National Library of Canada

Cataloguing Branch
Canadian Theses Division

Ottawa, Canada
K1A 0N4

Bibliothèque nationale du Canada

Direction du catalogage
Division des thèses canadiennes

NOTICE

The quality of this microfiche is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us a poor photocopy.

Previously copyrighted materials (journal articles, published tests, etc.) are not filmed.

Reproduction in full or in part of this film is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30. Please read the authorization forms which accompany this thesis.

THIS DISSERTATION
HAS BEEN MICROFILMED
EXACTLY AS RECEIVED

AVIS

La qualité de cette microfiche dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de mauvaise qualité.

Les documents qui font déjà l'objet d'un droit d'auteur (articles de revue, examens publiés, etc.) ne sont pas microfilmés.

La reproduction, même partielle, de ce microfilm est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30. Veuillez prendre connaissance des formules d'autorisation qui accompagnent cette thèse.

LA THÈSE A ÉTÉ
MICROFILMÉE TELLE QUE
NOUS L'AVONS REÇUE

UNIVERSITÉ D'OTTAWA
UNIVERSITY OF OTTAWA

CENTRAL POLYNOMIALS FOR JORDAN ALGEBRAS

A thesis submitted

by

Khanderao B. Patil

to

the School of Graduate Studies of

the University of Ottawa

in partial fulfillment of the requirements

for the degree of

Master of Science

in the subject of

Mathematics

November, 1975

ACKNOWLEDGEMENT

I sincerely thank Dr. M. Racine for introducing me to this field and suggesting the topic for the thesis. I wish also to acknowledge his personal warmth, unfailing guidance and valuable criticisms which made this work successful.

My thanks are due to Mrs. Zayat for her careful typing of this thesis.

CONTENTS

ABSTRACT

Recently M. Racine [6] showed that the family H_m, $m \geq 3$ of polynomials defined by Formanek [1] belongs to $FSQJ < X,Y >$, and are central for all simple quadratic Jordan algebras of degree m. They are non-vanishing for reduced quadratic Jordan algebras except for $J = H(\Phi_m, J_\nu)$, the J_ν-symmetric matrices with entries in the field Φ of char 2. In this thesis our purpose is to show the existence of family F_m, $m \geq 3$ of polynomials in $FSQJ < X, Y >$ which are non-vanishing and central for quadratic Jordan algebras $J = H(\Phi_m, J_\nu)$, Φ being a field of an arbitrary characteristic.

This thesis can be divided into two parts. The first part consists of Chapters 1, 2 and 3 in which we deal with the definitions, results and concepts used in the development of this work. In Chapter I facts concerning the linear and quadratic Jordan algebras are recalled. We have discussed in short the development of central polynomials for the quadratic Jordan algebras in Chapter 2. In Chapter 3 some results regarding the Zariski topology are given. Chapters 4 and 5 constitute the second part of the thesis. This part represents the main work of the author. In Chapter 4 we have defined the family F_m, $m \geq 3$ of polynomials in $FSQJ < X, Y >$ and proved that the polynomials are central for $J = H(\Phi_m, J_\nu)$ and are non-vanishing if $|\Phi| \geq m$. This exception is removed in Chapter 5 where it is showed that F_m, $m \geq 3$ are non-vanishing on J even when $|\Phi| < m$.

CHAPTER I

SOME DEFINITIONS AND RESULTS CONCERNING LINEAR AND QUADRATIC JORDAN ALGEBRAS

Definition. We define an *algebra* A to be a vector space over a field Φ with a binary product $(a,b) \to a \cdot b$ satisfying the following axioms.

(i) $(a_1+a_2) \cdot b = a_1 \cdot b + a_2 \cdot b$ and $a \cdot (b_1+b_2) = a \cdot b_1 + a \cdot b_2$ for all a, b, a_1, a_2, b_1 and b_2 in A.

(ii) $\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b)$, $\alpha \in \Phi$ and $a, b \in A$.

Definition. Let A be an algebra. The *nucleus* N(A) of A is the set of elements $n \in A$ such that $[n,a,b] = [a,n,b] = [a,b,n] = 0$ for all $a, b \in A$ where $[n,a,b] = (n \cdot a) \cdot b - n \cdot (a \cdot b)$. The *center* c(A) of A is the subset of N(A) of elements c such that $[c,a] = ca - ac = 0$ for all $a \in A$.

Definition. Define a *linear Jordan algebra* A to be an algebra over a field Φ of characteristic $\neq 2$ such that

(i) the product $a \cdot b$, satisfies $a \cdot b = b \cdot a$ for all a, $b \in A$.

(ii) A contains an element 1 such that $a \cdot 1 = 1 \cdot a$, $a \in A$.

(iii) $(a^2 \cdot b) \cdot a = a^2 \cdot (b \cdot a)$ where $a^2 = a \cdot a$ for all a, $b \in A$.

Note that for a linear Jordan algebra the center = the nucleus.

Definition. Let Φ be a field of arbitrary characteristic. We define *a unital quadratic Jordan algebra* over Φ to be a triple $(\mathcal{J}, U, 1)$ where $\mathcal{J}$ is a Φ-vector space, 1 a distinguished element of $\mathcal{J}$ and U is a mapping $a \to U_a$ into $\mathrm{End}_\Phi \mathcal{J}$ satisfying the following axioms.

(QJ 1) $U_1 = 1$, the identity operator.

(QJ 2) U is a Φ-quadratic, that is $U_{\lambda a} = \lambda^2 U_a$ for $\lambda \in \Phi$, $a \in \mathcal{J}$ and $U_{a,b} = U_{a+b} - U_a - U_b$, is Φ-bilinear in a and b.

(QJ 3) $U_b U_a U_b = U_{aU_b}$ for all $a, b \in \mathcal{J}$

(QJ 4) If $V_{a,b}$ is defined by $xV_{a,b} = aU_{x,b}$ then $U_b V_{a,b} = V_{b,a} U_b$ for all $a,b \in \mathcal{J}$.

(QJ 5) (QJ 1 - QJ 4) hold for $\mathcal{J}_P = \mathcal{J} \otimes_\Phi P$ for any extension field P over Φ.

If $\mathrm{char}\, \Phi \neq 2$, one can show that there is a category isomorphism between linear Jordan algebras over Φ and quadratic Jordan algebras over Φ [3]. All results concerning quadratic Jordan algebras for which no specific reference is given can be found in [4] in particular. From now on unital quadratic Jordan algebra will be abbreviated as Jordan algebra.

Let A be a unital associative algebra over Φ then $A^+ = (A, U, 1)$, where $bU_a = aba$, $a, b \in A$ is a Jordan algebra. A Jordan algebra $\mathcal{J}$ is *special* if $\mathcal{J}$ is a subalgebra of A^+ for some associative algebra A, otherwise $\mathcal{J}$ is said to be *exceptional*.

tional. Again let A be an associative algebra. We call an antiautomorphism $*$ of A an *involution* if $A^{**} = A$ for all $a \in A$. Then $H(A,*) = \{a \in A \mid a^* = a\}$ is a subalgebra of A^+. In particular consider Φ_m, the algebra of $m \times m$-matrices with entries in field Φ. Denote J_ν the involution of Φ_m given by $A^{J_\nu} = \nu A^t \nu^{-1}$ where A^t is the transpose of $A \in \Phi_m$ and $\nu = \mathrm{diag}(\nu_1, \nu_2, \ldots, \nu_m) \in \Phi_m$, $\nu_i \neq 0$. Let $Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \Phi_2$ and let $S = \begin{bmatrix} Q & & 0 \\ & \ddots & \\ 0 & & Q \end{bmatrix} \in \Phi_{2m}$ then $A^\sigma = SA^tS^{-1}$ defines an involution σ on Φ_{2m} called the *symplectic involution*. If ρ, τ are involutions of Φ_m then (Φ_m, ρ) is said to be *isomorphic* to (Φ_m, τ) if there exists an automorphism f of Φ_m such that $f(A^\rho) = (f(A))^\tau$ for every $A \in \Phi_m$. If $*$ is an involution of Φ_m which fixes $\Phi 1$, the center of Φ_m, then $(\Phi_m, *)$ is isomorphic either to (Φ_{2n}, σ) $(m = 2n)$ or (Φ_m, J_ν) for some diagonal matrix ν [3]. If $(\Phi_m, *) \simeq (\Phi_m, J_\nu)$ then $*$ is said to be of *transpose type*. In this thesis we will concern ourselves mostly with the Jordan subalgebras $H(\Phi_m, *)$ of Φ_m^+, where $*$ is transpose type.

Denote by $FSQJ\langle X_1, X_2, \ldots \rangle$ the subalgebra of $\Phi\langle X_1, X_2, \ldots \rangle^+$ generated by $1, X_1, X_2, \ldots$, where $\Phi\langle X_1, X_2, \ldots \rangle$ is the free associative algebra generated by a countable set of non-commuting variables $X_1, X_2, \ldots$. Then $FSQJ\langle X_1, X_2, \ldots \rangle$ is the free special quadratic Jordan algebra generated by $X_1, X_2, \ldots$ [4]. Consider the *reversal involution* in $\Phi\langle X_1, X_2, \ldots \rangle$ which is the linear map $a \to a^*$

of $\Phi < X_1, X_2, \ldots >$ such that $1^* = 1$ and $(X_{i_1} . X_{i_2} . \cdots X_{i_r})^* = X_{i_r} X_{i_{r-1}} \ldots . X_{i_1}$. If $H(\Phi < X_1, X_2, \ldots >, *)$ is the set of $*$-symmetric elements, $H(\Phi < X_1, X_2, \ldots >, *)$ is again a subalgebra of $\Phi < X_1, X_2, \ldots, >^+$ and it contains $1, X_1, X_2, \ldots$. Hence $H(\Phi < X_1, X_2, \ldots, >, *) \supseteq FSQJ < X_1, X_2, \ldots >$. We recall the following result.

Proposition 1.1. Let Φ be a field then

$$H(\Phi < X_1, X_2 >, *) = FSQJ < X_1, X_2 > .$$

PROOF. Clearly $H(\Phi < X_1, X_2 >, *) \supseteq FSQJ < X_1, X_2 >$. We define the length of a monomial $a \in \Phi < X_1, X_2 >$ as the numbers of factors in a, where we count X_i^n $(i = 1, 2)$ as one factor. For example $\ell(X_1^{\alpha_1}) = 1$, $\ell(X_2^{\alpha} X_1^{\beta} X_2^{\gamma} X_1^{\delta}) = 4$ where $\alpha, \beta, \gamma, \delta > 0$. Let $a \in H(\Phi < X_1, X_2 >, *)$ then a is sum of monomials P with $P^* = P$ and binomials $Q + Q^*$ where $Q^* \neq Q$. To prove $H(\Phi < X_1, X_2 >, *) \subseteq FSQJ < X_1, X_2 >$ we use induction on the length of monomials.

Let P be a monomial of length 1 then $P = X_i^{\alpha}$, $i = 1, 2$ and it can be seen very easily that $P \in FSQJ < X_1, X_2 >$. Again if P is a monomial of length 2 then $P = X_1^{\alpha_1} X_2^{\alpha_2}$ (or $X_2^{\beta_2} X_1^{\beta_1}$) and $P^* \neq P$. Consider $P + P^* = X_1^{\alpha_1} X_2^{\alpha_2} + X_2^{\alpha_2} X_1^{\alpha_1} = X_1^{\alpha_1} V_{X_2^{\alpha_2}}, 1 \in FSQJ < X_1, X_2 >$. Hence by the induction assumption for monomials of length $< n$, P or $P + P^* \in FSQJ < X_1, X_2 >$ according as $P^* = P$ or $P^* \neq P$. Now let P be

a monomial of length n. If $P^* = P$ then P must be of the type $X_i^{\alpha_1} Z X_i^{\alpha_1}$ $(i = 1, 2)$ and $Z^* = Z$ with $\ell(Z) = n - 2$ hence $Z \in FSQJ_\phi < X_1, X_2 >$. Also $P = Z \cup X_i^{\alpha_1}$ is in $FSQJ < X_1, X_2 >$. Now if $P^* \neq P$ then consider $P + P^*$.

Case 1. Let n be even. In this case $P = X_1^{\alpha_1} X_2^{\beta_1} \ldots X_1^{\alpha_{n/2}} X_2^{\beta_{n/2}}$. Let $Z = X_2^{\beta_1} \ldots X_1^{\alpha_{n/2}}$ so that $\ell(Z) = n - 2$. Then $P = X_1^{\alpha_1} Z X_2^{\beta_{n/2}} = Z \cup X_1^{\alpha_1}, X_2^{\beta_{n/2}} - X_2^{\beta_{n/2}} Z X_1^{\alpha_1}$ and $P^* = Z^* \cup X_1^{\alpha_1}, X_2^{\beta_{n/2}} - X_1^{\alpha_1} Z^* X_2^{\beta_{n/2}}$. So that $P + P^* = (Z + Z^*) \cup X_1^{\alpha_1}, X_2^{\beta_{n/2}} - r + r^*$ where $r = X_2^{\beta_{n/2}} Z X_1^{\alpha_1} = X_2^{\beta_{n/2} + \beta_1} \ldots X_1^{\alpha_{n/2} + \alpha_1}$ and $\ell(r) = n - 2$. Therefore $P + P^* \in FSQJ < X_1, X_2 >$.

Case 2. If n is odd, then $p = X_i^{\alpha_1} Z X_i^{\alpha_2}$ $(i = 1, 2)$ where $\ell(Z) = n - 2$. If $\alpha_1 = \alpha_2$ then $P = Z \cup X_i^{\alpha_1}$ and hence $P + P^* = (Z + Z^*) \cup X_i^{\alpha_1} \in FSQJ < X_1, X_2 >$. If $\alpha_1 \neq \alpha_2$ then by considering P^* if necessary we may assume $\alpha_1 > \alpha_2$, so that $P = X_i^{\alpha_2} X_i^{\alpha_1 - \alpha_2} Z X_i^{\alpha_2}$ and $P + P^* = (t + t^*) \cup X_i^{\alpha_2}$ where $t = X_i^{\alpha_1 - \alpha_2} Z$ a monomial of length $n - 1$ and therefore $P + P^* \in FSQJ < X_1, X_2 >$.

Now if $a \in H(\Phi < X_1, X_2 >, *)$ then a is the sum of monomials P with $P^* = P$ and binomials $Q + Q^*$ where $Q^* \neq Q$. But all these monomials P and binomials $Q + Q^*$ belong to $FSQJ < X_1, X_2 >$. Hence $a \in FSQJ < X_1, X_2 >$. Therefore

$H(\Phi \langle X_1, X_2 \rangle^*) \subseteq \mathrm{FSQJ} \langle X_1, X_2 \rangle$ which proves that

$$H(\Phi \langle X_1, X_2 \rangle^*) = \mathrm{FSQJ} \langle X_1, X_2 \rangle .$$

Here we recall some more definitions about Jordan algebras. Let $\mathfrak{B}$ be a Φ-vector subsapce of $\mathfrak{J}$. $\mathfrak{B}$ is an *ideal* of $\mathfrak{J}$ if for $a \in \mathfrak{J}$, $b \in \mathfrak{B}$, aU_b and bU_a belong to $\mathfrak{B}$. A Jordan algebra is said to be *simple* if it has no proper ideals. An element $e \in \mathfrak{J}$ is an *idempotent* if $e^2 = e$; two idempotents e and f are *orthogonal* if $eU_f = fU_e = 0$ and $eV_{f,1} = 0$. A non-zero idempotent e is called *absolutely primitive* if every element of $\mathfrak{J}U_e = \{aU_e \mid a \in \mathfrak{J}\}$ is of the form $\alpha e + z$ where $\alpha \in \Phi$ and z is nilpotent. If $1 = \sum_1^n e_j$ where e_j are absolutely primitive idempotents then $\mathfrak{J}$ is said to be *reduced*.

Let $\mathfrak{J}/\Phi$ be finite dimensional and $(u_1, u_2, \ldots, u_n)$ a basis for $\mathfrak{J}/\Phi$. Let P be the field extension $\Phi(\xi_1, \xi_2, \ldots, \xi_n)$ where ξ_i are algebraically independent over Φ and consider the algebra $\mathfrak{J}_P = \mathfrak{J} \otimes_\Phi P$. We shall call the element $x = \sum_1^n \xi_i u_i$ of $\mathfrak{J}_P$ a *generic element* of $\mathfrak{J}_P$. Let $m_x(\lambda)$ be the minimal polynomial of x in $\mathfrak{J}_P$ so that $m_x(\lambda) \in P[\lambda]$ and has leading coefficient 1. It can be seen ([4], p. 222) that $m_x(\lambda)$ has the form $m_x(\lambda) = \lambda^m - \sigma_1(\xi)\lambda^{m-1} + \ldots + (-1)^m \sigma_m(\xi)$ where $\sigma_j(\xi) = \sigma_j(\xi_1, \ldots, \xi_n) \in \Phi[\xi_1, \xi_2, \ldots, \xi_n]$ is homogeneous of degree j in the ξ_i's. Now let $a = \sum_1^n \alpha_i u_i \in \mathfrak{J}$. If we put $m_a(\lambda) = \lambda^m - \sigma_1(a)\lambda^{m-1} + \ldots + (-1)^m \sigma_m(a)$ where $\sigma_i(a) = \sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$ then $m_a(a) = 0$ [4]. We will call the

polynomial $m_a(\lambda) \in \Phi[\lambda]$, the *generic minimum polynomial of* a and the degree m of all $m_a(\lambda)$ in λ the generic degree of the algebra $\mathfrak{J}$.

CHAPTER II

CENTRAL POLYNOMIALS

Definition. Let Φ be a field, A an associative Φ-algebra. Denote by $\Phi < X_1, X_2, \ldots, >$ the free associative algebra generated by a countable set of non-commuting variables. A non-zero element $P(X) = P(X_1, X_2, \ldots, X_n)$ of $\Phi < X_1, X_2, \ldots >$ is said to be a *central polynomial* for A if $P(a_1, a_2, \ldots, a_n)$ belongs to the center of A for every subsitution $x_i = a_i \in A$. $P(X)$ is *non-vanishing* if it assumes a non-zero value of A for some substitution $X_i = a_i \in A$.

The first example of a central polynomial was discovered by Wagner [8]. He showed that $[X_1, X_2]^2 = (X_1X_2 - X_2X_1)^2$ is a non-vanishing central polynomial for simple associative algebras of degree 2. It was conjectured by Kaplansky [5] that such polynomials exist more generally and Formanek [1] solved the conjecture affirmatively. He showed the existence of a family H_m, $m \geq 3$ of polynomials such that for each m, H_m is non-vanishing and central for Φ_m, $m \times m$ matrices with entries in the field Φ.

In §1 we have seen that the center of linear Jordan algebra is a well defined object but the corresponding notion does not seem to have been investigated for quadratic Jordan algebras. Eventhough some difficulties arise [7] there is no question that if $\mathcal{J}$ is a unital quadratic Jordan algebra over Φ, $\Phi 1$

should be contained in any sensibly defined center. Therefore we define a polynomial to be *central* for $\mathcal{J}$ if it assumes values in $\Phi 1$ for every substitution from $\mathcal{J}$.

Professor Jacobson noted that Wagner's identity $[X_1, X_2]^2 = X_1 U_{X_2} V_{X_1} - X_1^2 U_{X_2} - X_2^2 U_{X_1} \in FSQJ < X_1, X_2, \ldots >$ and is a central polynomial for Jordan algebras of degree 2. It is non-vanishing for simple Jordan algebras except for some algebras in characteristic 2. He asked whether non-vanishing central polynomials exist for all simple Jordan algebras. Recently M. Racine [6] provided an affirmative answer to his question. He showed that the family H_m, $m \geq 3$ of polynomials defined by Formanek [1] belongs to $FSQJ < X, Y >$ and are central for all simple Jordan algebras of degree m. They are non-vanishing for reduced Jordan algebras except for $\mathcal{J} = H(\Phi_m, J_\nu)$ the J_ν-symmetric matrices with entries in a field Φ of characteristic 2. The purpose of this thesis is to give a family F_m, $m \geq 3$ of polynomials in $FSQJ < X, Y >$ which are central and non-vanishing for $\mathcal{J} = H(\Phi_m, J_\nu)$ where Φ is a field of arbitrary characteristic.

Here we recall some results of [1]. Let $\Phi[x] = \Phi[x_1, x_2, \ldots, x_{m+1}]$, $m \geq 3$ be the polynomial algebra over Φ in the commuting indeterminates $x_1, x_2, \ldots, x_{m+1}$ and let $\Phi < X, Y_1, Y_2, \ldots, Y_m >$ be the free associative algebra generated by non-commuting indeterminates $X, Y_1, \ldots, Y_m$. Let $f(x) =$

$f(x_1, x_2, \ldots, x_{m+1}) = \sum_{(n)} c_{(n)}\, x_1^{n_1} x_2^{n_2} \cdots x_{m+1}^{n_{m+1}} \in \Phi[x]$ where $(n) = (n_1, n_2, \ldots, n_{m+1})$. Define $P_f(X, Y_1, Y_2, \ldots, Y_m) = \sum_{(n)} c_{(n)}\, X^{n_1} Y_1 X^{n_2} Y_2 \cdots X^{n_m} Y_m X^{n_{m+1}}$. Let e_{ik} be the matrix units of Φ_m and $a_i \in \Phi$. We have $P_f(\sum_{i=1}^{m} a_i e_{ii}, e_{i_1 k_1}, \ldots, e_{i_m k_m}) = \sum_{(n)} c_{(n)}\, a_{i_1}^{n_1} a_{i_2}^{n_2} \cdots a_{i_m}^{n_m} a_{k_m}^{n_{m+1}} e_{i_1 k_1} \cdots e_{i_m k_m} =$

$\delta_{k_1 i_2} \delta_{k_2 i_3} \cdots \delta_{k_{m-1} i_m} e_{i_1 k_m} \sum_{(n)} c_{(n)}\, a_{i_1}^{n_1} a_{i_2}^{n_2} \cdots a_{i_m}^{n_m} a_{k_m}^{n_{m+1}}$

where $\delta_{rs} = 0$ if $r \neq s$ and $\delta_{rr} = 1$. Therefore the right hand side of the above expression is zero unless $k_j = i_{j+1}$, $1 \leq j \leq m-1$ in which case we get

① $P_f(\sum_{1}^{m} a_i e_{ii}, e_{i_1 i_2}, e_{i_2 i_3}, \ldots, e_{i_{m-1} i_m}, e_{i_m k_m}) = f(a_{i_1} a_{i_2} \cdots a_{i_m} a_{k_m}) e_{i_1 k_m}$.

We remark that since there are only m choices of the subscripts, two numbers in the sequence $(i_1, i_2, \ldots, i_m, k_m)$ are equal. Now suppose $f(x_1, x_2, \ldots, x_{m+1})$ has factors $x_i - x_j$ $i \neq j$ except $x_1 - x_{m+1}$ then right hand side of ① is zero if $i_r = i_s$ for $1 \leq r, s \leq m$ or if $i_r = k_m$, $2 \leq r \leq m$. Hence $P_f(\sum_{1}^{m} a_i e_{ii}, e_{i_1 i_2}, \ldots, e_{i_{m-1} i_m}, e_{i_m k_m}) \neq 0$ only if $k_m = i_1$. Thus we have the following result.

PROPOSITION 2.1 If $f(x_1, x_2, \ldots, x_{m+1})$ is divisible by $x_i - x_j$ $i \neq j$ except $x_1 - x_{m+1}$ and e_{ik} are matrix units of Φ_m and $a_i \in \Phi$ then

$$P_f\left(\sum_1^m a_i\, e_{ii}, e_{i_1 k_1}, \ldots, e_{i_m k_m}\right) = f(a_{i_1}, a_{i_2}, \ldots, a_{i_m}, a_{i_1}) e_{i_1 i_1}$$

if $k_j = i_{j+1}$ $1 \le j \le m - 1$ and $k_m = i_1$, otherwise

$$P_f\left(\sum_1^m a_i\, e_{ii}, e_{i_1 k_1}, \ldots, e_{i_m k_m}\right) = 0 .$$

CHAPTER III

ZARISKI TOPOLOGY

Definitions. Let Φ be an infinite field of arbitrary characteristic and V be a finite dimensional vector space over Φ. Let $\{e_1, e_2, \ldots, e_m\}$ be a basis of V over Φ. For $f(x_1, x_2, \ldots, x_m) \in \Phi[x_1, x_2, \ldots, x_m]$ we define a *polynomial function* f on V as $f(\sum_{i=1}^{m} a_i e_i) = f(a_1, a_2, \ldots, a_m)$. We say that the point $\sum_{i=1}^{m} a_i e_i \in V$ is a *zero of* f if $f(a_1, a_2, \ldots, a_m) = 0$. The set of zeros of f is called the *locus of* f. A subset W of V is called a, *hypersurface of* V if it is a locus of a non-constant polynomial function. We now topologize Φ by taking as closed sets the finite sets together with Φ and the empty set. The coarsest topology on V such that all polynomial functions on V are continuous is called the *Zariski topology*.

Here we recall some results regarding the Zariski topology.

(a) The complements of hypersurfaces of V form a basis for the open sets in the Zariski Topology.

(b) Any two non-empty open sets have non-empty intersection, that is, every non-empty open set in the Zariski Topology is dense.

Now consider the particular case $V = \mathfrak{J} = H(\Phi_m, J_\nu)$. For $A \in \mathfrak{J}$, let $\delta(A)$ be the discriminant of characteristic

polynomial of A. The mapping $\delta : \mathcal{J} \to \Phi$ sending A to $\delta(A)$ is a polynomial function. Clearly δ is non constant since $\delta(A) = 0$ for any scalar matrix A and $\delta(A) \neq 0$ for a diagonal matrix A with distinct diagonal entries. (Such a matrix exists in $\mathcal{J}$ since Φ is infinite). Therefore $\underline{V}(\delta) = \{A \in \mathcal{J} \mid \delta(A) = 0\}$ is a hypersurface of $\mathcal{J}$ and hence the complement $\mathcal{C}\underline{V}(\delta) = \{A \in \mathcal{J} \mid \delta(A) \neq 0\}$ is a non-empty open set. (In fact $\mathcal{C}\underline{V}(\delta)$ is a basic open set). Thus we have the following result.

Proposition 3.1. If Φ is an infinite field then the set $\{A \in \mathcal{J} \mid \delta(A) \neq 0\}$ is a Zariski dense set in $\mathcal{J}$.

The Zariski topology will be used in the following way. Let f be a polynomial function vanishing on a Zariski-dense set A of V. Since $f^{-1}(0)$ is a closed set containing A, $f^{-1}(0) = V$ or f vanishes on V. Thus if we wish to show that two polynomial functions are equal on V, it is sufficient to show that they are equal on a Zariski dense set on V.

CHAPTER IV

CENTRAL POLYNOMIALS FOR $\mathcal{J} = H(\Phi_m, J_\nu)$, Φ A FIELD WITH $|\Phi| \geq m$

Consider $f(x) = f(x_1, x_2, \ldots, x_{m+1}) \in \Phi[x_1, x_2, \ldots, x_{m+1}]$ defined as

$$f(x) = x_2(x_2 - x_m) \prod_{2\leq i\leq m} (x_1 - x_i)(x_{m+1} - x_i) \prod_{2<i<m} (x_i - x_m)^2 \prod_{2\leq i<j<m} (x_i - x_j)$$

Define $P_f \in \Phi < X, Y_1, Y_2, \ldots, Y_m >$ as given in §2.

Let $f_m(X, Y) = P_f(X, Y, Y, \ldots, Y)$ the element of $\Phi < X, Y >$ obtained by substituting Y for each Y_i in P_f.

LEMMA 4.1 Let A be a diagonal matrix and B be a J_ν-symmetric matrix in Φ_m then $f_m(A, B) \in \Phi 1$.

PROOF Let $A = \sum_{i=1}^{m} a_i e_{ii}$ and $B = \sum_{1\leq i, j\leq m} b_{ij} e_{ij}$ such that $b_{ji} = \nu_i^{-1} \nu_j b_{ij}$. Consider $f_m(A,B) = P_f(\sum_{i=1}^{m} a_i e_{ii}, \sum_{i,j} b_{ij} e_{ij}, \ldots, \sum_{i,j} b_{ij} e_{ij}) = \sum_{1\leq i_r, j_s\leq m} P_f(\sum_{1}^{m} a_i e_{ii}, b_{i_1 j_1} e_{i_1 j_1}, \ldots, b_{i_m j_m} e_{i_m j_m}$

$= \sum_{1\leq i_r, j_s\leq m} b_{i_1 j_1} b_{i_2 j_2} \cdots\cdots b_{i_m j_m} P_f(\sum_{1}^{m} a_i e_{ii}, e_{i_1 j_1}, \ldots, e_{i_m j_m})$.

Since $f(x_1, x_2, \ldots, x_{m+1})$ is divisible by $x_i - x_j$, $i \neq j$ except $x_1 - x_{m+1}$, by proposition 2.1,

$$f_m(A,B) = \sum_{1\leq i_r\leq m} b_{i_1 i_2} b_{i_2 i_3} \cdots\cdots b_{i_m i_1} f(a_{i_1}, a_{i_2}, \ldots, a_{i_m}, a_{i_1}) e_{i_1 j}$$

Replacing i_r by $\sigma(r)$, $\sigma \in S_m$, the group of permutations of m objects we have,

$$f_m(A,B) = \sum_{\sigma \in S_m} b_{\sigma(1)\sigma(2)}\, b_{\sigma(2)\sigma(3)} \cdots b_{\sigma(m)\sigma(1)} f(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(m)}, a_{\sigma(1)}) e_{\sigma(1)\sigma}$$

Let $b_{\sigma(1)\sigma(2)}\, b_{\sigma(2)\sigma(3)} \cdots b_{\sigma(m)\sigma(1)} = b_\sigma$ and

$$\prod_{2\le i\le m} (a_{\sigma(1)} - a_{\sigma(i)})^2 \prod_{2<i<m} (a_{\sigma(i)} - a_{\sigma(m)})^2 \prod_{2\le i<j<m} (a_{\sigma(i)} - a_{\sigma(j)})^2 = g_\sigma .$$

that is, $g_\sigma = \prod_{1\le i<j\le m} (a_i - a_j)^2$ except for the factor $(a_{\sigma(2)} - a_{\sigma(m)})^2$ and let $G_r = \{\sigma \in S_m \mid \sigma(1) = r\}$ so that $f_m(A,B)$ can be written as

$$② \qquad f_m(A,B) = \sum_{r=1}^{m} \sum_{\sigma \in G_r} a_{\sigma(2)} (a_{\sigma(2)} - a_{\sigma(m)})\, b_\sigma\, g_\sigma\, e_{\sigma(1)\sigma(1)} .$$

Now for $\sigma \in S_m$ define $\bar{\sigma} \in S_m$ as $\bar{\sigma}(i) = \sigma(m+2-i)$ for $2 \le i \le m$ and $\bar{\sigma}(1) = \sigma(1)$, so that $\bar{\sigma} \in G_{\sigma(1)}$ and $\bar{\sigma} \ne \sigma$. (Since $m \ge 3$, $\bar{\sigma}(2) = \sigma(m) \ne \sigma(2)$).

Also $b_{\bar{\sigma}} = b_{\bar{\sigma}(1)\bar{\sigma}(2)}\, b_{\bar{\sigma}(2)\bar{\sigma}(3)} \cdots b_{\bar{\sigma}(m-1)\bar{\sigma}(m)}\, b_{\bar{\sigma}(m)\bar{\sigma}(1)}$

$= b_{\sigma(1)\sigma(m)}\, b_{\sigma(m)\sigma(m-1)} \cdots b_{\sigma(3)\sigma(2)}\, b_{\sigma(2)\sigma(1)}$

$= b_{\sigma(2)\sigma(1)}\, b_{\sigma(3)\sigma(2)} \cdots b_{\sigma(1)\sigma(m)}$

$= \nu_{\sigma(1)}^{-1}\, \nu_{\sigma(2)}\, b_{\sigma(1)\sigma(2)}\, \nu_{\sigma(2)}^{-1}\, \nu_{\sigma(3)}\, b_{\sigma(2)\sigma(3)} \cdots \nu_{\sigma(m)}^{-1}\, \nu_{\sigma(1)}\, b_{\sigma(m)\sigma(1)}$

$= b_{\sigma(1)\sigma(2)}\, b_{\sigma(2)\sigma(3)} \cdots b_{\sigma(m)\sigma(1)}$

$= b_\sigma$

and $g_{\bar{\sigma}} = \prod_{1\le i<j\le m} (a_i - a_j)^2$ except for the factor $(a_{\bar{\sigma}(2)} - a_{\bar{\sigma}(m)})^2$. But $a_{\bar{\sigma}(2)} = a_{\sigma(m)}$ and $a_{\bar{\sigma}(m)} = a_{\sigma(2)}$,

hence $g_{\bar{\sigma}} = \prod_{1\le i<j\le m}(a_i - a_j)^2$ except the factor $(a_{\sigma(2)} - a_{\sigma(m)})^2$

$= g_\sigma$.

Consider $a_{\sigma(2)}(a_{\sigma(2)} - a_{\sigma(m)})\, g_\sigma\, b_\sigma\, e_{\sigma(1)\sigma(1)} +$

$a_{\bar{\sigma}(2)}(a_{\bar{\sigma}(2)} - a_{\bar{\sigma}(m)})\, g_{\bar{\sigma}}\, b_{\bar{\sigma}}\, e_{\bar{\sigma}(1)\bar{\sigma}(1)}$

$= a_{\sigma(2)}(a_{\sigma(2)} - a_{\sigma(m)})\, g_\sigma\, b_\sigma\, e_{\sigma(1)\sigma(1)} + a_{\sigma(m)}(a_{\sigma(m)} - a_{\sigma(2)})$

$g_\sigma\, b_\sigma\, e_{\sigma(1)\sigma(1)}$

$= g_\sigma\, b_\sigma\, e_{\sigma(1)\sigma(1)}(a_{\sigma(2)} - a_{\sigma(m)})^2$

$= \{g_\sigma(a_{\sigma(2)} - a_{\sigma(m)})^2\}\, b_\sigma\, e_{\sigma(1)\sigma(1)}$

$= \prod_{1\le i<j\le m}(a_i - a_j)^2\, b_\sigma\, e_{\sigma(1)\sigma(1)}$.

Again if $\sigma, \rho \in S_m$ then $\sigma \neq \rho$ implies $\bar{\sigma} \neq \bar{\rho}$ (since $\bar{\bar{\sigma}} = \sigma$) . Therefore G_r is disjoint union of pairs $\{\sigma, \bar{\sigma}\}$. Let K_r be a subset of G_r such that $G_r = K_r \cup \bar{K}_r$ and $K_r \cap \bar{K}_r = \Phi$ where $\bar{K}_r = \{\bar{\sigma} \in G_r \mid \sigma \in K_r\}$. Thus we have

③ $\sum_{\sigma \in G_r} a_{\sigma(2)}\,(a_{\sigma(2)} - a_{\sigma(m)}) g_\sigma b_\sigma e_{\sigma(1)\sigma(1)} = \prod_{1\le i<j\le m}(a_i - a_j)^2 \Big(\sum_{\sigma\in K_r} b_\sigma\Big) e_{r}$

Fix $r > 1$. If $\sigma \in G_1$, let $q = \bar{\sigma}^1(r)$, $a = b_{\sigma(1)\sigma(2)} \cdots b_{\sigma(q-1)\sigma($

and $c = b_{\sigma(q)\sigma(q+1)} \cdots b_{\sigma(m)\sigma(1)}$, then $b_\sigma = ac = ca = b_\rho$

where $\rho \in G_r$ and ρ is defined as $\rho(i) = \sigma(i + \bar{\sigma}^1(r) - 1)$.

The map $h : \sigma \to \rho$ is a bijection of G_1 onto G_r , the inverse map being given by $h' : \rho \to \sigma$ where σ is defined as $\sigma(i) = \rho(i + \bar{\sigma}^1(1) - 1)$. Moreover $h(\bar{\sigma}) = \bar{\rho}$. Indeed since

$\bar{\sigma}^{-1}(r) = m + 2 - \sigma^{-1}(r)$, we have $\bar{\sigma} \to \eta$ where $\eta(i) = \bar{\sigma}(i + m + 2 - \sigma^{-1}(r) - 1) = \sigma(m + 2 - i - m - 2 + \sigma^{-1}(r) + 1) = \sigma(1 + \sigma^{-1}(r) - i)$. While $\bar{\rho}(i) = \rho(m + 2 - i) = \sigma(m + 2 - i + \sigma^{-1}(r) - 1) = \sigma(1 + \sigma^{-1}(r) - i)$. Thus h restricted to K_1 is also a bijection. Also for $\sigma \in K_1$, if $h(\sigma) = \rho$ then $b_\sigma = b_\rho$ and hence $\sum_{\sigma \in K_r} b_\sigma = \sum_{\sigma \in K_1} b_\sigma = \tau$ say.

Therefore by (2) and (3)

④ $$f_m(A, B) = \sum_{r=1}^{m} \prod_{1 \le i < j \le m} (a_i - a_j)^2 \cdot \tau \, e_{rr}$$

$$= \alpha 1 \text{ where } \alpha = \tau \prod_{1 \le i < j \le m} (a_i - a_j)^2 .$$

Thus $f_m(A, B) \in \Phi 1$.

LEMMA 4.2 Let $A, B \in \mathcal{J} = H(\Phi_m, J_\nu)$ then $f_m(A, B) \in \Phi 1$.

PROOF Let $\hat{\Phi}$ be the algebraic closure of Φ and $\hat{\mathcal{J}} = H(\hat{\Phi}_m, J_\nu)$. Since $\mathcal{J}$ is a subalgebra of $\hat{\mathcal{J}}$ it is enough to prove that for $A, B \in \hat{\mathcal{J}}$, $f_m(A, B) \in \hat{\Phi} 1$.

Let $A, B \in \hat{\mathcal{J}}$ and $\delta(A)$ be the discriminant of the characteristic polynomial of A . Let $\delta(A) \neq 0$. Then the characteristic polynomial of A must have distinct roots and hence A is diagonalizable. If $\bar{C}^1 A C = D$, a diagonal matrix for some $C \in \hat{\Phi}_m$ then $AC = CD$ and $C^{J_\nu} A = D C^{J_\nu}$. Consider $DC^{J_\nu} C = C^{J_\nu} AC = C^{J_\nu} CD$. Thus $C^{J_\nu} C$ centralizes D . Since diagonal entries of D are distinct and C is invertible

$C^{J_\nu}C$ is a diagonal matrix whose diagonal entries are non-zero say $q_1, q_2, \ldots, q_m$. Let $Q = \mathrm{diag}(q_1^{-1/2}, q_2^{-1/2}, \ldots, q_m^{-1/2})$ then $Q^{-1} C^{-1} A C Q = D$ and $(CQ)^{J_\nu}CQ = 1$. Let $CQ = T$ then we have $T^{-1}AT = D$ and $T T^{J_\nu} = 1$ or $T^{-1} = T^{J_\nu}$.

Consider $f_m(A,B) = T[f_m(T^{-1}AT, T^{-1}BT)]T^{-1} = T[f_m(D, T^{J_\nu}BT)]T^{-1}$.

Now D is diagonal matrix and $T^{J_\nu}BT \in \hat{\mathcal{J}}$ hence by lemma 4.1 $f_m(D, T^{J_\nu}BT) \in \hat{\Phi}1$. Therefore $f_m(A,B) \in \hat{\Phi}1$. But by proposition 3.1 $\{A \in \hat{\mathcal{J}} | \delta(A) \neq 0\}$ is a Zariski dense set of $\hat{\mathcal{J}}$. Therefore $f_m(A,B) \in \hat{\Phi}1$ for all $A, B \in \hat{\mathcal{J}}$ and this proves the lemma.

LEMMA 4.3 Let Φ be a field with $|\Phi| \geq m$. If $A = \sum_{i=1}^{m} a_i e_{ii}$ with a_i's distinct elements of Φ and $B = \sum_{i=1}^{m} (\nu_i e_{i\,i+1} + \nu_{i+1} e_{i+1\,i}) \in \mathcal{J} = H(\Phi_m, J_\nu)$ then $f_m(A, B) = \nu_1 \nu_2, \ldots, \nu_m \prod_{1 \leq i < j \leq m} (a_i - a_j)^2 1$ and $f_m(A,B) \neq 0$. [Note that the subscripts are considered as integers modulo m].

PROOF Consider $G_1 = \{\rho \in S_m | \rho(1) \neq 1\}$. Let $\sigma \in G_1$ be the identity permutation. By choice of B for $\rho \in G_1$ $b_\rho = 0$ unless $\rho = \sigma$ or $\bar{\sigma}$ where $\bar{\sigma}$ is defined as $\bar{\sigma}(i) = \sigma(m + 2 - i)$ and $b_\sigma = \nu_1 \nu_2 \ldots \nu_m$. Thus $\sum_{\rho \in K_1} b_\rho = \nu_1 \nu_2 \ldots \nu_m$.

Therefore by (4) $f_m(A, B) = \nu_1 \nu_2 \ldots \prod_{1 \leq i < j \leq m} (a_i - a_j)^2 1$.

Also since $\nu_i \neq 0$ and a_i's are distinct $f_m(A, B) \neq 0$.

THEOREM 4.1 For $m \geq 3$ there exists a central polynomial

$F_m(X,Y) \in FSQJ\langle X, Y\rangle$ for the Jordan algebra $\mathcal{J} = H(\Phi_m, J_\nu)$, the J_ν-symmetric matrices with entries in a field Φ of arbitrary characteristic. Furthermore F_m is non-vanishing for $\mathcal{J}$ if $|\Phi| \geq m$.

PROOF Let * be the reversal involution of $\Phi\langle X, Y\rangle$. Define $F_m(X, Y) = f_m(X, Y)f_m^*(X, Y)$ where f_m is defined as above. Then $F_m^*(X, Y) = [f_m(X, Y)\, f_m^*(X, Y)]^* = f_m(X, Y)\, f_m^*(X, Y) = F_m(X, Y)$. Thus $F_m(X, Y) \in H(\Phi\langle X, Y\rangle, *)$ the space of * symmetric elements of $\Phi\langle X, Y\rangle$. By proposition 1.1 $H(\Phi\langle X, Y\rangle, *) = FSQJ\langle X, Y\rangle$. Hence $F_m(X, Y) \in FSQJ\langle X, Y\rangle$. Now by lemma 4.2 $f_m(A, B) \in \Phi 1$ for $A, B \in \mathcal{J}$. Let $f_m(A, B) = \alpha 1$, $\alpha \in \Phi$. Then $F_m(A, B) = f_m(A, B)\, f_m^*(A, B) = f_m(A, B)\cdot[f_m(A, B)]^{J_\nu} = (\alpha 1)\cdot(\alpha 1) = \alpha^2 1$ or $F_m(A, B) \in \Phi 1$ for $A, B \in \mathcal{J}$. Also by lemma 4.3 $f_m(A, B) \neq 0$ for $A = \sum_1^m a_i e_{ii}$, a_i distinct and $B = \sum_{i=1}^m (\nu_i e_{i\,i+1} + \nu_{i+1} e_{i+1\,i})$. Let $f_m(A, B) = \alpha 1$, $\alpha \neq 0$ then $F_m(A, B) = \alpha^2 1 \neq 0$.

Thus $F_m(X, Y) \in FSQJ\langle X, Y\rangle$ and it is central for $\mathcal{J} = H(\Phi_m, J_\nu)$. Moreover if $|\Phi| \geq m$ then F_m is non-vanishing for $\mathcal{J}$.

CHAPTER V

CENTRAL POLYNOMIALS FOR $\mathcal{J} = H(\Phi_m, J_\nu)$, $m \geq 3$

We have already proved (Theorem 4.1) that $F_m(X, Y)$ is non-vanishing on $\mathcal{J} = H(\Phi_m, J_\nu)$ if $|\Phi| \geq m$, now our aim is to show that $F_m(X, Y)$ is non-vanishing on $\mathcal{J}$ even when $|\Phi| < m$.

Proposition 5.1 Let Φ be a finite field with $|\Phi| = q$ and Γ be a field extension of degree m over Φ. If A is a matrix of the regular representation of a primitive element of Γ then there exists a $B \in \Phi_m$ such that $A^q = B^{-1} A B$. Moreover there exists a $U \in \Gamma_m$ such that $UAU^{-1} = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $(UBU^{-1})^{-1} (UAU^{-1}) (UBU^{-1}) = \text{diag}(\alpha_m, \alpha_1, \ldots, \alpha_{m-1})$.

PROOF Let θ be a primitive element of Γ over Φ i.e. $\Gamma = \Phi[\theta]$ and A be the matrix of regular representation of θ. The *unique* homomorphism $g : \Gamma = \Phi[\theta] \to \Phi[A]$ of Φ algebras such that $g(\theta) = A$ is an isomorphism and hence $\Gamma \simeq \Phi[A]$. Also the map $C \to C^q$, $C \in \Phi[A]$ is an automorphism of $\Phi[A]$ and it fixes Φ element wise hence by the Skolem-Noether Theorem [2] this automorphism of $\Phi[A]/\Phi$ extends to an automorphism of Φ_m and hence there exists a $B \in \Phi_m$ such that $A^q = B^{-1}AB$. Now θ, θ^q, θ^{q^2}, ..., $\theta^{q^{m-1}}$ are the characteristic roots of A. They are distinct and hence A can be diagonalized in Γ_m. Denote $\theta^{q^{m-1}}, \theta^{q^{m-2}}, \ldots, \theta$ by $\alpha_1, \alpha_2, \ldots, \alpha_m$ respectively. Pick a $U \in \Gamma_m$ such that $UAU^{-1} = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_m)$. Also

$(UBU^{-1})^{-1}(UAU^{-1})(UBU^{-1}) = UB^{-1}ABU^{-1} = UA^qU^{-1} = (UAU^{-1})^q =$ $\mathrm{diag}(\alpha_m, \alpha_1, \alpha_2, \ldots, \alpha_{m-1})$.

Proposition 5.2 [6, Prop 4.2] Let Φ be a finite field, Γ a field extension of degree m over Φ and J_ν is an involution of Φ_m . Then there exists a basis of Γ/Φ such that every matrix of the regular representation of Γ belongs to $H(\Phi_m, J_\nu)$.

THEOREM 5.1 $F_m(X, Y)$ is a non-vanishing central polynomial for $\mathcal{J} = H(\Phi_m, J_\nu)$ $m \geq 3$.

PROOF In view of theorem 4.1 we may assume that Φ is finite say $|\Phi| = q$. Let Γ be the field extension of degree m over Φ . By proposition 5.2 we may choose a basis of Γ/Φ such that the matrices of the regular representation are contained in $\mathcal{J}$. Let A be the matrix of regular representation of a primitive element θ of Γ . Let $h(u,v) = uvv^t$, u, v vectors in an m-dimensional $\hat{\Phi}$-vector space on which $\hat{\Phi}_m$ acts, where $\hat{\Phi}$ denotes the algebraic closure of Φ and t the transpose. Let $\{\alpha_i\}$ be the eigenvalues of A and $\{\omega_i\}$ be the set of eigenvectors of A corresponding to $\{\alpha_i\}$. For $i \neq j$ $\alpha_i\, \omega_i\, \nu\omega_j^t = h(\omega_i A, \omega_j^t) = \omega_i\, A\, \nu\omega_j^t = \omega_i\, \nu A^t\, \omega_j^t$ (since $A \in \mathcal{J}$) $= h(\omega_i, \omega_j A) = \alpha_j\, \omega_i\, \omega_j^t$ implies $\omega_i\, \nu\, \omega_j^t = 0$ (since $\alpha_i \neq \alpha_j$) . As h is non-degenerate and $h(\omega_i, \omega_j) = 0$, $i \neq j$ we get $h(\omega_i, \omega_i) \neq 0$. Since $\hat{\Phi}$ is algebraically closed, multiplying ω_i by $\nu_i^{1/2}\, h(\omega_i, \omega_i)^{-1/2}$ we may assume $h(\omega_i, \omega_i) = \nu_i$. Let $T \in \hat{\Phi}_m$ be the matrix with ω_i's as rows then $TT^{J_\nu} = 1$ and $TAT^{-1} =$

$TAT^{J_\nu} = \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_m)$. By proposition 5.1 there exists $B \in \Phi_m$ such that $B^{-1}AB = A^q$ and $(TBT^{-1})^{-1}(TAT^{-1})(TBT^{-1}) = \mathrm{diag}(\alpha_m, \alpha_1, \ldots, \alpha_{m-1})$. Thus action of the above inner automorphism permutes the roots cyclically and hence TBT^{-1} must equal the permutation matrix $\sum_{i=1}^{m} e_{i\,i+1}$ times a matrix which centralizes TAT^{-1} (recall that the indices are to be read modulo m) that is, times a diagonal matrix (the α_i's are distinct). Therefore $TBT^{-1} = \sum_{i=1}^{m} \beta_i e_{ii+1}$ and $\beta_i \neq 0$ for $1 \leq i \leq m$. Now consider , $(TBT^{-1})^{J_\nu} = (TBT^{J_\nu})^{J_\nu} = TB^{J_\nu}T^{J_\nu} = TB^{J_\nu}T^{-1}$. Thus $TB^{J_\nu}T^{-1} = (TBT^{-1})^{J_\nu} = \nu(TBT^{-1})^{t}\nu^{-1} = \nu(\sum_{i=1}^{m} \beta_i e_{i+1\,i})\nu^{-1} = \sum_{i=1}^{m} \beta_i \nu_{i+1}\nu_i^{-1} e_{i+1\,i}$ and hence

$$T(B + B^{J_\nu})T^{-1} = \sum_{i=1}^{m} \beta_i \nu_i^{-1}(\nu_i e_{i\,i+1} + \nu_{i+1} e_{i+1\,i}) \quad .$$

Therefore as in lemma 4.3

$$f_m(TAT^{-1}, T(B + B^{J_\nu})T^{-1} = \beta_1\beta_2 \cdots \beta_m \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j)^2 \cdot 1 \, .$$

Now $f_m(A, B + B^{J_\nu}) = T^{-1}(f_m(TAT^{-1}, T(B + B^{J_\nu})T^{-1})\,T =$

$$\beta_1 \beta_2 \cdots \beta_m \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j)^2 \, 1 \neq 0$$

(since $\beta_i \neq 0$ and α_i are distinct). Thus there exist $A, B + B^{J_\nu} \in \mathcal{J}$ such that $f_m(A, B + B^{J_\nu}) \neq 0$ and hence $F_m(A, B + B^{J_\nu}) \neq 0$ or $F_m(X, Y)$ is non-vanishing on $\mathcal{J} = H(\Phi_m, J_\nu)$.

Remark : $F_m(X, Y)$, $m \geq 3$ is not a central polynomial for Φ_m .

If Φ is infinite let $A = \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_m)$, α_i distinct elements of Φ with $\alpha_2 = 0$ and $B = \sum_{1}^{m} e_{i\,i+1}$ in Φ_m .

Then by using equation 4.2 we get $f_m(A,B) = \text{diag}(r_1, r_2, \ldots, r_m)$ where $r_i = f(\alpha_i, \alpha_{i+1}, \ldots, \alpha_{i+m})$, f being same as in §4. It is easy to see that

$r_i = \alpha_{i+1}(\alpha_{i+1} - \alpha_{i+m-1})^{-1} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2$. Now

$r_1 = \alpha_2 (\alpha_2 - \alpha_m)^{-1} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2 \neq 0$. For $j > 1$ α_2 is not a factor of r_j and α_i are distinct hence $r_i \neq 0$. Also $F_m(A, B) = \text{diag}(r_1^2, r_2^2, \ldots, r_m^2)$ and $r_1^2 = 0$, $r_i^2 \neq 0$ for $i > 1$. Therefore $F_m(A, B) \notin \Phi 1$.

If Φ is finite with $|\Phi| = q$ consider Γ, the field extension of degree m over Φ. Let θ be the primitive element. By proposition 5.1 there exists a $B \in \Phi_m$ such that $A^q = B^{-1}AB$. Moreover there exists a $U \in \Gamma_m$ such that $UAU^{-1} = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $(UBU^{-1})^{-1} (UAU^{-1}) (UBU^{-1}) = \text{diag}(\alpha_m, \alpha_1, \ldots, \alpha_{m-1})$ where $\alpha_i = \theta^{q^{m-i}}$ for $1 \le i \le m$. The action of the above inner automorphism permutes the roots cyclically and hence $UBU^{-1} = \sum_{i=1}^{m} \beta_i e_{i\,i+1}$ and $\beta_i \neq 0$, $1 \le i \le m$. (See the proof of theorem 5.1).

Now consider $f_m(A,B) = U^{-1} f_m(UAU^{-1}, UBU^{-1}) U = \text{diag}(r_1, r_2, \ldots, r_m)$ where $r_i = \beta_1 \beta_2 \ldots \beta_m f(\alpha_i, \alpha_{i+1}, \alpha_{i+m}) = \beta_1 \beta_2 \ldots \beta_m \alpha_{i+1}(\alpha_{i+1} - \alpha_{i+m-1})^{-1} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2$.

r_i are distint. For if $r_i = r_j$ and $i \neq j$ let $i < j$ then $\alpha_{i+1}(\alpha_{i+1} - \alpha_{i+m-1})^{-1} = \alpha_{j+1}(\alpha_{j+1} - \alpha_{j+m-1})^{-1}$. Therefore $\theta^{q^{m-i-1}}(\theta^{q^{m-i-1}} - \theta^{q^{-i+1}})^{-1} = \theta^{q^{m-j-1}}(\theta^{q^{m-j-1}} - \theta^{q^{-j+1}})^{-1}$.

This implies $\theta(q^{m-1} - q)(q^{-i} - q^{-j}) = 1$ but this means $q^m | (q^{m-1} - q)(q^{-i} - q^{-j})$ or $q^{m+j-1} | (q^{m-2} - 1)(q^{j-i} - 1)$. Now $(q^{m-2} - 1)(q^{j-i} - 1) < q^{m+j-i-2} < q^{m+j-1}$ and hence $(q^{m-2} - 1)(q^{j-i} - 1) = 0$. Since $q \geq 2$ and $m \geq 3$ $q^{j-i} = 1$ which contradicts the fact $i < j$. Therefore r_i are distinct. Now consider $F_m(A,B) = \text{diag}(r_1^2, r_2^2, \ldots, r_m^2)$. Since r_i are distinct and $m \geq 3$ at least two diagonal entries of $F_m(A,B)$ are distinct proving that $F_m(A, B) \neq \Phi 1$ or $F_m(X, Y)$ is not a central polynomial for Φ_m.

REFERENCES

[1] Formanek, E., Central polynomials for matrix rings, J. of Algebra 23 (1972), pp. 129-132.

[2] Herstein, I.N., Noncommutative Rings, The Carus Mathematical Monograph 15 (1968), pp. 99-100.

[3] Jacobson, N., Lectures on Quadratic Jordan Algebras, Lecture Notes, Tata Institute, Bombay.

[4] Jacobson, N., Structure and Representation of Jordan Algebras, Amer. Math. Soc. Colloq. Publ., Vol. 39.

[5] Kaplansky, I., Problems in the theory of rings, Amer. Math. Monthly 77 (1970), pp. 445-454.

[6] Racine, M., Central Polynomials for Jordan Algebras.

[7] Racine, M., The center of quadratic Jordan Algebra.

[8] Wagner, W., Über die Grundlagen der projectiven Geometrie and allgemeine Zahlensysteme, Math. Annalen, 113 (1936), pp. 528-567.