/\Omega}$ is a direct sum of hyperbolic planes $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and lines $\langle \pm 1 \rangle$. T.Y. Lam, Algebraic Theory of Quadratic Forms (Reading, Mass.: W.A. Benjamin, Inc., 1973).

1. determine two different bases $\{e_j^{(1)}\}_{j=1}^{n}$, $\{e_j^{(2)}\}_{j=1}^{n}$ with exactly the same orthogonality properties,

2. have the same representation in their respective bases, so that there exists a $\Gamma$-unitary transformation $U$ which carries $\{e_j^{(1)}\}$ onto $\{e_j^{(2)}\}$. This transformation induces an automorphism of the algebra which carries $\mathfrak{A}_2$ onto $\mathfrak{A}_1$.

The method for establishing the relation between an element $f \in \mathfrak{A}$ and a canonical basis of the form $\Gamma$ is the generalization of the diagonalization procedure in the case of the positive definite form. The diagonalization consists of two conceptual components:

a. finding a set of bases in which $f$ has the representation exhibiting its minimal polynomial

b. finding in this set a unique basis in which $\Gamma$ has the canonical representation.

Our method is the application of those two components to, generally, nondiagonalizable elements of the algebra.

Let $J$ be an involution in $M_{\Omega}^{n}$ and let $C_J$ be the set $\{J' \in J_h \mid J' = G^{-1} \circ J \circ G, G \in Aut\, M_{\Omega}^{n}\}$ (a class of involutions cogredient to $J$).[4]

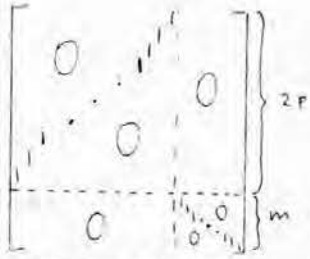
Similarly, let $C_\Gamma$ be the set $\{\Gamma' \in \mathfrak{F}_h \mid \Gamma'(x,y) = \Gamma(Gx, Gy), G \in GL(n,\Omega)$, where $\Gamma$ is a hermitian form associated with $J$. By the Witt theorem[5] the class $C_\Gamma$ contains a form $\Gamma_0$ which in a

---

[4] See Appendix 2.

[5] Nathan Jacobson, Linear Algebra (New York: D. Van Nostrand Company, Inc., 1953), Chapter V.

basis $\{e_i\}_{i=1}^{n}$ has the following representation:



(1)

where $n = 2p + m = p + m + p = q + p$ , ($n - 2p = m$ is a signature of the form)

and $\Gamma_0(e_i, e_j) = \delta_{i\,2p+1-j}$ $\quad 1 \le i, j \le 2p$

$\Gamma_0(e_i, e_j) = 0$ $\quad 1 \le i \le 2p \quad j \ge 2p+1$; $\quad n \ge i \ge 2p+1 \quad 1 \le j \le 2p$

$\Gamma_0(e_i, e_j) = \delta_{ij}$ $\quad n \ge i, j \ge 2p+1$

We can now represent the involution $J_0 \in G$ as a mapping $\left(M^n_{/\mathbb{C}\Omega}\right)_{e_i} \ni A \longrightarrow J_0(A) = \Gamma_{0|e_i}^{-1} A^+ \Gamma_{0|e_i}$ where $\left(M^n_{/\mathbb{C}\Omega}\right)_{e_i}$ is the representation of the algebra $M^n_{/\mathbb{C}\Omega}$ in the basis $\{e_i\}$ and the map $A \longrightarrow A^+$ is the hermitian conjugation in this basis. It follows[6] that $S_{J_0}\left(\left(M^n_{/\mathbb{C}\Omega}\right)_{e_i}\right) := \{A \in M^n_{/\mathbb{C}\Omega} \mid J_0(A) = A\}$ is given by the conditions:

$$(2) \qquad a_{ij} = \begin{cases} \bar{a}_{2p+1-j\;\,2p+1-i} & \text{if} \quad 1 \le i, j \le 2p+1 \\ \bar{a}_{j\,2p+1-i} & \text{if} \quad 1 \le i \le 2p \quad n \ge j \ge 2p+1 \\ a_{2p+1-j\;\,i} & \text{if} \quad n \ge i \ge 2p+1 \quad 1 \le j \le 2p \\ \bar{a}_{ji} & \text{if} \quad n \ge i, j \ge 2p+1 \end{cases}$$

---

6) See Appendix 3.

One knows that if $M^n_{/\Omega} \ni f$ then the order of its minimal polynomial $\mu_f(\lambda)$ is smaller or equal to $n$; hence, as $S_{J_\sigma}(M^n_{/\Omega}) \subset M^n_{/\Omega}$ the same applies to the elements of $S_{J_\sigma}(M^n_{/\Omega})$. Moreover, as the algebra $S_{J_\sigma}(M^n_{/\Omega})$ is an $F$-algebra, $\mu_f(\lambda)$ can have irreducible factors only of the degree 1 and 2 since only such primes exist in $F[\lambda]$. Therefore, if $\mu_f(\lambda)$ is of maximal degree then $\mu_f(\lambda) = (\lambda - \lambda_1)^{k_1} \vdots \ldots \vdots (\lambda - \lambda_\ell)^{k_\ell} \cdot \pi_{\ell+1}^{k_{\ell+1}}(\lambda) \vdots \ldots \vdots \pi_s^{k_s}(\lambda)$ with $\sum_{i=1}^{\ell} k_i + 2\sum_{i=\ell+1}^{s} k_i = n$.

Let's consider the subset $\tilde{\mathcal{F}}$ of $\mathcal{F}$ the elements of which have generators of maximal degree[7]. If $\sigma \in \tilde{\mathcal{F}}$ and $f \in \mathcal{G}_\sigma$ then we have $s$ primary idempotents $h_i(f)$ which define $s$ $\Gamma_\sigma$-orthogonal subspaces $V_i$ of $V^n_{/\Omega}$, so that $V = \bigoplus_i V_i$ and $f_{|V_i} = h_i(f) \circ f = f_i$. The minimal polynomial of $f_i \in \mathcal{O}_i(f_i)$ for $1 \le i \le \ell$ is $(\lambda - \lambda_i)^{k_i}, \lambda_i \in F$ and $\dim V_i = k_i$ so that $V_i$ is cyclic.[8] This implies the existence of a vector $X_{k_i} \in V_i$ with:

$$
\begin{aligned}
(f_i - \lambda_i) X_{k_i} &= X_{k_i - 1} \\
(f_i - \lambda_i) X_{k_i - 1} &= X_{k_i - 2} \\
&\vdots \\
(f_i - \lambda_i) X_2 &= X_1 \\
(f_i - \lambda_i) X_1 &= 0
\end{aligned}
\qquad (3)
$$

and with the set $\{X_1, X_2, \ldots, X_{k_i}\}$ being a basis in $V_i$.

---

[7] The degree of a generator is equal to the degree of its minimal polynomial.

[8] N. Jacobson, op. cit., Chapter III.

**Lemma II.4**: Let $f_i$ be as above with $k_i > 1$. Then:

1. the subspace $V_i$ has a basis $\{y_d\}_{d=1}^{k_i}$ such that

$$\Gamma_{0|V_i} = \begin{bmatrix} 0 & & & 1 \\ & \iddots & 1 & \\ & 1 & \iddots & \\ 1 & & & 0 \end{bmatrix} \quad \text{if } k_i = 2b,\ b \geq 1; \qquad \Gamma_{0|V_i} = \begin{bmatrix} 0 & & & 1 & 0 \\ & \iddots & 1 & & \\ & 1 & \iddots & & \\ 1 & & & 0 & \\ 0 & & & & 0 \end{bmatrix} \quad \text{if } k_i = 2b+1 \tag{3'}$$

2. there is an element of $\mathcal{G}_{\mathcal{O}_i}$ which in the basis $\{y_d\}_{d=1}^{k_i}$ has a representation (3)(after appropriate renumeration of the basis).

**Proof**: From (3) we obtain:

a) $\Gamma(x_1, x_1) = \Gamma(x_1, (f_i - \lambda)x_2) = \Gamma((f_i - \lambda_i)x_1, x_2) = 0$

b) $\Gamma(x_1, x_m) = \Gamma(x_1, (f_i - \lambda_i)x_{m+1}) = \Gamma((f_i - \lambda_i)x_1, x_{m+1}) = 0, \quad (m = 1, 2, \ldots, k_i - 1)$

$$\Gamma(x_2, x_m) = \Gamma(x_2, (f_i - \lambda_i)x_{m+1}) = \Gamma((f_i - \lambda_i)x_2, x_{m+1}) = \Gamma(x_1, x_{m+1}) =$$
$$= \Gamma(x_1, (f_i - \lambda_i)x_{m+2}) = \Gamma((f_i - \lambda_i)x_1, x_{m+2}) = 0 \quad (m = 1, \ldots, k_i - 2)$$
$$\vdots \qquad\qquad \vdots$$
$$\Gamma(x_{k_i-1}, x_m) = \Gamma(x_{k_i-1}, x_{m+1}) = \cdots = \Gamma(x_1, x_{m+k_i-2}) = 0 \quad (m = 1)$$

c) $\Gamma(x_{k_i}, x_1) = \Gamma(x_{k_i-1}, x_{m+1}) = \cdots = \Gamma(x_1, x_{k_i}) = \overline{\Gamma(x_{k_i}, x_1)}$

so that the elements on the antidiagonal are real and equal to $\Gamma(x_{k_i}, x_1)$.

d) $\Gamma(x_{k_i}, x_2) = \Gamma(x_{k_i}, (f_i - \lambda)x_{k_i}) = \Gamma(x_{k_i-1}, x_3) = \cdots$
$$\cdots = \Gamma(x_3, x_{k_i-1}) = \Gamma(x_2, x_{k_i}) = \overline{\Gamma(x_{k_i}, x_2)}$$
$$\vdots$$
$$\Gamma(x_{k_i}, x_{k_i-1}) = \Gamma(x_{k_i}, (f_i - \lambda_i)x_{k_i}) = \Gamma(x_{k_i-1}, x_{k_i}) = \overline{\Gamma(x_{k_i}, x_{k_i-1})}$$

which means that all other entries are real.

Hence, $\Gamma(x_a, x_b) =$

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & \Gamma_{1k_i} \\ 0 & 0 & 0 & \cdots & 0 & \Gamma_{1k_i} & \Gamma_{2k_i} \\ \vdots & & & & \Gamma_{2k_i} & \Gamma_{3k_i} & \\ & & & & \vdots & & \\ 0 & 0 & & & & & \\ 0 & \Gamma_{1k_i} & \Gamma_{2k_i} & \cdots & \Gamma_{k_i-2,k_i} & \Gamma_{k_i-1,k_i} & \\ \Gamma_{1k_i} & \Gamma_{2k_i} & \Gamma_{3k_i} & \cdots & \Gamma_{k_i-1,k_i} & \Gamma_{k_ik_i} & \end{bmatrix} \tag{4}$$

Claim: There exists a basis $\{\tilde{x}_j\}_{j=1}^{k_i}$ in $V_i$ in which $f_i$ has the representation:

$$\begin{aligned}
(f_i-\lambda_i)\,\tilde{x}_{k_i} &= \pm\,\tilde{x}_{k_i-1}\\
(f_i-\lambda_i)\,\tilde{x}_{k_i-1} &= \pm\,\tilde{x}_{k_i-2}\\
(f_i-\lambda_i)\,\tilde{x}_{k_i-2} &= \pm\,\tilde{x}_{k_i-3}\\
&\vdots \qquad\qquad \vdots\\
(f_i-\lambda_i)\,\tilde{x}_2 &= \pm\,\tilde{x}_1\\
(f_i-\lambda_i)\,\tilde{x}_1 &= 0
\end{aligned} \tag{5 $\pm$}$$

and which reduces (4) to

$$\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$$

Proof of the Claim: Let the $j$-th $(j=2,3,\ldots,k_i)$ sequence of transformations $G_j$ be given by

$$\begin{aligned}
G_j(x_1) &= G_{j-1}(x_1) \qquad (G_2(x_1) = x_1\\
G_j(x_2) &= G_{j-1}(x_2)\\
&\vdots\\
G_j(x_{j-1}) &= G_{j-1}(x_{j-1})\\
G_j(x_j) &= G_{j-1}(x_j) + \alpha\, G_{j-1}(x_1)\\
G_j(x_{j+1}) &= G_{j-1}(x_{j+1}) + \alpha\, G_{j-1}(x_2)\\
&\vdots\\
G_j(x_{k_i}) &= G_{j-1}(x_{k_i}) + \alpha\, G_{j-1}(x_{k_i-j+1})
\end{aligned}$$

where $\alpha$ is obtained by the condition $\Gamma(G_j(x_j),\, G_j(x_{k_i})) = 0 =$

$= \Gamma(G_{j-1}(x_j), G_{j-1}(x_{k_i})) + \alpha\,\Gamma(G_{j-1}(x_1), G_{j-1}(x_{k_i})) + \alpha\,\Gamma(G_{j-1}(x_{k_i-j+1}),\, G_{j-1}(x_j))$

and $G_j(x_\alpha)$ is the image of $x_\alpha$ under $G_j \circ G_{j-1} \circ \cdots \circ G_2$ transformation. One notices that $(f_i-\lambda)\,G_j(x_{j+k}) = (f_i-\lambda_i)\,G_{j-1}(x_{j+k}) +$

$+ \alpha\,(f_i-\lambda_i)\,G_{j-1}(x_{k+1}) =$

$= G_{j-1}(x_{j+k-1}) + \alpha G_{j-1}(x_k)$ so that (3) is preserved under every transformation $G_j$. Also, as $\Gamma(G_{j-1}(x_1), G_{j-1}(x_{k_i})) = \Gamma(G_{j-1}(x_{k_i-j+1}), G_{j-1}(x_j))$ we get $0 = (\alpha + \alpha)\,\Gamma(G_{j-1}(x_1), G_{j-1}(x_{k_i})) + \Gamma(G_j(x_j), G_j(x_{k_i}))$. Hence, $\alpha$ can be chosen real since $\Gamma_{ab}$'s are real.

The $j = 1$ sequence of transformations (performed as the last one) is:

$$G_1(x_a) = \frac{x_a}{\Gamma(x_1, x_{k_1})}.$$

In the above, $a = 1, \ldots, k_1$ and $\Gamma(x_1, x_{k_1}) > 0$. Hence, $\Gamma(G_1(x_a), G_1(x_{k_1-a+1})) = \dfrac{\Gamma(x_a, x_{k_1-a+1})}{\Gamma(x_1, x_{k_1})} = 1$ as a result of $\Gamma(x_a, x_{k-a+1}) = \Gamma(x_1, x_{k_1})$.

Since this transformation again preserves (3) we have proven the claim (with the "+" sign in (5)).

If $\Gamma(x_1, x_k) < 0$ then the $j = 1$ transformation is given by

$$\begin{aligned} G_1(x_{k_1}) &= \frac{x_{k_1}}{\Gamma(x_1, x_{k_1})} \\ G_1(x_{k_1-1}) &= x_{k_1-1} \\ &\vdots \\ G_1(x_1) &= x_1 \end{aligned}$$

This transformation changes (5) to

$$\begin{aligned} (f_1 - \lambda_1)\, x_{k_1} &= -x_{k_1-1} \\ (f_1 - \lambda_1)\, x_{k_1-1} &= -x_{k_1-2} \\ &\vdots \\ (f_1 - \lambda_1)\, x_1 &= 0 \end{aligned}$$

but $\Gamma(x_{k_1}, -(f_1 - \lambda_1)\, x_2) = \Gamma((f_1 - \lambda_1)\, x_{k_1}, -x_2) = \Gamma(-x_{k_1-1}, -x_2) =$

$\Gamma(x_{k_1-1}, x_2) = \cdots = \Gamma(x_1, x_{k_1})$

so that the antidiagonal elements are nonetheless equal

and as $\Gamma(G_i(x_{k_i}), G_i(x_1)) = \Gamma(-x_{k_i}, x_1) = -\Gamma(x_{k_i}, x_1) = +1$ we get the desired representation of $\Gamma$.

Suppose now that $f_{|V_i} = f_i$ has the representation (5-) in the final bases $\{x_\delta\}_{\delta=1}^{k_i}$. Then one notices that if we take the element $f_i'$ which has the representation (5+) in this basis we have $[f_i, f_i'] = 0$. As both $f_i$, $f_i'$ are cyclic transformations on $V_i$, $f_i'$ is also an element of $\mathcal{G}_{\sigma_i}$. If we now renumerate the basis vectors in the following way:

$y_1 := x_1$ $\quad$ $y_1 = x_1$

$y_2 := x_2$ $\quad$ $y_2 := x_2$

$\cdot$ $\quad$ $\cdot$

$\cdot$ if $k_i = 2t$ and $\cdot$ if $k_i = 2t+1$

$\cdot$ $\quad$ $\cdot$

$y_{k_i-1} := x_{k_i-1}$ $\quad$ $y_{k_i-1} := x_{k_i-2}$

$y_{k_i} := x_{k_i}$ $\quad$ $y_{k_i} := x_{\frac{k_i+1}{2}}$

we get the desired representation (3') of the form $\Gamma_0$.

We will show now that a similar procedure can be carried out if the minimal polynomial of $f_i$ is irreducible. Let $f_i = h_i \circ f$ be the projection of $f$ on $V_i$ with $i > l$. Its minimal polynomial on $V_i$ is $\overline{\pi}_i^{k_i}(\lambda)$ which is a power of an irreducible in $P[\lambda]$ polynomial of the second degree. By virtue of $P(i) = \angle\Omega_i$ being complete we can split $\overline{\pi}_i^{k_i}(\lambda)$ into $(\lambda - \lambda_i)^{k_i}(\lambda - \bar{\lambda}_i)^{k_i}$ in $P(i)[\lambda]$ so that $V_i = V_i' \oplus \overline{V}_i'$ where $V_i$, $V_i'$, $\overline{V}_i'$ are cyclic subspaces of V. (It is important to notice that $\Gamma(V_i', \overline{V}_i') \neq 0$; $V_i'$, $\overline{V}_i'$ are not orthogonal to each other.) This implies the existence of vectors $x_{k_i} \in V_i'$, $x_{2k_i} \in \overline{V}_i'$ such that:

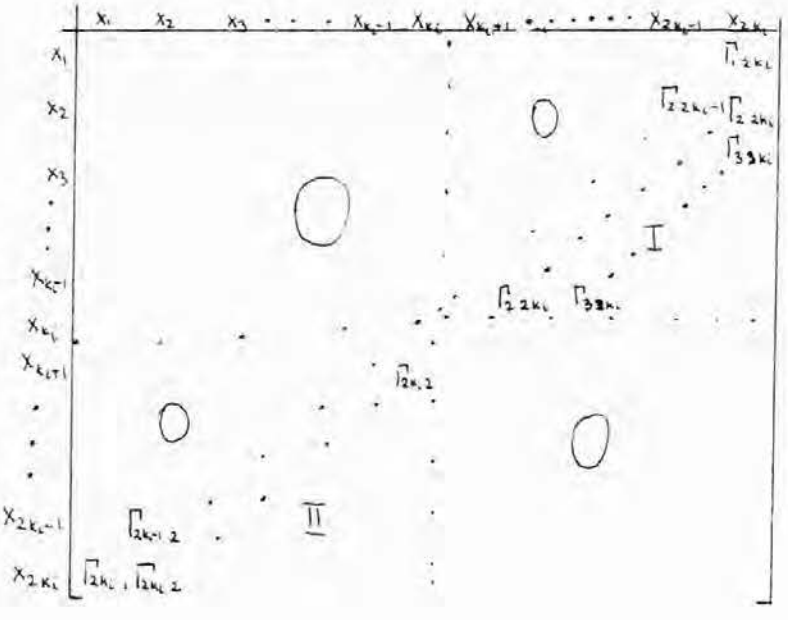
$$
(6)\qquad
\begin{aligned}
(f-\lambda)\,x_{k_i} &= x_{k_i-1} & (f-\bar\lambda)\,x_{k_i} &= (\lambda-\bar\lambda)\,x_{k_i} + x_{k_i-1}\\
(f-\lambda)\,x_{k_i-1} &= x_{k_i-2} & (f-\bar\lambda)\,x_{k_i-1} &= (\lambda-\bar\lambda)\,x_{k_i-1} + x_{k_i-2}\\
&\vdots & &\vdots\\
(f-\lambda)\,x_2 &= x_1 & (f-\bar\lambda)\,x_2 &= (\lambda-\bar\lambda)\,x_2 + x_1\\
(f-\lambda)\,x_1 &= 0 & (f-\bar\lambda)\,x_1 &= (\lambda-\bar\lambda)\,x_1\\
(f-\bar\lambda)\,x_{2k_i} &= x_{2k_i-1} & (f-\lambda)\,x_{2k_i} &= (\bar\lambda-\lambda)\,x_{2k_i} + x_{2k_i-1}\\
(f-\bar\lambda)_{2k_i-1} &= x_{2k_i-2} & (f-\lambda)\,x_{2k_i-1} &= (\bar\lambda-\lambda)\,x_{2k_i+2} + x_{2k_i-2}\\
&\vdots & &\\
(f-\bar\lambda)\,x_{k_i+2} &= x_{k_i+1} & (f-\lambda)\,x_{k_i+2} &= (\bar\lambda-\lambda)\,x_{k_i+2} + x_{k_i+1}\\
(f-\bar\lambda)\,x_{k_i+1} &= 0 & (f-\lambda)\,x_{k_i+1} &= (\bar\lambda-\lambda)\,x_{k_i+1}
\end{aligned}
$$

**Lemma II.5**: Let $f_i, V_i$ be as above. Then, there exists a basis $\{y_1, \dots, y_{2k_i}\}$ in $V_i$ such that $\Gamma(y_a, y_b)$ has the form as in the Lemma II.4 and the relations (6) are fulfilled.

**Proof**:

**Claim**: $\Gamma_{|V_i}(x_a, x_b)$ has the following representation in the basis $\{x_1, \dots, x_{2k_d}\}$:

where $\Gamma_{1\,2k_i} = \Gamma_{2\,2k_i-1} = \dots = \Gamma_{k_i\,k_i+1} = \overline{\Gamma}_{k_i+1\,k_i} = \dots = \Gamma_{2k_i\,1}$,



Proof of the Claim:

1. $\Gamma(x_1, x_1) = \Gamma(x_{k_1+1}, x_{k_1+1})$ because $\Gamma(x_1, f x_1) = \Gamma(x_1, \lambda x_1) =$

$= \Gamma(x_1, x_1)\lambda_1 = \Gamma(f_1 x_1, x_1) = \bar{\lambda}_1 \Gamma(x_1, x_1)$ $(\lambda_1 \in F(i))$

This implies $(\bar{\lambda}_1 - \lambda_1)\Gamma(x_1, x_1) = 0$ Hence $\Gamma(x_1, x_1) = 0$

and $\Gamma(x_{k_1+1}, x_{k_1+1}) = 0$

2. a) $0 = \Gamma(x_1, x_1) = \Gamma(x_1, (f_1 - \lambda_1) x_2) = \Gamma((f_1 - \bar{\lambda}_1) x_1, x_2) = (\bar{\lambda}_1 - \lambda_1)\Gamma(x_1, x_2) = \cdots$

$\cdots = (\bar{\lambda}_1 - \lambda_1)^{k_1 - 1} \Gamma(x_1, x_{k_1}) = 0$ so that $\Gamma(x_1, x_a) = 0$ ; $a = 1, \ldots, k_1$

b) $\Gamma(x_{2k_1-1}, x_1) = \Gamma(x_{2k_1-1}, (f_1 - \lambda_1) x_2) = \Gamma((f_1 - \bar{\lambda}_1) x_2) = \Gamma(x_{2k_1-2}, x_2) =$

$= \cdots = \Gamma(x_{k_1+1}, x_{k_1-1}) = \Gamma((f_1 - \bar{\lambda}_1) x_{k_1+1}, x_{k_1+1}) = 0$

$\Gamma(x_{2k_1-2}, x_1) = \Gamma(x_{2k_1-3}, x_2) = \cdots = \Gamma(x_{k_1+1}, x_{k_1-2}) =$

$= \Gamma((f - \bar{\lambda}) x_{k_1+1}, x_3) = 0$

$\vdots$

$\Gamma(x_{k_1+2}, x_1) = \Gamma((f - \bar{\lambda}) x_{k_1+2}, x_2) = \Gamma(x_{k_1+1}, x_2) =$

$= \Gamma((f - \bar{\lambda}) x_{k_1+1}, x_3) = 0$

so that $0 = \Gamma(x_a, x_b)$ for $2k_1 - 1 \leq a \leq k_1 + 1$ , $1 \leq b \leq 2k_1 - a$

and their conjugate elements.

3. $0 = \Gamma(x_2, x_1) = \Gamma((f - \bar{\lambda}) x_2, x_2) = \Gamma(x_2, x_2)(\bar{\lambda}_1 - \lambda_1) + \Gamma(x_2, x_1)$

implies that $\Gamma(x_2, x_2) = 0$.

Let $\Gamma(x_2, x_i) = 0$ for $i \leq m < k_1$

Then $0 = \Gamma(x_2, x_m) = \Gamma(x_2, x_{m+1})(\bar{\lambda}_1 - \lambda_1) + \Gamma(x_2, x_m)$

so that $\Gamma(x_2, x_{m+1}) = 0$

$\Gamma(x_2, x_{k_1})$ is the last element of this type that we can prove to be equal to zero by this method. We can similarly prove that $\Gamma(x_a, x_b)$ vanishes for $1 \leq a, b \leq k_1$

4. The repetition of the steps 2. and 3. for $\Gamma_{a\,b}$ ; $k_{i-1} \leq a, b \leq 2k_i$ with the application of the equation $0 = \Gamma(x_{k_i+1}, x_{k_i+1})$ gives us the vanishing of this part of the matrix.

5. $\Gamma(x_{2k_i}, x_1) = \Gamma((\xi-\bar{\lambda})x_{2k_i}, x_2) = \Gamma(x_{2k_i-1}, x_2) = \cdots$

$\cdots = \Gamma(x_{k_i+1}, x_{k_i}) = \overline{\Gamma}(x_{k_i}, x_{k_i+1}) = \cdots = \Gamma(x_1, x_{2k_i})$

6. $\Gamma(x_2, x_{2k_i}) = \Gamma((\xi-\lambda)x_3, x_{2k_i}) = \Gamma(x_3, (\xi-\bar{\lambda})x_{2k_i}) = \Gamma(x_3, x_{2k_i-1}) = \cdots$

$\cdots = \Gamma(x_{k_i-1}, x_{k_i+3}) = \Gamma(x_{k_i}, x_{k_i+2})$

$\Gamma(x_3, x_{2k_i}) = \cdots = \Gamma(x_{k_i}, x_{k_i+3})$

$\Gamma(x_{k_i-1}, x_{2k_i}) = \Gamma(x_{k_i}, x_{2k_i-1})$

This establishes relations in the triangle I and the conjugate triangle II. In order to prove the lemma we have to reduce those triangles to zero.

Let us introduce a similar sequence of transformations $G_j$ $(j = 2,3, \ldots, k_i)$ as in the proof of the Lemma II.4 (the elements in the triangles I and II fulfill the same relations as (4)).

$$G_j(x_1) = G_{j-1}(x_1) \qquad G_2(x_1) = x_1$$
$$G_j(x_2) = G_{j-1}(x_2)$$
$$\vdots$$
$$G_j(x_{j-1}) = G_{j-1}(x_{j-1})$$
$$G_j(x_j) = G_{j-1}(x_j) + \alpha\, G_{j-1}(x_1)$$
$$\vdots$$
$$G_j(x_{k_i}) = G_{j-1}(x_{k_i}) + \alpha\, G_{j-1}(x_{k_i-j+1})$$

$$\Gamma(G_j(x_j), x_{2k_i}) = \Gamma_{j\,2k_i} = \Gamma(G_{j-1}(x_j) + \alpha\, G_{j-1}(x_1), x_{2k_i}) =$$
$$\Gamma(G_j(x_j), x_{2k_i}) + \bar{\alpha}\,\Gamma(G_{j-1}(x_1), x_{2k_i}).$$

Hence $\Gamma(G_j(x_j), x_{2k_i}) = 0$ iff $\bar{\alpha} = \dfrac{\Gamma(G_{j-1}(x_j), x_{2k_i})}{\Gamma(G_{j-1}(x_j), x_{2k_i})}$.

Clearly, each $G_j$ preserves (6) so that all relations in the triangles I, II are preserved except those elements of which are reduced to zero by the application of $G_j$ .

The last step consists in getting $\Gamma_{12k_i} = \cdots = \Gamma_{2k_i} = 1$ on the antidiagonal.

Let $x'_{2k_i} = \frac{x_{2k_i}}{r} e^{-i\alpha}$ where $re^{i\alpha} = \Gamma(x_1, x_{2k_i})$ so that $\Gamma(x'_1, x'_{2k_i}) = 1$

$$\vdots$$

$$x'_{2k_i-1} = \frac{x_{2k_i-1}}{r} e^{-i\alpha}$$

$$\vdots$$

$$x'_{k_i+1} = \frac{x_{k_i+1}}{r} e^{-i\alpha}$$

$$x'_{k_i} = x_{k_i}$$

$$\vdots$$

$$x'_1 = x_1$$

As this transformation also preserves (6) we have proven the Lemma.

Lemma II.6: Let $f$ has a minimal polynomial which contains a linear factor in the first power. Then there exists a vector $\gamma \in V$ such that $\Gamma(\gamma, \gamma) = \pm 1$ and

(7). $f_{|\Omega\gamma} = \lambda \cdot \gamma$

Proof: If $V_i$ is the cyclic subspace of $V$ , then $V_i$ is one dimensional and any vector in it satisfies $(f_i - \lambda_i)\gamma = 0$ Let $h_i(f)$ be the projection operator on $V_i$ defined as

previously. $h_i(\ell) \in S_{\mathcal{J}}(M''_{/\Omega})$ and accordingly $\Gamma(V_i, V_d) = \Gamma(h_i V_i, h_d V_d) =$ $= \Gamma(V_i, h_i \cdot h_d V_d) = 0$ so that $V_i$ is orthogonal to all other subspaces $V_d$. Hence $\Gamma(\gamma, \gamma) \neq 0$ due to the nondegeneracy of $\Gamma$ and there is $\gamma' = \frac{\gamma}{\Gamma(\gamma,\gamma)}$ such that $\Gamma(\gamma', \gamma') = \pm 1$ □

These three Lemmas show that an element $f_i = h_i \circ f$ characterized by a power $\kappa_i > 1$ of any prime polynomial of $P[\lambda]$ can be given a representation exhibiting this power of the prime in the basis which respects the form $\Gamma$. We have to show now that the conditions 1-4 of the theorem describe all possible types of minimal polynomials.

Definition II.7: Let $\vartheta \in \mathcal{F}'$, $f \in \mathcal{J}_\vartheta$ with $\mu_f(\lambda) = (\lambda - \lambda_1)^{\kappa_1} \cdot \ldots \cdot (\lambda - \lambda_\ell)^{\kappa_\ell} \cdot \Pi_{\ell+1}^{\kappa_{\ell+1}}(\lambda) \cdot \ldots \cdot \Pi_s^{\kappa_s}(\lambda)$. The generalized characteristical basis (g.c.b.) $\{\gamma(\ell)\}$ in $V''_{/\mathbb{C}}$ is a basis obtained through the stringing together the collection of vectors $\{\gamma_i(\ell)\}_{i=1}^{s}$ determined in each subspace $V_i$ through the construction presented in the Lemmas II.4, II.5, II.6.

Corollary II.8: Conditions 1-4 of Theorem II.2 are characteristic of the elements of $\tilde{\mathcal{F}}'$.

Proof: Let $\vartheta \in \mathcal{F}'$, $f \in \mathcal{J}_\vartheta$ be given. If $\kappa_i > 1$ for every $i \leq \ell$ then the form $\Gamma_0$ has the representation

$$\begin{bmatrix} 0 & \cdots & 1 & & \\ \vdots & \iddots & 0 & 0 & \\ 1 & 0 & & & \\ \hline & 0 & & \ddots & \\ & & & & 1 \end{bmatrix} \begin{matrix} \} 2a \\ \} b \end{matrix} \qquad (8')$$

in the g.c.b. $\{\gamma(\ell)\}$.

If $\mu_f(\lambda)$ has $h$ linear factors (with $k_i = 1$) and $g$ linear factors with $k_i = 2z+1$, $z>0$ then $\Gamma_c$ has the representation

$$(\delta'') \qquad \begin{matrix} 2c \\ \\ \\ \\ n+g \end{matrix} \left\{ \begin{bmatrix} 0 & & & 0 \\ & \ddots & & \\ & & 0 & \\ 0 & & & 0 \end{bmatrix} \right. \qquad \begin{matrix} \text{if } g<m \\ m-g = \#\text{ of linear primes with} \\ \quad \text{vectors of positive length} \\ h-(m-g) = \#\text{ of linear primes with} \\ \quad \text{length} = -1 \end{matrix}$$

in the g.c.b. $\{\gamma(\delta)\}$.

Due to the theorem of inertia of the signature we get that $2a = 2p_1$ and $2c = 2p + m - h - g$ [9]. The possible numbers $c$ of hyperbolic planes $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and the possible numbers $h+g$ of lines $\langle \pm 1 \rangle$ determine the distribution of $k_i$'s in the sequence $\{k_1, \dots, k_s\}$, because the powers of primes in $\mu_f(\lambda)$ have to distribute themselves in such a way as to always give one of the representations $(\delta)$ cogredient to (1). The number $t$ of odd powers $k_{i_j}$ $(i_j \le \ell)$ has to be at least $m$ to produce at least $m$ $\langle 1 \rangle$-subspaces. It can be more, however only at the expense of hyperbolic planes $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ which always can split into $\langle \pm 1 \rangle$ subspaces. This way we get the point 1 & 3 of the Theorem II.2.

---

9) If $g<m$ then $m-g$ is the number of linear primes with characteristical vectors $\gamma$ such that $\Gamma(\gamma,\gamma) = 1$ and $h-(m-g)$ is the number of linear primes with characteristical vectors $\gamma$ such that $\Gamma(\gamma,\gamma) = -1$;
if $g>m$ then $\ell - m$ is the number of hyperbolic planes split due to the odd powers $k_i$ $(i \le \ell)$ and $h \ge \ell - m$
All characteristical vectors $\gamma$ of $h$ linear primes have $\Gamma(\gamma,\gamma) = 1$

Also all $k_i$'s $(i \leq \ell)$ fulfill the condition $0 \leq k_i \leq 2p+1$ for $(\lambda - \lambda_i)^{2p+1}$ gives $p$ hyperbolic planes and one line $\langle 1 \rangle$ and $p$ is the maximal number of hyperbolic planes of $\Gamma_0$. Similar argument applies to the case of $k_i$'s when $i > \ell$. This proves the point $2^0$ of the Theorem. One notices, of course, that a particular value of any of $k_i$'s restricts possible values of others in accordance with the point 1, 2, 3, of the Theorem. Point 4 expresses this very fact. □

Corollary II.9: For every sequence $\{k_1, \ldots, k_s\}$ satisfying conditions $1^0$-$4^0$ there is $\vartheta \in \widetilde{\mathcal{F}}$ characterized by it.

Proof: a) Let us assume that $k_i > 1$ for all $i \leq \ell$. And, let us take the canonical basis $\{e_i\}_{i=1}^n$ of $\Gamma_0$ (in which $\Gamma_0$ has the representation (1)) and subdivide it into the bases of $s$ orthogonal subspaces $V_i$ composed of the number of hyperbolic planes and lines $\langle 1 \rangle$ accordingly to the rules 1-4. In each of them, we can take $f_i$ $i = 1, \ldots, s$ defined by the relation (5), (6), (7) so that $f = \sum_{i=1}^{s} f_i$ and $\mu_f(\lambda) = \prod_i \mu_{f_i}(\lambda)$ where $\mu_{f_i}(\lambda)$ is a minimal polynomial of $f_i$. If we compare now the matrix form of $f$ in this basis with (2) we notice that $f \in S_{\mathcal{J}}(M^n_{/\mathbb{Z}})$ so that $\vartheta(f) \in \widetilde{\mathcal{F}}'$.

b) Suppose now that there are some $k_i = 1$ $(i \leq \ell)$. By the method described in the proof of the Corollary II.8 we find out the number of hyperbolic planes and $\langle \pm 1 \rangle$

lines associated with the sequence $\{k_1, \ldots, k_s\}$, subdivide the basis $\{e_i'\}$ (in which $\Gamma_c$ has a cogredient form $\Gamma_c'$ equal $(8'')$), define an appropriate $f'$ through the relations (5), (6), (7), and by inspection we find that $f' \in S_{J_0}(M''_{/\Omega})$. By the Lemma 2 in the Appendix 1 there is an element $f \in S_{J_0}(M''_{/\Omega})$ with the same minimal polynomial. □

To finish the proof of the Theorem II.2 we have to prove the uniqueness of the characterization by the sequence $\{k_1, \ldots, k_s\}$ and to show that $\tilde{\mathcal{F}}' = \mathcal{F}'$. This is the content of the next three lemmas.

Lemma II.10: Let $f_1, f_2 \in S_{J_0}(M''_{/\Omega})$, $f_i \in \mathcal{F}_{\mathcal{O}_i}$, $f_i \notin \mathcal{F}_{\mathcal{O}_j}$ $(i \neq j)$ and let the sequences $\{k_1', \ldots, k_s'\}, \{k_1'', \ldots, k_s''\}$ be identical. Then $\mathcal{O}_i$ $i = 1, 2$ lie on the same orbit of Aut $(S_J(M''_{/\Omega}))$

Proof: Let $\mu_{f_i}(\lambda)$ be the minimal polynomials of $f_i$'s By the Lemma I.4 and the fact that $F(i)$ is algebraically closed we can assume $\mu_{f_1}(\lambda) = \mu_{f_2}(\lambda)$. Let $\{\gamma_i^{(1)}\}, \{\gamma_i^{(2)}\}$ be g.c.b. obtained via the construction of the Lemmas II.4, II.5, II.6 in which $\Gamma_c$ has the representation (8). The representation of $f_i$'s in those bases might differ in the following ways:

a) if $k_i > 1$ by the "-" sign as in (5)

b) if $k_i = 1$ by the fact that the same eigenvalue might be associated with vectors of different "length": $\Gamma(\gamma_i, \gamma_i) = \pm 1$

We can however, choose (by the Lemma II.4) such $f_i' \in \mathcal{G}_{\mathcal{O}_i}$ which will have exactly the same representation in the respective bases.

Let $U$ be a linear transformation such that $U y_i^{(1)} = y_i^{(2)}$. Since $\Gamma_o(y_i^{(1)}, y_i^{(1)}) = \Gamma_o(y_i^{(2)}, y_i^{(2)})$ then $\Gamma_o(Ux, Ux) = \Gamma_o(x,x)$ for every $x \in V_{/\Omega}^n$ ; hence $G_U = U \cdot U^+$ is an element of Aut $\mathcal{G}_{J_o}(M_{/\Omega}^n)$ and $f_2' = G_U(f_1') = U f_1' U^+$ (by the uniqueness of the matrix representation of $f_i'$ in $\{y_j^{(i)}(f)\}$ ). Hence $\mathcal{O}_2 = G_U(\mathcal{O}_1)$ □

Lemma II.11: There is only one orbit of separable subalgebras $\mathcal{O} \subset \widetilde{\mathcal{F}}'$

Proof: By the Proposition I.3 $\mathcal{O}$ is separable iff the $\mu_f(\lambda) = (\lambda - \lambda_1) \dots (\lambda - \lambda_n)$ for every $f \in \mathcal{G}_{\mathcal{O}}$ . Let $\mathcal{O}(f_i)$ $i = 1,2$ be separable subalgebras and $\{ y_j^{(i)}(f) \}_{j=1}^n$ be the appropriate g.c.b.'s. Obviously, $\Gamma_o(y_j^{(i)}, y_k^{(i)}) = \begin{bmatrix} -I_p & 0 \\ 0 & I_{n-p} \end{bmatrix}$ by the nondegeneracy of the form and the inertia theorem. Again, we can choose $f_i' \in \mathcal{G}_{\mathcal{O}_i}$ such that the eigenvalue $\lambda_j^{(i)}$ has a eigenvector $y_j^{(1)}$ with $\Gamma_o(y_j', y_j') = -1$ iff $\lambda_j^{(2)} (= \lambda_j^{(1)})$ has an eigenvector $y_j^{(2)}$ with $\Gamma_o(y_j^{(2)}, y_j^{(2)}) = -1$ . If we define a transformation $U : V_{/\Omega}^n \longrightarrow V_{/\Omega}^n$ by $U(y_j^{(1)}) = y_j^{(2)}$ then $\Gamma_o(U y_k^{(1)}, U y_j^{(1)}) = \Gamma_o(y_k^{(2)}, y_j^{(2)})$,

$= \delta_{kj}$ for $j = 1, \dots, n$ $k = 1, \dots, n$; $\Gamma(Ux, Uy) = U(x,y)$

$\left( \Gamma_o(x,y) = \Gamma_o(\Sigma \alpha_m y_m^{(1)}, \Sigma \beta_k y_k^{(1)}) = -\sum_{i=1}^{p} \tilde{\alpha}_i \beta_i + \sum_{i=p+1}^{n} \tilde{\alpha}_i \beta_i \right.$ . $\Gamma_o(Ux, Uy) = \Gamma_o\left(\sum \alpha_m U y_m^{(1)}, \sum \beta_k U(y_k^{(1)})\right.$

$\left. = \Gamma_o(\Sigma \alpha_m y_m^{(2)}, \Sigma \beta_k y_k^{(2)}) = \sum_{i=1}^{p} \tilde{\alpha}_i \beta_i + \sum_{i=p+1}^{n} \tilde{\alpha}_i \beta_i \right)$ Hence, $G_U \in$ Aut $(\mathcal{G}_{J_o}(M_{/\Omega}^n))$ and $U f_1' U^+ = f_2'$ or $G_U(f_1') = f_2'$ . This implies $G_U(\mathcal{O}_1) = \mathcal{O}_2$ .

□

Lemma II.12: $\widetilde{\mathcal{F}}' = \mathcal{F}'$

Proof: To prove this lemma one has to show that if $\mathcal{O} \in \mathcal{F}$, $f \in \mathcal{G}_{\mathcal{O}}$ then there is $\mathcal{O}' \in \mathcal{F}$, $g \in \mathcal{G}_{\mathcal{O}'}$ such that $f = f(g)$, $\mathcal{O}' \supset \mathcal{O}$ and $\mathcal{O}'$ is maximal.

Let $f \in S_{J=0}(M^{n}_{/\Omega})$ and $\mu_f(\lambda) \equiv \mu_t(\lambda) = (\lambda-\lambda_1)^{k_1} \dots (\lambda-\lambda_t)^{k_t} \pi_{t+1}^{k_{t+1}}(\lambda) \dots \pi_s^{k_s}(\lambda) \equiv \tau_1^{k_1}(\lambda) \dots \tau_t^{k_t}(\lambda)$

It follows that the characteristical polynomial $\rho_f(\lambda)$ of f is equal to $\mu_1(\lambda)\,\mu_2(\lambda) \dots \mu_t(\lambda)$ with $\mu_i(\lambda)$ dividing $\mu_{i+1}(\lambda)$ [10] so that

$$\mu_i(\lambda) = \tau_{i_1}^{k_{i_1}}(\lambda) \dots \tau_{i_{s_i}}^{k_{i_{s_i}}}(\lambda)$$

where $\tau_{i_p}$ is one of the primes in $\mu_t(\lambda)$. Hence, $V = \bigoplus_{i=1}^{t} V_i$ and $V_i = \bigoplus_{k=1}^{s_i} V_{i_k}$ with $V_{i_p}$ cyclic. We can choose a basis in each of those subspaces in which $f$ has the form:

where $f_i =$

$$\begin{bmatrix} f_{i_1} & & & \\ & f_{i_2} & & 0 \\ & & \ddots & \\ & 0 & & f_{i_{s_i}} \end{bmatrix} \Big\} m = \partial(\mu_i(\lambda))$$

$$\begin{bmatrix} f_1 & & & \\ & f_2 & & 0 \\ & & \ddots & \\ & 0 & & f_t \end{bmatrix}$$

$f_{i_j} =$

$$\begin{bmatrix} \lambda_{i_j} & 1 & & \\ & \lambda_{i_j} & 1 & 0 \\ & & \ddots & \\ & 0 & & \lambda_{i_j} \end{bmatrix} \Big\} m = k_{i_j}$$

if $\partial(\tau_{i_j}) = 1$; and $f_{i_j} =$

$$\begin{bmatrix} \lambda_{i_j} & 1 & & & \\ & \lambda_{i_j} & 1 & & 0 \\ & & \lambda_{i_j} & 0 & \\ & & & \lambda_{i_j} & 1 \\ & 0 & & & \lambda_{i_j} \end{bmatrix} \Big\} 4 k_{i_j}$$

if $\partial(\tau_{i_j}) = 2$

We can define now $g \in M^{n}_{/\Omega}$ such that

---

[10] N. Jacobson, op. cit., Chapter III.

$$g = \begin{bmatrix} g_1 & & & 0 \\ & g_2 & & \\ & & \ddots & \\ 0 & & & g_{t-1} \, g_t \end{bmatrix} \qquad g_{i_j} = \begin{bmatrix} \lambda'_{i_j} & 1 & & 0 \\ & \lambda'_{i_j} & 1 & \\ & & \ddots & 1 \\ 0 & & & \lambda'_{i_j} \end{bmatrix}$$

$$g_i = \begin{bmatrix} g_{i_1} & & & 0 \\ & g_{i_2} & & \\ & & \ddots & \\ 0 & & & g_{i_{s_i}} \end{bmatrix} \qquad g_{i_j} = \begin{bmatrix} \lambda'_{i_j} & 1 & & & & \\ & \lambda'_{i_j} & 1 & & & \\ & & \ddots & \ddots & & \\ & & & \lambda'_{i_j} & & \\ & & & & \ddots & 1 \\ & & & & & \lambda'_{i_j} \end{bmatrix}$$

where $\lambda'_{a_b} \neq \lambda'_{c_d} \begin{pmatrix} a \neq c \\ b \neq d \end{pmatrix}$ and $\lambda'_{a_b}$ is not a root of $\mu_f(\lambda)$

We see that: 1. $[f, g] = 0$

2. $\mu_{g_{i_j}}(\lambda) = \begin{cases} (\lambda - \lambda'_{i_j})^{k_{i_j}} = \tau_{g_{i_j}}^{k_{i_j}}(\lambda) & \text{if } \partial(\tau_{i_j}) = 1 \\ (\lambda^2 + (\lambda'_{i_j} + \bar{\lambda}'_{i_j})\lambda + |\lambda'_{i_j}|^2)^{k_{i_j}} = \tau_{g_{i_j}}^{k_{i_j}}(\lambda) & \text{if } \partial(\tau_{i_j}) = 2 \end{cases}$

3. $\mu_g(\lambda) = \tau_{1_1}^{k_{1_1}}(\lambda) \vdots \cdots \vdots \tau_{1_{s_1}}^{k_{1_{s_1}}}(\lambda) \; \tau_{2_1}^{k_{2_1}}(\lambda) \vdots \cdots \vdots \tau_{t-1_{s_{t-1}}}^{k_{t-1_{s_{t-1}}}}(\lambda) \; \mu_t(\lambda)$

4. $g \in S_J(M^n_{/P(\lambda)})$

This point requires some elaboration: let $h_i(f)$ be the projections defined as previously. $h_i$'s are $\Gamma$-orthogonal J-symmetric operators. Let $W_i$ be the set $\{ y \in V \mid h_i(f)x = y, \; x \in V \}$ It is obvious that $W_k \perp W_\ell$ for $k \neq \ell$ and $V = \bigoplus_i W_i$. One also notices that $W_i = \bigoplus_{p=1}^{s} V_{p_i}$ i.e. it is the direct sum of those subspaces $V_{a_b}$ in which $f$ has as its minimal polynomial a factor of $\mu_f(\lambda)$. However, $V_{p_i}$'s are not $\Gamma$-orthogonal in $W_i$. Nonetheless, one can choose a basis in $V_{p_i}$ in which $\Gamma$ will have canonical form, $V_{p_i} \perp V_{p_j}$ and in which $g$ will be J-symmetric as well. The procedure for finding such a basis is similar to the one described in Lemmas II.4-II.5. Hence $g \in S_J(M^n_{/\mathbb{C}})$.

5. $f = f(g)$ because as $g$ is cyclic the only operators which commute with $g$ are $P(i)$ -functions of $g$ . If $f = \sum_{i=1}^{k} \alpha_i g^i$ with $\alpha_i \in P(i)$ then $J(f) = \sum_i \bar{\alpha}_i J(g^i) = \sum_i \bar{\alpha}_i g^i = f$ . This gives $\alpha_i \in F$. □

The Theorem II.2, apart from giving the sufficient condition of the Theorem I.1, has the interest of its own. It gives for any real closed field $F$ the full characterization of the action of $\mathrm{Aut}\left(S_J\left(M^n_{/P(i)}\right)\right)$ on the set $\mathcal{F}'$ . It's interesting to notice that for any $p>0$ there is a unique separable orbit - all other orbits have elements containing operators which can be mapped nontrivially only into zero. Whereas for $p<\frac{n}{2}$ there are no orbits of subalgebras with $\mathrm{Hom}(\mathcal{O}, P)=\emptyset$, only for $p=0$ we have the unique orbit in $\mathcal{F}'$ . It is the orbit of separable algebras.

## 2. Proof of the Necessary Condition for $\mathrm{Aut}(\mathcal{H}_{/B})$ to Be Transitive on the Family $\mathcal{F}'$ of the Algebra $(\mathcal{H}_{/B}, \sigma, \alpha)$ The Necessary and Sufficient Condition for the Algebra $(\mathcal{H}_{/B}, \sigma, \alpha)$ to Be Separable.

We turn now to the necessary condition of the Theorem II.1.

In order to prove it one has to show that unless the field $F$ is real closed and the two product algebra is given by a nonisotropic involution there always is $n>1$

such that the family $\mathcal{F}'$ associated with the algebra characterized by $n$ has more than one orbit.

Construction of the family $\mathcal{F}'$ for the algebra $(M^n_p, L, J_-, L, J_-)$

Let the family $\mathcal{F}$ of $M^n_p$ be given by the general construction described in Chapter I. Then, through the introduction of the inclusion relation, and because of the finite dimensionality of the problem we can find the family $\mathcal{F}'$ of maximal subalgebras.

Let $\tilde{\mathcal{F}}'$ be the set of subalgebras which are characterized by minimal polynomials of the degree $n$. It is clear that $\tilde{\mathcal{F}}' \subseteq \mathcal{F}$. Is it true however, that $\tilde{\mathcal{F}}' = \mathcal{F}'$? Or, in other words do all elements of $\mathcal{F}'$ have the same dimension? Obviously a positive answer to this question is a necessary (though not sufficient) condition for the transitivity of Aut $(\mathcal{H})$ on $\mathcal{F}'$.

Let $\mathcal{O} \in \tilde{\mathcal{F}}'$ with $\mu_f(\lambda) = \pi_1^{k_1}(\lambda) \cdot \ldots \cdot \pi_s^{k_s}(\lambda)$ for some $f \in \mathcal{G}_\sigma$ and $\sum \partial(\pi_i) k_i < n$ be given. If $f_i := h_i(f) \circ f$ then $V = \bigoplus_{i=1}^{s} V_i$. The minimal polynomial of $f_i \in \mathcal{O}_{(f_i)}$ is $\pi_i^{k_i}(\lambda)$. There is at least one $i \in \{1, 2, \ldots, s\}$ such that $\dim V_i > \partial(\pi_i) k_i$ otherwise we have $\partial(\mu_f(\lambda)) = n$. This implies that $V_i = V_{i_1} \oplus \cdots \oplus V_{i_\mu}$ where $f_i|_{V_{i_j}} =: f_{i_j}$. The minimal polynomial $\mu_{f_{i_j}}(\lambda)$ of $f_{i_j}$ (considered as an element of the algebra of linear transformations on $V_{i_j}$) is $\pi_i^{k_{i_j}}$ with $k_{i_j}$ dividing $k_i$. In order to prove that there exists $g \in M^n_p$ such that $f = f(g)$ and $\partial \mu_g(\lambda) = n$ it is necessary and sufficient to find

for each $i,j$ , an element $g_{ij} \in \mathfrak{V}_{ij}(f_{ij})$ with $u_{g_{ij}}(\lambda) \neq \pi_i(\lambda)^{k_{ij}}$ but with $\partial(u_{g_{ij}}) = \partial(\pi_i)k_{ij}$. If $\mathfrak{V}_{ij}(f_{ij})$ has such an element then by the Lemma I.4 we get that $u_{g_{ij}}(\lambda) = \tau_{ij}(\lambda)^{k_{ij}}$ with $\partial(u_{g_{ij}}) = \partial(\pi_i)k_{ij}$. After finding $g_{ij}$ of this type for every $j$ for which $\dim V_i > \partial(\pi_i)k_i$ we set $g := \bigoplus_j g_{ij}$ This construction gives an element $g$ with $\partial(u_g(\lambda)) = n$ if and only if $g_{ij} \neq g_{kl}$ for $i \neq k$, $j \neq l$ . Hence, the necessary and sufficient condition for $\mathfrak{F}'$ to contain only subalgebras of the same dimension is the existence of a big "reservoir" of irreducible polynomials in $F[\lambda]$. In the case of infinite fields the following procedure indicates that we can always find enough polynomials to perform the described imbedding of $\mathfrak{V}(f)$ into $\mathfrak{V}(g)$:

Let $\pi_{ij}^{k_{ij}}(\lambda) = \lambda^k + a_{k-1}\lambda^{k-1} + \dots + a_1\lambda + a_0$ and let $\lambda = A\lambda' - B$ Since the linear substitutions constitute a set of automorphism in $F[\lambda]$, $\pi_{ij}(\lambda)$ is irreducible iff $\pi'_{ij}(\lambda') \equiv \pi_{ij}(\lambda(\lambda'))$ is irreducible. If $\pi'_{ij}(\lambda') = x_k\lambda'^k + \dots + x_1\lambda' + x_0$ with $x_i$'s unknown we can find them through the solution of the equation $\pi_{ij}^{k_{ij}}(\lambda(\lambda')) = \pi'_{ij}(\lambda')$ . For our purpose, one only needs $x_k$ , and $x_{k-1}$ expressed in terms of $a_i$'s and A,B. It is easy to see that $x_k = A^k$, $x_{k-1} = a_{k-1}A^{k-1} + A^{k-1}B$ . This means that by putting $A = A_0$ and changing B to our wish we can produce any number of irreducible polynomials of the degree $k$.

In the case of finite fields the reservoir of polynomials is clearly limited; therefore a "subreservoir" of irreducible ones is also limited. This means that for

every irreducible polynomial $p(\lambda) = F[\lambda]$ there is $n>0$ such that the family $\mathcal{F}'$ of $M^n_{/P}$ contains $\mathfrak{G}$ characterized by the minimal polynomial of the degree $<n$. (It is enough to take $n = (\mathcal{V}(p)+1)\,\partial(p(\lambda))$ where $\mathcal{V}(p)$ is the finite number of irreducible polynomials of the degree equal to $\partial(p(\lambda))$. Hence if $\mu_f(\lambda)=p(\lambda)$ for some $f\in\mathfrak{G}_P$, $\mathfrak{G}$ can be imbedded only in such $\mathfrak{G}(g)$ which is characterized by $\mu_g(\lambda)$ with $\partial(\mu_g(\lambda)) = \mathcal{V}(p)\cdot\partial(p(\lambda))$.) Clearly, in this case, the structure of the family $\mathcal{F}'$ is very complicated due to different dimensionalities of its elements.

Action of Aut $(M^n_{/F})$ on $\mathcal{F}'$.

On the basis of the previous considerations one obtains: if $F$ is finite there exists $n>0$ such that for every $n'>n$ the group Aut $(M^n_{/F})$ can not be transitive on the family $\mathcal{F}'(M^n_{/P})$. However, the same observation can be made if the field $F$ is infinite for it is easy to see that any polynomial $p(\lambda)\in F[\lambda]$ can be taken as a minimal polynomial of a generator of some $\mathfrak{G}\in\mathcal{F}'$. However, any two subalgebras $\mathfrak{G}_1$, $\mathfrak{G}_2$ which have generators $f_1$, $f_2$ characterized by the same minimal polynomial $p(\lambda)$ are on one orbit of the automorphism group. In order to show this one can use the fact that any linear transformation $f$ on the space $V^n_{/F}$ with the minimal polynomial $p(\lambda)$ of the degree $n$ is cyclic, i.e. there exists a basis $\{y_j(f)\}_{j=1}^n$ such that $f$ has the following representation in it:

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & p_0 \\ 0 & 0 & 1 & & & p_1 \\ & & & \ddots & & \\ & & & & & p_{n-1} \\ 0 & 0 & & \cdots & & \end{bmatrix}$$

If $f_1$ , $f_2$ belong to different subalgebras then we have two different bases $\{\gamma_j^{(i)}\}_{j=1}^{n}$ in which $f_i$ have the same representations. If we define now a transformation $U$ by setting $U\gamma_j^{(1)} = \gamma_j^{(2)}$ , $j = 1, \dots, n$ we get $G_U(f_1) \equiv U f_1 U^{-1} = f_2$. $U$, by construction, belongs to $GL(n, F)$ and since $GI(n, F)$ is the automorphism group of $(M_F^n, [\,,\,]_+, [\,,\,]_-)$ we get $G_U(\Theta_1) = \Theta_2$ This, in particular, implies that for any sequence of integers $\{k_1, \dots, k_s\}$ such that $\sum_{i=1}^{s} k_i = n$ we have an orbit the elements of which are characterized by minimal polynomials of the type $u(\lambda) = (\lambda - \lambda_1)^{k_1} \dots (\lambda - \lambda_s)^{k_s}$ . If the field $F$ is algebraically closed then these are the only orbits present in $\mathcal{F}$ ; otherwise there are additional orbits characterized by minimal polynomials which have irreducible factors of the higher than one degree. In all cases there is a unique orbit of separable subalgebras characterized by the minimal polynomial $u(\lambda) = (\lambda - \lambda_1)^{k_1} \dots (\lambda - \lambda_s)^{k_s}$ where $s = \min\{n,$ number of elements in the field $F\}$ , and for every $n > 1$ this orbit is <u>not</u> the only orbit in $\mathcal{F}$.

<u>Orbits in the families $\mathcal{F}$ associated with two product algebras given by an involution of the second kind</u>.

Let $\Gamma : V^n_{/F(\theta)} \times V^n_{/F(\theta)} \longrightarrow F(\theta)$ be a hermitian form associated with the involution $J$ . By the Witt theorem[11] $\Gamma = \Gamma_h \oplus \Gamma_d$ , $V^n = V^{2r} \oplus V^{n-2r}$ , where $\Gamma_h$ is the hyperbolic part of

---

11) N. Jacobson, op. cit., Chapter V.

and $\Gamma_d$ is the definite part. This decomposition implies that

$$S_J(M^n_{/F(\theta)}) \supset S_{\Gamma_h}(M^{2r}_{/F(\theta)}) \oplus S_{\Gamma_d}(M^{n-2r}_{/F(\theta)})$$

where $S_{\Gamma_h}(M^{2r}_{/F(\theta)})$ is an algebra of $J_h$-hermitian elements of $M^{2r}_{/F(\theta)}$ and $S_{\Gamma_d}(M^{n-2r}_{/F(\theta)})$ is an algebra of $J_d$ hermitian elements of $M^{n-2r}_{/F(\theta)}$. ($J_h$ is the involution in $M^{2r}_{/F(\theta)}$ associated with the form $\Gamma_h$ and $J_d$ is the involution in $M^{n-2r}_{/F(\theta)}$ associated with the form $\Gamma_d$). It is important to notice that $I_{S_J} = I_{S_{\Gamma_d}} + I_{S_{\Gamma_h}}$ where $I_{S_J}$ is the unit in $S_J(M^n_{/F(\theta)})$, $I_{S_h}$ is the unit in $S_{\Gamma_h}(M^{2r}_{/F(\theta)})$ and $I_{S_{\Gamma_d}}$ is the unit in $S(M^{n-2r}_{/F(\theta)})$. It follows that if $S_J(M^n_{/F(\theta)}) \ni f = f_1 + f_2$ ; $f_1 \in S_{\Gamma_h}(M^{2r}_{/F(\theta)})$, $f_2 \in S_{\Gamma_d}(M^n_{/F(\theta)})$ then $\mu_f(\lambda) = l.c.m\{\mu_{f_1}(\lambda), \mu_{f_2}(\lambda)\}$. Clearly, there always is at least one orbit of separable subalgebras in $\mathcal{F}$. Therefore, any additional orbit will be obtained if we can find $\mathcal{A}_1 \in S_{\Gamma_h}(M^{2r}_{/F(\theta)})$ $\mathcal{A}_2 \in S_{\Gamma_d}(M^{n-2r}_{/F(\theta)})$ the dimensions of which are, respectively, $2r$ and $n-2r$, and which are not separable. Then the set $\{G(\mathcal{A}_1 \oplus \mathcal{A}_2) \mid G \in Aut(S_J(M^n_{/F(\theta)}))\}$ constitutes an additional orbit.

The considerations of Section II.1 suggest that the family $\mathcal{F}[S_{\Gamma_h}(M^{2r}_{/F(\theta)})]$ contain subalgebras characterized by minimal polynomials of the type:

$$\mu_1(\lambda) = (\lambda - \lambda_1)^{2k_1} \vdots \cdots \vdots (\lambda - \lambda_\ell)^{2k_\ell} \pi_{\ell+1}^{k_{\ell+1}}(\lambda) \vdots \cdots \vdots \pi_s^{k_s}(\lambda)$$

where $2\sum_{i=1}^{\ell} k_i + 2\sum_{i=\ell+1}^{s} k_i = 2r$, $\lambda_i \in P$ and $\pi_i(\lambda)$ is an irreducible in $P[\lambda]$ polynomial of the second degree which splits in $P(\theta)[\lambda]$ .

One also knows that there is a basis $\{e_i\}$ in $\sqrt{}^{n-2\nu}_{F(\theta)}$ in which $\Gamma_d$ has the following representation:

$$\begin{bmatrix} \omega_1 & & 0 \\ & \omega_2 & \\ & & \ddots \\ 0 & & & \omega_{n-2\nu} \end{bmatrix}$$

where $\omega_i \in \dot{F}/\dot{F}^1$ . We will show that as long as there are at least two different elements $\omega_{i_1} \neq \omega_{i_2}$ on the diagonal of this representation the family $\mathcal{F}'(S_{\Gamma_d}(M^{n-2\nu}_{/F(\theta)}))$ has nonseparable elements. The proof of this claim has two steps:

1. the pair $(\omega_{i_1}, \omega_{i_2})$ is not equal to $(a, 1)$ where $a = \varepsilon^2$ If $\omega_{i_1} = a$, $\omega_{i_2} = 1$ then there exists $f \in S_{\Gamma_d}(M^{n-2\nu}_{/F(\theta)})$ with $\mu_f(\lambda) = (\lambda^2 - a)(\lambda - \lambda_1)\ldots(\lambda - \lambda_{n-2\nu-2})$ which in the basis $\{e_i\}$ has the representation

$$\begin{bmatrix} 0 & 1 & & & \\ a & 0 & & & \\ & & \lambda_1 & & 0 \\ & & & \ddots & \\ 0 & & & & \lambda_{n-2\nu-2} \end{bmatrix}$$

But this means that there are two eigenvectors $e_1'$ $e_2'$ of $f$ such that $f e_1' = \theta e_1'$, $f e_2' = -\theta e_1'$ and $\Gamma_d(e_i', f e_i') = \pm \theta \Gamma_d(e_i', e_i') = \mp \Gamma(e_i', \theta e_i') = \mp \Gamma(e_i, e_i)\theta$. Hence $\Gamma_d(e_i', e_i') = 0$ which is impossible by the definition of $\Gamma_d$.

2. Let now a pair $(\omega_{i_1}, \omega_{i_2}) \neq (a, 1)$ be given. Then there exists $f_1 \in S_{\Gamma_d}(M^{n-2\nu}_{/F(\theta)})$ which in the basis $\{e_i\}$ (properly renumerated) has the following representation:

$$\begin{bmatrix} 0 & 1 & & & \\ \frac{\omega_{i_1}}{\omega_{i_2}} & 0 & & & \\ & & \lambda_1 & & 0 \\ & & & \ddots & \\ 0 & & & & \lambda_{n-2\nu-2} \end{bmatrix}.$$

Clearly the minimal polynomial $\mu_{f_1}(\lambda)$ of $f_1$ is equal to

$\left(\lambda^2 - \frac{\omega_j}{\omega_i}\right)(\lambda - \lambda_1) \cdots (\lambda - \lambda_{n-2r-2})$. Its degree is $n-2r$ and it has an irreducible factor of the second degree.

Let now $f \in S_J(M^n_{/F(\Theta)})$ be given such that $f = f_1 + f_2$ where $f_1 \in S_\Pi(M^{2r}_{/F(\Theta)})$ with $\mu_{f_1}(\lambda) = (\lambda - \lambda_1)^{2k_1} \cdots (\lambda - \lambda_\ell)^{2k_\ell} \Pi^{k_{\ell+1}}_{\ell+1}(\lambda) \cdots \Pi^{k_s}_s(\lambda)$ and $f_2 \in S_\Omega(M^{n-2r}_{/F(\Theta)})$ with $\mu_{f_2}(\lambda) = \left(\lambda^2 - \frac{\omega_i}{\omega_j}\right)(\lambda - \lambda'_{\ell+1}) \cdots (\lambda - \lambda_{n-2r-2})$ Then, if we choose $\lambda_i$ $i = 1, \ldots, \ell, \ell+1, \ldots, n-2r-2$ in such a way that all of them are different we get $\mu_f(\lambda) = \mu_{f_1}(\lambda) \cdot \mu_{f_2}(\lambda)$ Hence the set $\{G(f(\Theta)) \mid G \in Aut(S_J)\}$ is the additional orbit.

These remarks suggest the following formulation of the necessary conditions the fulfillment of which will exclude the described types of orbits:

(*) For every $n > 1$ there exists a sequence $\{\omega_j\}_{j=1}^n$ of elements of $P_{/P^1}$ such that for every sequence $\{x_j\}_{j=1}^n$, $x_j \in F(\Theta)$

$$\sum_{j=1}^n \omega_j \bar{x}_j x_j \neq 0$$

(if $x_j = x_j^{(1)} + \Theta x_j^{(2)}$, $x_j^{(1)}, x_j^{(2)} \in F$ then $\bar{x}_j = x_j^{(1)} - \Theta x_j^{(2)}$)

(**) For every $n > 1$ a diagonal representation of the definite form $\Gamma$ has to have the property that $\omega_i = \omega_j$ for $i \neq j$.

Both these conditions imply that for every $n > 1$ the field $F$ has to have the following property:

$$\omega\left[\sum x_j^{(1)2} - a \sum_{j=1}^n x_j^{(2)2}\right] \neq 0$$

for any two sequences $\{x_j^{(1)}\}_{j=1}^n$, $\{x_j^{(2)}\}_{j=1}^n$
In particular if $x_j^{(2)} = 0$ for all $j$, we get that

$$\omega \sum_j x_j^{(1)2} \neq 0$$

which is equivalent to the condition

$$-1 \neq \sum_{j=1}^{n-1} \left(\frac{\gamma_j^{(1)}}{\gamma_1^{(1)}}\right)^2$$

This means that in order to exclude the described types of orbits the field $P$ has to be formally real.

Now we can make use of the following theorem of Krakowski.[12)]

Krakowski Theorem

Let $K$ be a formally real field and $P$ its real closure; let $\lambda_0 \in P$ be a root of some irreducible polynomial $p_{\lambda_0}(\lambda) \in K[\lambda]$ Then there exists a $K$-symmetric matrix the minimal polynomial of which is equal to $p_{\lambda_0}(\lambda)$.

If $P$ is formally real and $F$ is not real closed then there always exists an element $\lambda_0$ of the Krakowski theorem. Let $n$ be the degree of $p_{\lambda_0}(\lambda)$. If $(\mathcal{L}_{|P}, \sigma, \alpha) = S_J(M^n_{/F(\theta)})$ with $m \geq n$ and $J$ is an involtuion associated with the form $\Gamma$ fulfilling the condition (**) then there always exists an element $f \in S_J(M^m_{/F(\theta)})$ with the minimal polynomial $\mu_f(\lambda)$ of the degree $m$ containing $p_{\lambda_0}(\lambda)$ as an irreducible factor. Hence the set $\{G(\theta(f)) \mid G \in Aut(S_J)\}$ constitutes an additional orbit.

All considerations up to now concerned the algebras of the type $S_J\left(M^n_{/F(\theta)}, \frac{1}{2}[\,,\,]_+, \frac{1}{2\theta}[\,,\,]\right)$. They are, however, also

---

12)von Fred Krakowski, "Eigenwerte und Minimal polynome symmetrischer Matrizen in kommutativen Kopern," Commentarii Mathematici Helvetici, vol. 32 fasc. 3, 1958.

valid in the case of algebras of the type

$$S_J\left(M^n_{/\Delta(F(\theta))}, \tfrac{1}{2}[\,,\,]_+, \tfrac{1}{2\theta}[\,,\,]_-\right)$$

Due to the fact that $F = S_J\left(M^n_{/\Delta(F(\theta))}\right)$ we have $S_J\left(M^n_{/\Delta(F(\theta))}\right) \supset S_{J'}\left(M^n_{/F(\theta)}\right)$ where $J'$ is an involution induced in $M^n_{/F(\theta)}$ by the involution $J$ of $M^n_{/\Delta(F(\theta))}$. Since there are no division rings over an algebraically closed field no algebra of the type $S_J\left(M^n_{/\Delta(F(\theta))}\right)$ can have a unique orbit because $F$ never can be real closed. This last remark proves the Theorem II.1.

Proposition II.13: The conditions of the Theorem II.1 are also necessary and sufficient conditions for the algebra $(\mathcal{H}_{/P}, \sigma, \alpha, a \neq 0)$ to be separable for every $n > 1$.

Proof: The Proposition I.3 asserts that $\vartheta(\ell)$ is separable iff it is characterized by the minimal polynomials of the type $\mu(\lambda) = (\lambda-\lambda_1)\cdots(\lambda-\lambda_s)$. Hence, in order to prove the necessary condition one has to show that unless $F$ is real closed and the algebra $(\mathcal{H}_{/P}, \sigma, \alpha)$ is given by an unisotropic involution, for every other type of a two product algebra there is $n > 1$ such that this algebra contains a nonseparable subalgebra or in other words, it contains a subalgebra characterized by the different type of the minimal polynomial. But the existence of additional orbits of automorphism group explicitely depends (because of Lemma I.4) on the presence of such

nonseparable elements in a given algebra. Hence, both the separability of the algebra and transitivity of the group are explicitely dependent on the same concept. Therefore the proof of the Theorem II.1 is also the proof of this proposition. □

# APPENDIX 1

## Algebraic Theory of Real Fields

The algebraic theory of real fields was developed by Artin and Schreier.[1] The main goal of their work was to establish purely algebraic foundations of real numbers and to analyze their consequences in an algebraic setting.

The theory rests on two concepts, those of ordering and formal reality.

Definition 1: A field $F$ is ordered if the property of positiveness ($>0$) is defined for its elements, and if it satisfies the following conditions:

1. For every element $a$ in $F$, just one of the relations $a = 0$, $a > 0$, $a < 0$ is valid

2. If $a > 0$ and $b > 0$ then $a + b > 0$, $ab > 0$

Definition 2: A field $F$ is formally real iff $-1$ is not expressible in it as a sum of squares.

A field $\bar{F}$ is real closed if $F$ is formally real but not extension of it formally real.

The immediate consequence of this definition is that a real closed field $F$ is not algebraically closed for the polynomial $x^2+1$ cannot have a root in $F$. One can show,

---

[1] E. Artin and O. Schreier, "Algebraische Konstruktion reeller Kopper," Abh. Math. Sam. Hamburg, vol. 5, 1926, pp. 83-115.

however, that the extension $F(i)$ where $i$ is the root of $X^2+1$, is already algebraically closed.

The interplay between the ordering idea and real closedness is contained in:

Lemma 3: Every real closed field $F$ has a unique ordering.

The proof of this lemma consists in showing that every element $0 \neq a \in F$ is a square or $-a$ is a square (but not both simultaneously). Since for any ordering squares have to be nonnegative the unique ordering is given by postulating $a>0$ iff $a$ is a square.

This lemma implies that Aut $(F)$ where $F$ is real closed equals $\{id\}$. It is important to notice that a formally real field which is not real closed might have several possible orderings. Important examples of formally real fields are rationals (with a unique ordering induced by the ordering of the ring of integers) and the extension of rationals containing the square roots of all positive elements.

To prove the existence of a real closure $P$ for a formally real field $F$ one needs to assume the countability of the field $P$. (One might also use a weaker assumption of well-ordering.) The proof is based on the fact that the algebraic closure of a countable field is countable.

If $\Omega$ is the algebraic closure of a countable formally real field $F$ then one can define a denumerable sequence

of extension fields $\Sigma_1, \Sigma_2, \ldots$ of $F$ as follows:

$$\Sigma_1 = F$$

$$\Sigma_{n+1} = \Sigma_n(\omega_n) \text{ if } \Sigma_n(\omega_n) \text{ is formally real}$$

$$\Sigma_{n+1} = \Sigma_n \text{ if } \Sigma_n(\omega_n) \text{ is not formally real}$$

$\omega_1, \omega_2, \ldots, \omega_n, \ldots$ is the set of elements of $\Omega$. If $P = \bigcup_{i=1}^{\infty} \Sigma_i$ then by induction $P$ is formally real. Since algebraic extension of $P$ cannot be formally real $P$ is real closed. Obviously $P$ is countable as a subfield of countable field $\Omega$. If $P$ is an ordered formally real field then $P$ is unique up to isomorphism. This results in the field of real algebraic numbers as the real closure of rationals.

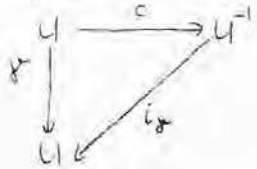
## APPENDIX 2

## Connection Between Involutions in $M^n_{\Delta}$ and Sequilinear Forms on $V^n_{\Delta}$.

1. The concept of an involution in the associative algebra $U$ over a field $F$ is a special case of a more general idea, namely that of an antiautomorphism. Any antiautomorphism of $U$ can be discussed conveniently with the help of an opposite algebra $U^{-1}$ of $U$.

An opposite algebra $U^{-1}$ of $U$ is an algebra over $F$ such that there exists a linear one-to-one, onto map $C: U \longrightarrow U^{-1}$ given by $C(\alpha A) = \alpha C(A)$, $C(A+B) = C(A)+C(B)$, $C(AB) = C(B)\cdot C(A)$. For any $U$ its opposite $U^{-1}$ is given by the canonical construction.[1)]

Any antiautomorphism $\gamma: U \longrightarrow U$ such that $\gamma(P) = P$ can be now factored through the canonical map $C: U \longrightarrow U^{-1}$ and an isomorphism $i_\gamma$




2. Let a division ring $\Delta$ over a field $F$ be given and let $\gamma: \Delta \longrightarrow \Delta$ be an antiautomorphism in $\Delta$. (Since the division ring $\Delta$ is an associative algebra over $F$, the previous discussion applies here.)

---

1) A. Albert, Structure of Algebras (Providence, R.I.: Am. Math. Society, Colloquium Publications, 1961), vol. 24.

Let $V^r_{/\Omega}$ be a right vector space over $\Omega$. With the help of the antiautomorphism $\delta$ this vector space can be considered as a left vector space $V'$ over $\Omega$ by setting $a \vee := \vee \delta(a)$ for every $a \in \Omega$, $\vee \in V$. One may check that

$$b(a\vee) = (a\vee)\delta(b) = (\vee\delta(a))\delta(b) = \vee(\delta(a)\delta(b)) = \vee\delta(ba) = (ba)\vee .$$

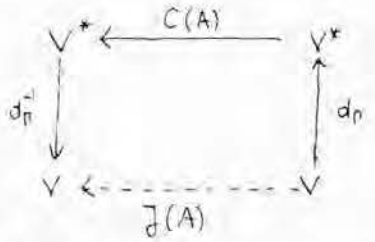
Any bilinear form $\tilde{\Gamma}: V' \times V \longrightarrow \Omega$, $\tilde{\Gamma}(a\vee_1, b\vee_2) = a\,\Gamma(\vee_1,\vee_2)\,b$ induces a sequilinear form $\Gamma$ on $V$ by allowing

$$\Gamma(\vee_1 a, \vee_2 b) := \tilde{\Gamma}(\delta^{-1}(a)\vee_1, \vee_2 b) = \delta^{-1}(a)\,\tilde{\Gamma}(\vee_1,\vee_2)\,b = \delta^{-1}(a)\,\Gamma(\vee_1,\vee_2)\,b .$$

Let then $\Gamma(\vee,\vee)$ be a sequilinear form on $V\times V$ with respect to the antiautomorphism $\delta^{-1}: \Omega \longrightarrow \Omega$, and let the map $d_\Gamma: V \longrightarrow V^*$ be given by $d_\Gamma(\vee) := \Gamma(\vee,\cdot)$. The map $d_\Gamma$ is a sequilinear map from the space $V$ into its dual $V^*$: $d_\Gamma(\vee a) = \Gamma(\vee a,\cdot) = \delta^{-1}(a)\,\Gamma(\vee,\cdot) = \delta^{-1}(a)\,d_\Gamma(\vee)$. If the form $\Gamma$ is nondegenerate (as we continue to assume in the sequel) then $d_\Gamma$ is one-to-one and onto.

3. If $U = M^n_{/\Omega}$ is an algebra of linear transformations on the vector space $V^n_{/\Omega}$ then, by remarks in point 1. of this Appendix there exists a canonical opposite algebra $U^-$ of $U$, which in this case is isomorphic to the algebra of linear transformations $M^{*n}_{/\Omega}$ on the dual space $V^*_{/\Omega}$. Let $C: M^n_{/\Omega} \longrightarrow M^{**n}_{/\Omega}$, $C(A) = A^*$ (if $f \in V^*$ then $A^* f := f \circ A$ for $A \in M^n_{/\Omega}$).

With the help of the canonical map $C$ and the map $d_\Gamma$ (which explicitly depends on the form $\Gamma$) we can construct an antiautomorphism $\mathcal{J}$ of $M^n_{/\Omega}$ by the demand of the commutativity of the following diagram:



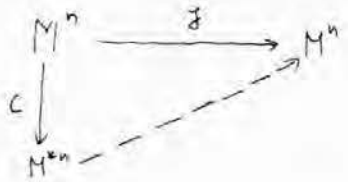

where $\mathcal{J}$ is the following map: $M^n_{/\mathfrak{A}} \ni A \longrightarrow \mathcal{J}(A) = d_\Gamma^{-1} \circ A^* \circ d_\Gamma \in M^n_{/\mathfrak{A}}$

The antiautomorphism property is induced in $\mathcal{J}$ by the antiautomorphism property of the canonical map $C(A) = A^*$ : $C(AB) = B^* A^*$.

In the case when $a$ belongs to the center of $\mathfrak{A}$ we have $\mathcal{J}(a) = \delta^2(a)$. This way we have shown that every nondegenerate sequilinear form on the space $V^n_{/\mathfrak{A}}$ induces an antiautomorphism in the algebra $M^n_{/\mathfrak{A}}$. We will show that the converse also holds.

4. Let $\mathcal{J} : M^n_{/\mathfrak{A}} \longrightarrow M^n_{/\mathfrak{A}}$ be an antiautomorphism and $C : M^n_{/\mathfrak{A}} \longrightarrow M^n_{/\mathfrak{A}}$ be a canonical antiautomorphism $C(A) = A^*$

The demand of the commutativity of the following diagram




induces an isomorphism $\Psi : M^{*n}_{/\mathfrak{A}} \longrightarrow M^n_{/\mathfrak{A}}$

where $\Psi \circ C = \mathcal{J}$

By the isomorphism theorem[2] there exists a sequilinear transformation $\epsilon : V^* \longrightarrow V$ (where $V^*$ is considered as a right vector space $V^* a := \delta(a) V$ with $\delta$ being an antiautomorphism

---

[2] N. Jacobson, Linear Algebra, Chapter IX, Section II.

of the ring $\Omega$ ) such that $\mathcal{J}(A) = \varphi \circ A^* \circ \varphi^{-1}$.

If $s : V^* \times V \longrightarrow \Omega$ is a canonical bilinear form $s(f, v) = f(v)$ then we can define a form $\Gamma(y, x) := s(\varphi^{-1}(y), x)$ on the space $V^n_\Omega$. The form is clearly sequilinear:

$$\Gamma(ya, xb) = s(\varphi^{-1}(ya), xb) = s(\varphi^{-1}(y)\delta(a), x)b = s([\gamma \circ \delta^{-1}](a)\varphi^{-1}(y), x)b =$$
$$= [\gamma \circ \delta^{-1}](a)\, s(\varphi^{-1}(y), x)\, b = \omega(a)\, \Gamma(y, x)\, b.$$

The map $\delta : \Omega \longrightarrow \Omega$ is an antiautomorphism of $\Omega$ associated with the sequilinear map $\varphi$ , and $b \longrightarrow \omega(b)$ is an antiautomorphism in $\Omega$ .

Moreover, $\Gamma(y, Ax) = s(\varphi^{-1}(y), Ax) = s(A^* \varphi^{-1}(y), x) = s(\varphi^{-1}\mathcal{J}(A)y, x) = \Gamma(\mathcal{J}(A)y, x)$

The nondegeneracy of $\Gamma$ implies the existence of a unique sequilinear map $\varphi : V \longrightarrow V$ , $\varphi(ax) = \omega^{-1}(a)\varphi(x)$ such that $\Gamma(y, x) = \omega(\Gamma(\varphi y, x))$ and $\omega^{-2}$ is a square of an inverse of the antiautomorphism $\omega : \Omega \longrightarrow \Omega$ . With the help of $\varphi$ one finds out that $\varphi A \varphi^{-1} = \mathcal{J}^2(A)$ so that $\mathcal{J}$ is an involution ($\mathcal{J}^2 = id$) iff $\varphi A \varphi^{-1} = A$ i.e. if $\varphi$ is a scalar multiplication on the left or equivalently if $\Gamma(y, x) = \varepsilon\, \omega(\Gamma(x, y))$ ($\varepsilon = \pm 1$) . We also get then $\omega^{-2}(a) = a$ which means that $\omega$ in an involution in the ring $\Omega$ .

5. The above remarks establish the existence of a correspondence between the set of nondegenerate sequilinear forms $\mathcal{G}(V^n_\Omega)$ on the space $V^n_\Omega$ and the set of involutions $\mathcal{J}(M^n_\Omega)$ in the ring of linear transformations on this space.

Lemma 1: The correspondence $\mathcal{J} \to \mathcal{G}$ induces a well defined, one-to-one, onto map $\mathcal{J} \to \mathcal{G}/\sim$, where $\sim$ is an equivalence relation given by: $\Gamma' \sim \Gamma$ iff $\Gamma' = a\,\Gamma$.

Proof: Let $\Gamma_1(y, x)$ be another hermitian form defined as in point 4 of this Appendix, $a \longrightarrow \omega'(a)$ be a second involution and $\mathcal{J}' : M^n_D \longrightarrow M^n_D$ be the involution to which both of those forms are associated. If we denote $\mathcal{J}(A)$ as $A'$ then

$$\Gamma_1(y, Ax) = \Gamma_1(A'y, x) \quad \text{iff} \quad \Gamma(y, Ax) = \Gamma(A'y, x).$$

Let $y \longrightarrow X, \Gamma(y, y)$ be the map $A = x_1 * y_1$

Then $(x_1 * y_1) = y_1 * x_1$ so that

$$\Gamma_1(u_1, [x_1 * y_1]\,v) = \Gamma_1([y_1 * x_1]\,u_1, v)$$

$$= \Gamma_1(u\, x_1 \Gamma(y_1, v)) = \Gamma_1(u, x_1)\,\Gamma(y_1, v) = \Gamma_1(y_1 \Gamma(x_1, u), v) = \omega'(\Gamma(x_1, u))\,\Gamma(y_1, v).$$

This implies that $\Gamma_1(x, y) = \Gamma(x, y)\,\delta$.

Also $\Gamma_1(x, \alpha y) = \Gamma_1(x, y)\,\omega'(\alpha) = \Gamma(x, y)\,\delta\,\omega'(\alpha) = \Gamma(x, y)\,\omega(\alpha)\,\delta$

so that $\omega'(\alpha) = \delta^{-1}\,\omega(\alpha)\,\delta = \omega(\alpha)$ because $F$ is a field.

This lemma implies that if $\Gamma_1(x,y)$ is a skew hermitian form associated with automorphism $\alpha \longrightarrow \omega(\alpha) \neq \alpha$ then $\Gamma_1(x,y)\delta$ is hermitian, so that both of them are connected with the same involution. It follows that the map $\mathcal{L}(M^n) \longrightarrow \mathcal{F}(V^n_{\Omega})/\sim$ is one-to-one and onto.

6. Congredience of forms in the set $\mathcal{G}(V^n_{\Omega})/\sim \;=\; \mathcal{F}(V^n_{\Omega})$

One knows that the set $\mathcal{F}(V^n_{\Omega})$ has another equivalence relation given by the congredience of forms: $\Gamma_1 \sim \Gamma_2$ iff there is $G \in GL(n, \Omega)$ such that $\Gamma_1(Gy, Gx) = \Gamma_2(x, y)$. Let $\mathcal{J}_2$ be an involution connected with $\Gamma_2$ and $\mathcal{J}_1$ with $\Gamma_1$. We have

then:

$$\Gamma_1(y, Ax) = \Gamma_1(J_1(A)y, x)$$
$$\Gamma_2(y, Ax) = \Gamma_2(J_2(A)y, x)$$
$$\Gamma_1(Gy, Gx) = \Gamma_2(y, x)$$

which implies that $\Gamma_2(y, Ax) = \Gamma_1(Gy, GAx) = \Gamma_1(Gy, GAG^{-1}Gx) =$

$\Gamma(y', GAG^{-1}x') = \Gamma_2(J_{\sigma_2}(A)y, x) = \Gamma_1(GJ_{\sigma_2}(A)y, x) = \Gamma_1(GJ_2(A)G^{-1}Gy, Gx) =$

$= \Gamma_1(GJ_2(A)G^{-1}y', x) = \Gamma_1(J_1(GAG^{-1})y', x')$

and $J_1(GAG^{-1}) = GJ_2(A)G^{-1}$ and $J_2^2 = \tilde{G}^{-1} \circ J_1 \circ \tilde{G}$ (where $\tilde{G}$ is an automorphism of $M^n_{/\Omega}$ induced by $G \in Gl(n, \Omega)$)

so that the cogredience relation in $\tilde{G}(V^n_{/\Omega})$ introduces in this way a cogredience relation in $\mathcal{J}(M^n_{/\Omega})$ and $\mathcal{J}(M^n_{/\Omega}) \longleftrightarrow \tilde{G}(V^n_{/\Omega})/\sim$

Let $J_1$, $J_2$ be cogredient involutions and $S_{J_1}(M^n)$, $S_{J_2}(M^n)$ be respective algebras of $J_i$-symmetric elements. Let $A \in S_{J_1}(M^n_{/\Omega})$ then $\tilde{G}^{-1}(A) \in S_{J_2}(M^n_{/\Omega})$: $J_2(\tilde{G}^{-1}(A)) = (\tilde{G}^{-1} \circ J_1 \circ \tilde{G} \circ \tilde{G}^{-1})(A) =$

This way we proved

<u>Lemma 2</u>: Let $S_{J_i}(M^n_{/\Omega})$ $i=1,2$ be two algebras defined by the cogredient hermitian forms $\Gamma_i$ $\therefore$ $\Gamma_1(Gy, Gx) = \Gamma_2(x, y)$. Then $S_{J_i}$ are isomorphic where isomorphism is given by

$$S_{J_2} \longrightarrow S_{J_1} = \tilde{G}(S_{J_2})$$
$$A \longrightarrow GAG^{-1}$$

There are three kinds of involutions possible in the algebra $M^n_{/\Omega}$:

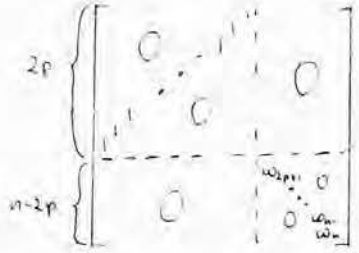
a. $J = id$ (and then $S_J(M^n_{/\Omega}) = M^n_{/\Omega}$)

b. $J \neq id$ in $M^n_{/\Omega}$ but $J_{/\Omega} = id$. It is the involution of the first kind.

c. $J \neq id$ in $M^n_{/\Omega}$ nor in $\Omega$. It is the involution of the second kind.

# APPENDIX 3

Let the sequilinear form $\Gamma$ have the following representation in the basis $\{e_i\}_{(i=1)}^{n}$ of the space $V^{n}_{/F(\Theta)}$:



$$\Gamma_{ij} = \begin{cases} \delta_{i\,2p+1-j} & \text{if } 1 \le j,i \le 2p \\ 0 & \text{if } \begin{matrix} 1 \le i \le 2p & j \ge 2p+1 \\ i \ge 2p+1 & 1 \le j \le 2p \end{matrix} \\ \omega_i \delta_{ij} & \text{if } n \ge i,j \ge 2p+1 \end{cases}$$

Let $\mathcal{J}$ be the involution in $M^{n}_{/F(\Theta)}$ associated with this form. Then if $A \in \left(M^{n}_{/F(\Theta)}\right)_{e_i}$, $\left(\mathcal{J}(A)\right)_{e_i} = \left(\Gamma^{-1} A^{+} \Gamma\right)_{e_i}$.

($\left(M^{n}_{/F(\Theta)}\right)_{e_i}$ is the representation of $M^{n}_{/\Omega}$ in the basis $\{e_i\}_{(i=1)}^{n}$, $A^{+}$ is the hermitian conjugate of $A$ with respect to a positive definite form on $V^{n}_{/F(\Theta)}$.)

We are going to find out the conditions for the matrix $(a_{ik}) \equiv A$ to be $\mathcal{J}$- symmetric i.e. to satisfy $A = \mathcal{J}(A)$.

If $(a_{ik})$ is matrix of $A$ then $(t_{ki}) = (\bar{a}_{ik})$ is the matrix of $A^{+}$ and

$$\left(\mathcal{J}(A)\right)_{e_j} = \sum_{k,l=1}^{n} \Gamma^{-1}_{lk}\, t_{ki}\, \Gamma_{ij}.$$

This results in

$$\mathcal{J}(A)_{e_j} = \begin{cases} \bar{a}_{2p+1-j\;\,2p+1-e} & \text{if } 1 \le e \le 2p \quad 1 \le j \le 2p \\ \omega_j\, \bar{a}_{j\;2p+1-e} & \text{if } 1 \le e \le 2p \quad n \ge j \ge 2p+1 \\ \frac{1}{\omega e}\, \bar{a}_{2p+1-j\;\,e} & \text{if } n \ge e \ge 2p+1 \quad 1 \le j \le 2p \\ \frac{\omega_j}{\omega e}\, \bar{a}_{je} & \text{if } n \ge e,j \ge 2p+1 \end{cases}$$

Therefore the condition $\mathcal{J}(A) = A$ is equivalent to

$$a_{ij} = \begin{cases} \bar{a}_{2p+1-j\ 2p+1-i} & \text{if } 1 \le i, j \le 2p \\ \omega_j \bar{a}_{j\ 2p+1-i} & \text{if } 1 \le i \le 2p \quad n \ge j \ge 2p+1 \\ \frac{1}{\omega_i} \bar{a}_{2p+1-j\ i} & \text{if } n \ge i \ge 2p+1, \ 1 \le j \le 2p \\ \frac{\omega_j}{\omega_i} \bar{a}_{ji} & \text{if } n \ge i, j \ge 2p+1 \end{cases}$$

## Bibliography

E. Grgin and A. Petersen. "Duality of Observables and Generators in Classical and Quantum Mechanics." J. of Math Phys., 15(6), 764-9, June 1974.

E. Grgin and A. Petersen. "Algebraic Implications of Composability of Physical Systems." (To be published in Comm. in Math Physics.)

E. Grgin and A. Petersen. Classification of Two Product Algebras. (To be published.)

E. Grgin and A. Petersen. Hamiltonian Mechanics. (Unpublished.)

N. Jacobson. Linear Algebra. New York: D. Van Nostrand Company, Inc., 1953.

T.Y. Lam. Algebraic Theory of Quadratic Forms. Reading, Mass.: W. A. Benjamin, Inc., 1972.

Von Fred Krakowski. "Eigenverte und Minimal Polynome Symmetrischer Matrizen in Kommutative Koppern." Commenteni Mathematici Helveci, vol. 32,

E. Artin and O. Schreier. "Algebraisehe Konstruction Reeler Koppern." Abh. Math Sam Hamburg, vol. 5, 1926, pp. 83-115.

A. Albert. Structure of Algebras. Providence, R.I.: Am. Math Society, Colloquium Pub. 1961, vol. 24.