Polynomial Time Decomposition of Modules over Algebras and its Application

Alexander Chistov * Marek Karpinski†

Abstract

Let K be algebraically or real closed field, Λ a finite dimensional assotiative K–algebra with the unity element and V a finitely generated Λ–module. An algorithm of polynomial complexity is described in the paper which decomposes V into the direct sum $V = \oplus_{i \in I} V_i$ of indecomposable Λ–modules V_i. In particular an algorithm is suggested for constructing all the projective non–isomorphic indecomposable Λ–modules. Also an algorithm of polynomial complexity is constructed which given two Λ–modules V_1 and V_2 decides whether V_1 is isomorphic to V_2 and if it is the fact constructs this isomorphism.

As an application the following results are obtained. Let $A_1, \ldots, A_m$ and $A'_1, \ldots, A'_m$ be two families of $n \times n$–matrices with coefficients from K. An algorithm of polynomial complexity is described in the paper which decides whether there exists a nonsingular (respectively orthogonal) $n \times n$–matrix S with coefficients from K such that $SA_iS^{-1} = A'_i$ for all $1 \leq i \leq m$ and if it is the fact this algorithm constructs such a matrix S.

*St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia, 14th line 39, St. Petersburg, Russia and Department of Computer Science, University of Bonn, 53117 Bonn. Research supported by the Volkswagen–Stiftung, Program on Computational Complexity.

†Department of Computer Science, University of Bonn, 53117 Bonn and International Computer Science Institute, Berkeley, California.

Introduction

The aim of this paper is to construct polynomial–time algorithms for for decomposing finitely generated modules (or representation) over associative algebras with the unity element into the direct sums of indecomposable modules (representations). The cases of algebraically or real closed ground fields are considered. Such a decomposition is unique up to the order of the direct summands due to the theorem of Krull–Schmidt which is valid in this situation [?]. We solve also in polynomial time the problem of isomorphism of two finitely generated modules over an algebra. Our presentation is self–contained in its algorithmic part and uses only some results about projective modules over an algebra Λ in its mathematical background which can be found in [?].

In the theory of representations of finite dimensional algebras both irreducible and indecomposable representations are considered. Irreducible representations correspond to simple modules over algebras.

The module is called indecomposable if it is a nonzero module and it can not be represented as a direct sum of two nonzero submodules. Indecomposable modules or representations can be characterized by the fact that their algebras of endomorphisms are local, i.e. all irreversible endomorphisms of indecomposable modules are nilpotent [?]. Each irreducible module is indecomposable. In the case when the considered algebra is semisimple each indecomposable module is irreducible and projective. The case of semisimple algebras and modules over them was considered in many papers. The references see in [?].

Many problems (similar to decomposing finitely generated modules into the direct sum) related to semisimple algebras over the field of rational numbers are hard from the point of view of the theory of complexity and at least as difficult as factoring integers [?]. So we bound ourself by the case of algebraically and real closed ground fields. Randomized and deterministic algorithms for semisimple algebras over $\mathbb{R}$ and $\mathbb{C}$ and modules over these algebras were constructed in [?], [?], [?]. The known deterministic algorithm, according to [?], for decomposing of a module over such a semisimple algebra used the reductions to the case of algebras over finite fields and the theory of lattices in a semisimple algebra over a field of algebraic numbers.

We suggest in Section 1 deterministic algorithms for decomposing modules over semisimple algebras over algebraically and real closed fields which are straitghforward and uses only linear algebra. We include this material in the paper also since we need the exact and detailed information in next sections about this decomposition.

Further, in Section 2 we consider projective modules over an arbitrary finite dimensional algebra Λ with the unity element. Let $\mathfrak{R} = \mathfrak{R}(\Lambda)$ be the radical of the algebra Λ. It is known [?] that there exists a bijective correspondence between the classes of isomorphic indecomposable projective Λ–modules and the classes of

isomorphic simple $\Lambda/\mathfrak{R}$–modules. A polynomial–time algorithm is described for constructing representatives of all classes of isomorphic indecomposable projective Λ–modules under the mentioned correspondence. We show that one can decide within the polynomial time whether a given Λ–module is projective. Besides that a polynomial–time algorithm is suggested for decomposing of a given projective module into the direct sum of indecomposable projective modules.

Decomposition of an algebra into the direct sum of projective ideals requires lifting of idempotents from its semisimple reduction modulo the radical. This construction can be considered as a generalization of Hensel's lemma. A polynomial–time algorithm for this construction is described in Section 2 when the field of definition of the reduction of these idempotents is an extension (the same for all of them) of a polynomial degree of the initial field of definition of the algebra. But when the reductions of idempotents have different fields of definition with a big composite field this construction does not wok directly in polynomial time. In Section 3 an algorithm for lifting idempotents in this situation is described.

In Section 4 the required polynomial–time algorithm for decomposition of arbitrary finitely generated Λ–modules into the direct sum of irreducible is described. Considering the algebra of endomorphisms of the given module we reduce the general case to the case of projective modules.

Further, in Section 5 an algorithm of polynomial complexity is constructed for the problem of the isomorphism of finitely generated Λ–modules, and even a more general result is obtained here. The isomorphism constructed is defined over the field of definition of the considered modules. In other words one can construct within the polynomial time the isomorphism (if it exists) of modules over algebras over a field which is a finite extension of $\mathbb{Q}$ or a finite field, see Theorem 2 below.

In Section 6 we consider applications of the results obtained to the problem of similarity of families of matrices, see Theorem 4 below Note that the solved in Section 6 problem of similarity of families of matrices is a particular case of the following well Edmond's problem. Given a subspace W of the space of square matrices over a field, decide within a polynomial time whether the determinant is not identical zero on W.

In Section 7 a polynomial–time algorithm is constructed for the problem of orthogonal similarity of families of matrices, see Theorem 5 below.

Now we give the precise statements. Let H be the field of rational numbers $\mathbb{Q}$ or a finite field of q elements, the characteristic $\mathrm{char}(H) = p$ (so p is a prime or zero); the field $k = H(\theta)$ where θ is algebraic over the field H with the minimal polynomial $F \in H[Z]$ and leading coefficient $\mathrm{lc}_Z F$ of F is equal to 1. We shall consider two cases. In the first case denote by $K = \overline{k}$ the algebraic closure of k. In the second case suppose that k is a real field, i.e. θ is a real root of F and denote by $K = \widetilde{k}$ the real closure of k, see e.g. [?].

Let Λ' be an associative k–algebra which is given by its basis $\{\lambda_i\}_{1\leq i\leq n}$ and multiplication table

$$\lambda_i\lambda_j = \sum_{1\leq s\leq n} c_{i,j}^{(s)}\lambda_s,\ 1\leq i,j\leq n$$

where all $c_{i,j}^{(s)}\in k$. Let the K–algebra $\Lambda = \Lambda'\otimes_k K$. In this situation we shall say that Λ is defined over the field k and is given by its k–structure. We shall use the similar definition also for extensions k_1 of k instead of k.

If it is not specially mentioned the modules and the ideals considered in the paper are left modules and the ideals. Let V' be a finitely generated Λ'–module which is given by its basis $\{v_j\}_{1\leq j\leq m}$ and by the multiplication table giving the action of Λ' on V':

$$\lambda_i v_j = \sum_{1\leq s\leq m} d_{i,j}^{(s)} v_s,\ 1\leq i\leq n,\ 1\leq j\leq m$$

where all $d_{i,j}^{(s)}\in k$. Let the Λ–module $V = V'\otimes_k K$. In this situation we shall say that the module V is defined over the field k and is given by its k–structure. The homomorphism $V_1\to V_2$ of two Λ–modules defined over k is defined over k if and only if it is induced by the homomorphism $V_1'\to V_2'$ of k–structures by the extension of scalars. We shall use the similar definition also for extensions k_1 of k instead of k.

Set $H_0 = \mathbb{Z}$ if $H = \mathbb{Q}$ and $H_0 = H$ if H is a finite field. We shall represent an arbitrary polynomial $f\in k[X]$ in the form

$$f = \frac{1}{a_0}\sum_i \sum_{0\leq j<degf} a_{i,j}\theta^j X^i\,,$$

where $a_0, a_i\in H_0$, $\gcd_{i,j}(a_0, a_{i,j}) = 1$. Define the length $l(a)$ of $a\in H_0$ by the formula $l(a) = \min\{s\in\mathbb{Z}:\ |a|<2^{s-1}\}$ if $H_0 = \mathbb{Z}$ and $l(a) = \min\{s\in\mathbb{Z}:\ q\leq 2^s\}$ if H is a finite field with q elements. The length $l(f)$ of coefficients from H_0 of the polynomial f is defined to be the maximum of length of coefficients from H_0 of polynomials $a_0, a_{i,j}$ and in the similar way one can define $l(f)$ for a polynomial $f\in k_1[X]$ where the field $k_1 = H(\theta_1)$ and the element θ_1 are analogous to k and θ; in particular one can do it when k_1 is algebraic over k.

We shall suppose that we have the following bounds

$$\deg_Z(F) < d_1,\ l(F) < M_1\ l(c_{i,j}^{(s)}) < M_2\ l(d_{i,j}^{(s)}) < M_3$$

for i, j, s.

The size $L(f)$ of the polynomial f such as above is defined to be the product of $l(f)$ to the number of all the coefficients from H_0 of f in the dense representation. Thus, we have

$$L(F) < d_1M_1,\ L(c_{i,j}^{(s)}) < d_1M_2,\ L(d_{i,j}^{(s)}) < d_1M_3\ .$$

Now we can formulate our results.

THEOREM 1. Let the algebra Λ and the module V be as above. Then one can construct within the time polynomial in d_1, M_1, M_2, M_3, n, m and the characteristic of the field k the isomorphism of the decomposition into the direct sum

$$V \simeq \oplus_{i \in I} V_i^{\varepsilon_i}$$

where all V_i are indecomposable Λ–modules, $1 \leq \varepsilon_i \in \mathbb{Z}$, I is a finite set. The module V_i is defined over over a separable extension K_i of k which is constructed. The degree $[K_i : k] \leq m^6$, if $K = \widetilde{k}$ and $[K_i : k] \leq m^3$, if $K = \overline{k}$. Besides that, the representation of V_i by its K_i–structure is constructed for every $i \in I$.

Now consider two Λ–modules V_1 and V_2 similar to V and defined by their k–structures V_1' and V_2'. Let $d_{1,i,j}^{(s)}$ and $d_{2,i,j}^{(s)}$ be similar to $d_{i,j}^{(s)}$ and satisfy to the same estimations for $\deg_{t_\alpha}$ and the lengths of coefficients from H_0 as $d_{i,j}^{(s)}$.

THEOREM 2. One can decide within the time polynomial in d_1, M_1, M_2, M_3, n, m and the characteristic of the field k whether the Λ–modules V_1 and V_2 are isomorphic and if it is the fact to construct the isomorphism between them. Besides that, one can construct such an isomorphism defined over the field k, i.e. this isomorphism is given by the isomorphism of Λ'-modules V_1' and V_2'.

THEOREM 3. Let the algebra Λ and the module V be as above. Then one can decide within the time polynomial in d_1, M_1, M_2, M_3, n, m whether V is a projective Λ–module. One can construct within the time polynomial in d_1, d_2, M_1, M_2, n and the characteristic of the field k the system of representatives $\mathcal{S}$ of all classes of isomorphic indecomposable projective Λ–modules, herewith $\#\mathcal{S} \leq n$.

Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ be two families of $r \times r$–matrices with coefficients from the field k. Let $A_i = (a_{i,j_1,j_2})_{1 \leq j_1,j_2 \leq r}$, $B_i = (b_{i,j_1,j_2})_{1 \leq j_1,j_2 \leq r}$ where all the coefficients $a_{i,j_1,j_2}, b_{i,j_1,j_2} \in k$. Let all $a_{i,j_1,j_2}, b_{i,j_1,j_2}$ satisfy to the same estimations for the lengths of coefficients from H_0 as $d_{i,j}^{(s)}$.

THEOREM 4. Let two families $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ of $r \times r$–matrices with coefficients from the field k be given. Then within the time polynomial in d_1, M_1, M_2, M_3, n, m, r and the characteristic of the field k one can decide whether there exists a nonsingular $r \times r$–matrix S with coefficient from K such that $SA_iS^{-1} = B_i$ for all $1 \leq i \leq m$ and if it is the fact can construct such a matrix S. Besides that, such a matrix S can be constructed with coefficients from k.

Let K be real closed. The square matrix A with coefficients from K is orthogonal if and only if $AA^T = E$ where A^T is transposed to A and E is the unity matrix.

THEOREM 5. Let k be a real ordered field and K real closure of k. Let two families $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ of $r \times r$–matrices with coefficients from the field k be given. Then within the time polynomial in d_1, M_1, M_2, M_3, n, m, r one can decide whether there exists an orthogonal $r \times r$–matrix S with coefficient from K such that $SA_iS^{-1} = B_i$ for all $1 \leq i \leq m$ and if it is the fact can construct such a matrix S.

1 Algorithms for semisimple algebras and modules over them

The material of this section is known, see [?],[?], [?]. But for the completeness and since our representation of input data is slightly different from the considered earlier we shall sketched the required results with the proofs.

Let an algebra Λ and a finitely generated Λ–module V be given, see introduction. Suppose additionally that the algebra Λ is semisimple, i.e. the radical $\mathfrak{R} = \mathfrak{R}(\Lambda) = 0$. In this case by the structural theorems about semisimple algebras and modules over them, see e.g. [?],

$$\Lambda = \oplus_{i \in I} \Lambda_i \tag{1}$$

where all Λ_i are simple algebras over K and I is a finite set. Further, $V = \oplus_{i \in I} \Lambda_i V$ where each $\Lambda_i V$ is Λ–module and Λ_i–module. Besides that, $\Lambda_i V$ is an isotypical module or equal to zero, i.e. $\Lambda_i V \simeq U_i^{\varepsilon_i}$ where U_i is a (uniquely defined up to isomorphism) simple Λ_i–module, $0 \leq \varepsilon_i \in \mathbb{Z}$ for all $i \in I$. So we have the decomposition of V into the direct sum of simple (and indecomposable) modules

$$V \simeq \oplus_{i \in I} U_i^{\varepsilon_i}. \tag{2}$$

We have $\Lambda \simeq \Lambda' \otimes_k K$ and we shall identify Λ and $\Lambda' \otimes_k K$ using this isomorphism.

To construct (1) denote by $Z = Z(\Lambda) = \{c \in \Lambda : c\lambda_i = \lambda_i c \ \forall 1 \leq i \leq n\}$ the center of the algebra Λ. Similarly $Z' = Z(\Lambda') = \{c \in \Lambda' : c\lambda_i = \lambda_i c \ \forall 1 \leq i \leq n\}$ is the center of the algebra Λ'. So we have $Z(\Lambda) \simeq Z(\Lambda') \otimes_k K$, $\dim_k Z' \leq n$.

Compute the k–basis $c_j, j \in J$ of Z' and a primitive element c of the separable commutative algebra Z' over k. Thus, the isomorphism $Z' = k[c] \simeq k[Z]/(f(Z))$ is constructed where f is minimal polynomial of c over k such that the leading coefficient $\mathrm{lc}_Z f = 1$. We have $\deg_Z f \leq n$. The algorithm for constructing a primitive element is similar to the case when Z' is a field, see e.g. [?]. So $c = \sum_{j \in J} z_j c_j$ where all $z_j \in \mathbb{Z}$, $|z_j| < n^2$. Factor $f = \prod_{i \in I_1} f_i$ where f_i are irreducible over k polynomials with $\mathrm{lc}_Z f_i = 1$ for all i. Denote by $H_i = \{\eta \in \overline{k} : f_i(\eta) = 0\}$ the set of roots of the polynomial f_i in the algebraically closed field $\overline{k}$.

Suppose that $\deg_Z f > 1$. Then for every $i \in I_1$ and $\eta \in H_i$ denote $f_\eta = f(Z_1)/(Z_1 - \eta) \in k[\eta][Z_1]$ where Z_1 is a new variable. Set $\eta_1 = Z_1 \bmod f_\eta \in k[\eta][Z_1]/(f_\eta)$. Note that k–algebras $k[\eta, \eta_1]$ are isomorphic over k for different $\eta \in H_i$. We have $\dim_k k[\eta, \eta'] \leq n(n-1)/2$.

At first, consider the case when $K = \overline{k}$. So the elements of H_i are conjugated over k. We have

$$Z = Z' \otimes_k K \simeq K[Z]/(f(Z)) \simeq \prod_{i \in I_1} \prod_{\eta \in H_i} K[Z]/(Z - \eta) \simeq \prod_{i \in I_1} \prod_{\eta \in H_i} k[\eta] \otimes_{k[\eta]} K. \tag{3}$$

Then

$$\prod_{\eta' \in H_i, \eta' \neq \eta} k[\eta'] \otimes_{k[\eta']} K \simeq k[\eta][Z_1]/(f_\eta) \otimes_{k[\eta]} K$$

and therefore,

$$Z' \otimes_k k[\eta] \simeq k[\eta][Z_1]/(f_\eta) \times k[\eta],$$

$$Z \simeq k[\eta][Z_1]/(f_\eta) \otimes_{k[\eta]} K \times k[\eta] \otimes_{k[\eta]} K.$$

Thus, for every $i \in I_1$ and $\eta \in H_i$ solving a linear system over the field $k[\eta]$ construct the central idempotent $e_\eta \in Z' \otimes_k k[\eta] \subset \Lambda' \otimes_k k[\eta] \subset \Lambda$ such that $e_\eta Z = k[\eta] \otimes_{k[\eta]} K$ under isomorphism (3). Set $\Lambda_\eta = \Lambda e_\eta$ and $\Lambda'_\eta = \Lambda' e_\eta$ and construct a $k[\eta]$–basis of Λ'_η. Then Λ'_η is a simple $k[\eta]$–algebra, Λ_η is a simple K–algebra, $\Lambda_\eta = \Lambda'_\eta \otimes_{k[\eta]} K$ for every for every $i \in I_1$ and $\eta' \in H_i$ and we have the isomorphism

$$\Lambda \simeq \prod_{i \in I_1} \prod_{\eta \in H_i} \Lambda_\eta$$

which gives isomorphism (1) after changing the set of indices. It is proved additionally that each simple algebra Λ_η is defined over the field $k[\eta]$ and the element η has minimal polynomial f_i, over k with $\deg_Z f_i \leq n$, $i \in I_1$.

Now consider the case when $K = \widetilde{k}$, in particular $\mathrm{char}(k) = 0$. Compute positive integers $z_1, z_2 \leq \mathcal{P}(n)$ for a polynomial $\mathcal{P}$ such that the element $\xi' = z_1(\eta + \eta_1) + z_2\eta\eta_1$ is a primitive element of the subalgebra $k[\eta+\eta_1, \eta\eta_1]$ of separable commutative algebra $k[\eta, \eta_1]$ for every $i \in I_1$ and $\eta \in H_i$. Compute the minimal polynomial Φ_i of the element $\xi' \in k[\eta, \eta_1]$ over k. We have $\deg \Phi_i \leq n(n-1)/2$.

REMARK 1. Additionally we require that G.C.D.$(\prod_{i \in I_1} \Phi_i, f) = 1$ (there exist always $z_1, z_2 \leq \mathcal{P}(n)$ such that this additional condition is satisfied). Note that the last condition about G.C.D. will be required later only for defining the set I of indices which must be different. One can do not require the fulfillment of this condition but choose another denotations for the set of indices I later.

Compute the representation

$$\eta + \eta_1 = S_1(\xi') = \sum_{0 \leq j \leq \deg \Phi} s_{1,j} \xi'^j \in k[\xi'],$$

$$\eta\eta_1 = S_2(\xi') = \sum_{0 \leq j \leq \deg \Phi} s_{2,j} \xi'^j \in k[\xi']$$

where all $s_{1,j}, s_{2,j} \in k$. Factor $\Phi_i = \prod_{j \in J_i} \Phi_j$ where Φ_j are irreducible over k polynomials with $\mathrm{lc}_Z \Phi_j = 1$ for all $i \in I_1, j \in J_i$. We have $\deg \Phi_j \leq n(n-1)/2$.

Set $H'_i = H_i \cap \widetilde{k}$ and

$$\Xi_j = \{\xi \in \widetilde{k} \, : \, \Phi_j(\xi) = 0 \,\&\, S_1(\xi)^2 - 4S_2(\xi) < 0\}.$$

Set the field $k[\xi, \eta'] = k[\xi][Z]/(Z^2 - S_1(\xi)Z + S_2(\xi))$ where $\eta' = Z \bmod Z^2 - S_1(\xi)Z + S_2(\xi)$. The roots of Φ and therefore, the elements of Ξ_j can be given by their approximations in $\mathbb{Q}[\sqrt{-1}]$ with precision $2^{-M_1 \mathcal{P}(n)}$ for some polynomial $\mathcal{P}$.

For arbitrary $\eta \in H_i \setminus H_i'$ denote by $\overline{\eta}$ its conjugate over $\overline{k}$. Now we have

$$\begin{array}{l} Z = Z' \otimes_k K \simeq K[Z]/(f(Z)) \simeq \\ \prod_{i\in I_1}(\prod_{\eta\in H_i'} K[Z]/(Z-\eta) \times \prod_{\{\eta,\overline{\eta}\}\subset H_i\setminus H_i'} K[Z]/((Z-\eta)(Z-\overline{\eta}))) \simeq \\ \prod_{i\in I_1}(\prod_{\eta\in H_i'} K[Z]/(Z-\eta) \times \prod_{j\in J_i}\prod_{\xi\in\Xi_j} K[Z]/(Z^2 - S_1(\xi)Z + S_2(\xi))) \simeq \\ \prod_{i\in I_1}(\prod_{\eta\in H_i'} k[\eta] \otimes_{k[\eta]} K \times \prod_{j\in J_i}\prod_{\xi\in\Xi_j} k[\xi,\eta'] \otimes_{k[\xi]} K) \end{array} \tag{4}$$

Similarly to the considered case of algebraically closed field construct for every $i \in I_1$ and $\eta \in H_i'$ the central idempotent $e_\eta \in Z' \otimes_k k[\eta] \subset \Lambda' \otimes_k k[\eta] \subset \Lambda$ such that $e_\eta Z = k[\eta] \otimes_{k[\eta]} K$ under isomorphism (4). Set $\Lambda_\eta = \Lambda e_\eta$ and $\Lambda_\eta' = \Lambda' e_\eta$ and construct a $k[\eta]$–basis of Λ_η'. Then Λ_η' is a simple $k[\eta]$–algebra, Λ_η is a simple K–algebra, $\Lambda_\eta = \Lambda_\eta' \otimes_{k[\eta]} K$, i.e. Λ_η is defined over $k[\eta]$. The center of Λ_η' is $k[\eta]$, the center of Λ_η is $K = k[\eta] \otimes_{k[\eta]} K$

Further, in a similar way for every $i \in I_1$, $j \in J_i$ and $\xi \in \Xi_j$ construct the central idempotent $e_\xi \in Z' \otimes_k k[\xi] \subset \Lambda' \otimes_k k[\xi] \subset \Lambda$ such that $e_\xi Z = k[\xi,\eta'] \otimes_{k[\xi]} K$ under isomorphism (4). Set $\Lambda_\xi = \Lambda e_\xi$ and $\Lambda_\xi' = \Lambda' e_\xi$ and construct a $k[\xi]$–basis of Λ_ξ'. Then Λ_ξ' is a simple $k[\xi]$–algebra, Λ_ξ is a simple K–algebra, $\Lambda_\xi = \Lambda_\xi' \otimes_{k[\xi]} K$, i.e. Λ_ξ is defined over $k[\xi]$. The center of Λ_ξ' is $k[\xi,\eta']$, the center of Λ_ξ is $\overline{K} = K[\eta'] = k[\xi,\eta'] \otimes_{k[\xi]} K$. Construct a $k[\xi,\eta']$–basis of Λ_ξ'. Denote by Φ the minimal polynomial of the element ξ over k with leading coefficient $\mathrm{lc}\Phi = 1$. So we have $\deg\Phi \le n(n-1)/2$.

If $\eta \in H_i \setminus H_i'$ and $\overline{\eta}$ is conjugated to η over k then define also the nonzero idempotents $e_\eta, e_{\overline{\eta}} \in \Lambda \otimes_K \overline{K} \supset \Lambda$ such that $e_\eta + e_{\overline{\eta}} = e_\xi$ where $\xi = e_\eta + e_{\overline{\eta}} + z e_\eta e_{\overline{\eta}}$.

Therefore, we have the isomorphism

$$\Lambda \simeq \prod_{i\in I_1}(\prod_{\eta\in H_i'} \Lambda_\eta \times \prod_{j\in J_i}\prod_{\xi\in\Xi_j} \Lambda_\xi)$$

which gives isomorphism (1) after changing the set of indices.

The described above construction of the decomposition of Λ into the direct product can be effect also in the case when $\deg f = 1$. It is trivial in this case.

Set

$$I = \bigcup_{i\in I_1} H_i \text{ if } K = \overline{k}$$

and

$$I = \bigcup_{i\in I_1}(H_i' \cup \bigcup_{j\in J_i} \Xi_j) \text{ if } K = \widetilde{k}.$$

Set $E_i = H_i$ if $K = \overline{k}$ and $E_i = H_i' \cup \bigcup_{j\in J_i} \Xi_j$ if $K = \widetilde{k}$. So we have in the both cases

$$I = \bigcup_{i\in I_1} E_i$$

Thus, isomorphism (1) is constructed and we can suppose that every Λ_i is defined over a finite extension k_i of the field k, $k_i \subset K$, i.e. $\Lambda_i \simeq \Lambda_i' \otimes_{k_i} K$ where Λ_i' is a

simple k_i algebra. The field k_i (which is $k[\eta]$ or $k[\xi]$ in denotations of (3) and (4)) and the k_i–basis of the algebra $\Lambda'_i \subset \Lambda' \otimes_k k_i$ are constructed for every $i \in I$. Denote by k'_i the center of Λ'_i (which is $k[\eta]$ or $k[\xi, \eta']$) in denotations of (3) and (4)). Then Λ'_i is a simple central k'_i–algebra and Λ_i is a simple central $k'_i \otimes_{k_i} K$–algebra (note that $k'_i \otimes_{k_i} K = K$–algebra if $k_i = k[\eta]$ and $k'_i \otimes_{k_i} K = \overline{K}$ if $k_i = k[\xi]$ in denotations of (3) and (4)). The field k'_i and the k'_i–basis of the algebra $\Lambda'_i \subset \Lambda' \otimes_k k'_i$ are constructed for every $i \in I$.

We have $\Lambda = \Lambda' \otimes_k K$ and $\Lambda \otimes_K \overline{K} = \Lambda' \otimes_k \overline{K}$. Hence, the Galois group $\mathrm{Gal}(K/k)$ acts in the natural way on Λ and the Galois group $\mathrm{Gal}(\overline{K}/k)$ acts on $\Lambda \otimes_K \overline{K}$. These actions are trivial on Λ'.

Now let A' be an L–structure of a submodule A (of Λ) defined over the field L which is an extension of k. Then every embedding $\sigma : L \to K$ over k is extended uniquely till the embedding $A' \to \Lambda$ which we shall also denote without ambiguity by σ. This embedding $\sigma : A' \to \Lambda$ is such that $\sigma(a) = a^{\widetilde{\sigma}}$ for $a \in A'$ where $\widetilde{\sigma} \in \mathrm{Gal}(K/k)$ is an arbitrary element for which the restriction $\widetilde{\sigma}|_L = \sigma$. The embedding $\sigma : A' \to \Lambda$ does not depend on the choice of $\widetilde{\sigma}$ since A' is invariant relatively to the Galois group $\mathrm{Gal}(K/L)$.

REMARK 2. For every $i \in I$ and for every embedding $\sigma : k_i \to K$ of fields over k there exists $j \in I$ such that $i = j^\sigma$ and there exists $u \in I_1$ such that $i, j \in E_u$ under our choice of the sets of indices. Besides that we have for such $i, j \in E_u$ that $(\Lambda'_i)^\sigma = \Lambda'_j$ and for the idempotents $e_i^\sigma = e_j$.

REMARK 3. Set for $i \in I_1$ the algebra $\Lambda_i = \oplus_{j \in E_i} \Lambda_j$. The central idempotent corresponding to the algebra Λ_i is equal in the both cases to $\sum_{j \in H_i} e_j = \sum_{j \in E_i} e_j$. So the algebras Λ_i, $i \in I_1$ are defined over the field k and $\sum_{i \in I_1} \Lambda_i \simeq \Lambda$. The k–structures for the algebras Λ_i, $i \in I_1$ and this isomorphism defined over the field k can be constructed within the polynomial time as it follows from the construction described.

Now our aim will be to construct for every $i \in I$ the simple Λ_i–module U_i. Note that $\Lambda_i \simeq U_i^{m_i}$ where $1 \leq m_i \in \mathbb{Z}$. Construct a k_i–basis of the Λ'_i–module $\Lambda'_i \subset \Lambda_i \otimes_k k_i$.

Let $\{\lambda_{i,j}\}_{1 \leq j \leq n_i}$ be the k_i–basis of Λ'_i constructed with the multiplication table and defining the algebra Λ'_i. So we have the regular representation $j : \Lambda_i \to M_{n_i}(K)$ of the algebra Λ_i given by the basis $\{\lambda_{i,j}\}_{1 \leq j \leq n_i}$.

If $K = \overline{k}$ then by the the Wedderbern theorem we have $\Lambda_i \simeq M_{m_i}(K)$ where $M_{m_i}(K)$ is the matrix algebra over K of the order $m_i = \sqrt{n_i}$ and the simple module over Λ_i is isomorphic to the space of columns K^{m_i}.

If $K = \widetilde{k}$ then by the Wedderbern theorem, see e.g. [**?**], we have $\Lambda_i \simeq M_{m_i}(D_i)$ where $M_{m_i}(D_i)$ is a matrix algebra of the order m_i over the division algebra D_i over K and the simple module over Λ_i is isomorphic to the space of columns $D_i^{m_i}$. Besides that, Λ_i is identified with the algebra of endomorphisms $\mathrm{Hom}_{D_i}(D_i^{m_i}, D_i^{m_i})$ of the right D_i–vector space $D_i^{m_i}$. Further, we have one of the following cases

(i) $D_i = K$,

(ii) $D_i = K[\sqrt{-1}] = \overline{K}$,

(iii) $D_i = \mathbb{H}(K)$ where $\mathbb{H}(K)$ is the algebra of the Hamiltonian quaternions over K, i.e. this algebra has the basis $1, \mathbf{i}, \mathbf{j}, \mathbf{ij}$ over K with the multiplication table $\mathbf{i}^2 = \mathbf{j}^2 = -1$, $\mathbf{ij} = -\mathbf{ji}$,

Set $\dim_K D_i = d_i$ where $d_i > 0$. Then d_i is equal to $1, 2$ or 4 according to cases (i), (ii) or (iii). We have $n_i = m_i^2 d_i$. Set also $D_i = K$, $d_i = 1$ if $K = \overline{k}$. Note that the case (ii) holds if and only if $k_i' \neq k_i$, i.e. when $Z(\Lambda_i) = k[\xi, \eta']$ for some ξ and η' in (4). So we can always decide whether (iii) holds.

Suppose also without loss of generality, extending in advance if it is necessary the field H, that it contains sufficiently many elements, namely, more than $\mathcal{P}(n)$ elements for some polynomial $\mathcal{P}$. Let $a = \sum_{1 \leq j \leq n_i} a_j \lambda_{i,j} \in \Lambda_i'$ be a nonzero element such that all coefficients $a_j \in H_0$ and have small sizes $l(a_j) < \mathcal{O}(\log n)$ if $H_0 = \mathbb{Z}$. In the case when $K = \overline{k}$ choose such an element a. In the case when $K = \widetilde{k}$ we shall specify later (when the case $K = \overline{k}$ will be considered completely) how to choose a. So let a be given.

Compute the characteristic polynomial $\chi_1 \in k_i[Z]$ of the matrix $j(a) \in M_{n_i}(K)$. Factor χ_1 over k_i. Similarly to that it was by constructing isomorphisms (3) and (4) for every irreducible over k_i factor χ_2 of the polynomial χ_1 construct the set of irreducible over K factors $\chi_3 \,|\, \chi_2$ with leading coefficient $\mathrm{lc}\chi_3 = 1$. So the degree of χ_3 is 1 or 2 and the last case may occur only when $K = \widetilde{k}$. More precisely, construct for every χ_3 the field $k_i[\zeta] \supset k_i$ (it depends on χ_3) generated by the coefficients of χ_3, $k_i[\zeta] \subset K$, c.f. constructing $k[\xi]$ above. The element ζ is given over the field k_i by its minimal polynomial $\Psi_i \in k_i[Z]$ with $\mathrm{lc}_Z \Psi = 1$. Denote $K_i = k_i[\zeta]$ Set $W(\chi_3) = \{x \in \Lambda_i \,:\, \chi_3(j(a))x = 0\}$ the annulator of $\chi_3(j(a))$ and $d(\chi_3) = \dim_K W(\chi_3)$. Set $d(a) = \min_{\chi_3 | \chi_2 | \chi_1} d(\chi_3)$.

The multiplicity of every root of χ_1 is no less than $m_i = \sqrt{n_i/d_i} \geq \sqrt{n_i}/2$. So the degree of the minimal polynomial of the matrix $j(a)$ is no more than $\sqrt{n_i d_i} \leq 2\sqrt{n}$. Hence, $\deg \Psi_i \leq 2n$ if $K = \widetilde{k}$ and $\deg \Psi_i \leq \sqrt{n_i}$ if $K = \overline{k}$. Therefore, the degree $[K_i : k] \leq n^3$ if $K = \widetilde{k}$ and $[K_i : k] \leq n^{3/2}$ if $K = \overline{k}$.

REMARK 4. If $K = \overline{k}$ then we shall suppose also that we choose polynomials χ_3 such that additionally the following condition is satisfied. If $i, j \in I$ and the embedding $k_i \to K$ of fields over k are such that $j = i^\sigma$ (see Remark 2) than $\Psi_i^\sigma = \Psi_j$ i.e the coefficients of polynomials Ψ_i and Ψ_j are conjugated by σ.

Note also that $W(\chi_3)$ is defined over K_i. Namely, set $W'(\chi_3) = \{x \in \Lambda_i' \otimes_{k_i} K_i \,:\, \chi_3(j(a))x = 0\}$. Then $W(\chi_3) = W'(\chi_3) \otimes_{K_i} K$ and $d(\chi_3) = \dim_{K_i} W'(\chi_3)$. So all $d(\chi_3)$ and therefore $d(a)$ can be computed within the polynomial time. Compute $d(a)$ and denote by χ some factor χ_3 for which $d(a) = d(\chi)$ and fix χ. So the field generated by the coefficients of χ is $K_i \subset K$.

Show that $d(a) \geq m_i d_i$ and $m_i d_i \,|\, d(a)$. Set $U_i(\chi) = \{x \in U_i \,:\, \chi(j(a))x = 0\}$ the annulator of $\chi(j(a))$. Then $W(\chi) \simeq U_i(\chi)^{m_i}$ and $W(\chi)$, $U_i(\chi)$ are nonzero right linear spaces over D_i. Therefore, $\dim_K U_i(\chi) \geq d_i$ and $d(a) \geq \dim_K W(\chi) = m_i \dim_K U_i(\chi) = m_i d_i \dim_{D_i} U_i(\chi) \geq m_i d_i$. The required assertion is proved.

Suppose that if $K = \overline{k}$ then $d(a) > m_i = \sqrt{n_i}$; if $K = \widetilde{k}$ then $d(a) = m_i \max\{2, d_i\} = 2\sqrt{n_i}$ and (i) or (iii) holds. In this case we shall construct a new element a' similar to a such that $d(a') < d(a)$ if it exists. If $K = \overline{k}$ we shall show that a' exists in our assumptions. If $K = \widetilde{k}$ and a' exists in our assumptions then (i) holds and we shall show that conversely if (i) holds then a' exists.

To construct a' compute the K_i–basis $\mathbf{e}$ of the space $W'(\chi)$. Compute an additional family of vectors $\mathbf{e}'$ such that $\mathbf{e}, \mathbf{e}'$ is a K_i–basis of the algebra $\Lambda_i' \otimes_{k_i} K_i$

Set the subalgebra

$$C' = \{x \in \Lambda_i' \otimes_{k_i} K_i \,:\, xW'(\chi) \subset W'(\chi)\}.$$

The condition $xW'(\chi) \subset W'(\chi)$ is equivalent to the fact that $xe \in W'(\chi)$ for every element e from the basis $\mathbf{e}$. This is equivalent to the fact that all the coefficients in the elements from $\mathbf{e}'$ of the representation of the vector xe in the basis $\mathbf{e}, \mathbf{e}'$ are zeros for every element e from $\mathbf{e}$. So solving the linear system relatively to the coefficients in the representation of x in the basis of $\Lambda_i' \otimes_{k_i} K_i$ compute the K_i–basis of the algebra C'.

So $W'(\chi)$ is C'–module. Denote by $C'(\chi)$ the image of the trough homomorphism

$$j_1 \,:\, C' \to \mathrm{Hom}_{K_i}(W'(\chi), W'(\chi)) \simeq M_{d(a)}(K_i)$$

and construct the basis over K_i of $C'(\chi) \subset M_{d(a)}(K_i)$ (recall that the basis of $W'(\chi)$ was chosen above). We have $W(\chi) \simeq U_i(\chi)^{m_i}$ and $U_i(\chi) \subset U_i$ is a right vector subspace over D_i of the simple module U_i. In particular, $\dim_K U_i(\chi) = d(a)/(m_i d_i)$. Further, Λ_i is identified with the algebra of endomorphisms $\mathrm{Hom}_{D_i}(U_i, U_i)$ of the right D_i–vector space U_i.

Therefore, the algebra $C = C' \otimes_{K_i} K \simeq \{x \in M_{m_i}(D_i) \,:\, xU_i(\chi) \subset U_i(\chi)\}$ and $C(\chi) = C'(\chi) \otimes_{K_i} K \simeq M_{d(a)/(m_i d_i)}(D_i)$. Therefore, our assumption that $d(a)/m_i > 1$ if $K = \overline{k}$ and $d(a)/m_i = \max\{2, d_i\}$ implies $\dim_{K_i} C'(\chi) > 1$ if $K = \overline{k}$ and $\dim_{K_i} C'(\chi) = 4$ if $K = \widetilde{k}$.

LEMMA 1.

(a) If $K = \overline{k}$ one can construct within the polynomial time an element $b \in C'(\chi)$ such that $b \notin 1 \cdot K_i$ where 1 is the unity element of $C'(\chi)$ if $K = \overline{k}$,

(b) If $K = \widetilde{k}$ then one can decide within the polynomial time whether there exists an element $b \in C'(\chi)$ such that the minimal polynomial of the matrix $b \in M_{d(a)}(K_i)$ over K_i is not equal to a linear polynomial or square polynomial with negative discriminant. More precisely, such an element b exists if (i) holds and does not exists if (iii) holds. One can construct b if it exists within the polynomial time.

PROOF. We need only to prove (b). Compute an element $c \in C'(\chi)$ such that 1, c are linearly independent over K_i. So the minimal polynomials of c over K_i is not linear. Hence, we can suppose without loss of generality (otherwise the required b can be constructed) that this minimal polynomial is a square polynomial with negative discriminant. Replacing c by $c-\nu\cdot 1$ with appropriate $\nu \in K_i$ we can suppose without loss of generality that $c^2 = -\nu_1 \cdot 1$ where $\nu_1 > 0$. Now compute an element $d \in C'(\chi) \setminus K_i[c]$. This is possible since $\dim_{K_i} C'(\chi) = 4$. Similarly we can suppose without loss of generality that $d^2 = -\nu_2 \cdot 1$ where $\nu_2 > 0$.

Now our aim is to prove that we can suppose without loss of generality (otherwise the required b can be constructed) that $cd + dc = 0$. Indeed, consider the element $c+\tau d \in C'(\chi)$ where $\tau \in K_i$. Similarly as it was above we can suppose without loss of generality that $(c + \tau d - \tau_1 \cdot 1)^2 = \tau_2 \cdot 1$, $\tau_2 < 0$ for uniquely defined $\tau_1, \tau_2 \in K_i$ depending on τ. So we have

$$(-\nu_1 - \nu_2\tau^2 - \tau_2)\cdot 1 - 2\tau_1(c+\tau d) + \tau(cd+dc) = 0.$$

If there exist two different τ for which $\tau_1 \neq 0$ we get from here a contradiction that 1, c, d are linearly dependent over K_i. Therefore, $cd + dc = \tau_3 \cdot 1$ where $\tau_3 \in K_i$. Further, note that $cd \notin K_i[c]$. So replacing d by cd in our consideration we can suppose without loss of generality that $c(cd) + (cd)c = \tau_4 \cdot 1$ where $\tau_3 \in K_i$. But on the other hand $c(cd) + (cd)c = c^2 d + (\tau_3 \cdot 1 - dc)c = \tau_3 c$. Therefore, $\tau_3 = \tau_4 = 0$ and our assertion is proved. So we have got that the subalgebra $K_i[c,d] \subset C'(\chi)$ has the basis 1, c, d, cd and is a quaternions algebra and hence (iii) holds. In this case one get immediately that there exists no b. In other cases one can construct the required element b. Therefore, $C(\chi) = C'(\chi) \otimes_{K_i} K$ is not isomorphic to the quaternions algebra. Hence, (i) holds. The Lemma is proved.

Suppose that b is constructed. Solving a linear system compute the set $\mathcal{L}$ of the elements $b' \in C'$ such that $j_1(b') = b$. Note that the factor space $(\Lambda_i' \otimes_{k_i} K_i)/W'(\chi)$ is C'–module. So we have the natural homomorphism

$$j_2 : C' \to \mathrm{Hom}_{K_i}((\Lambda_i' \otimes_{k_i} K_i)/W'(\chi), (\Lambda_i' \otimes_{k_i} K_i)/W'(\chi)).$$

Choose an element $h \in H_0$ which is different from all roots of the characteristic polynomial of the matrix b. Show that there exists $b'' \in \mathcal{L}$ such that $j_2(b'') = h \cdot 1$ where 1 is the identity isomorphism of $(\Lambda_i \otimes_{k_i} K_i)/W'(\chi)$. Indeed, extending the field we get that $\Lambda_i/W(\chi) \simeq (U_i/U_i(\chi))^{m_i}$, the image of $j_2 \otimes_{K_i} K$ is isomorphic to $M_{r_i}(D_i)$ where $r_i = m_i - d(a)/(m_i d_i)$ and the natural homomorphism $C \to C(\chi) \times M_{r_i}(D_i)$ is an epimorphism defined over the field K_i. Our assertion is proved. Thus, again solving the K_i–linear system relatively to parametric coefficients in the representation of $\mathcal{L}$ as an affine subspace of C', compute such an element $b'' \in \mathcal{L}$.

One gets immediately from the construction described that $d(b'') < d(a)$. Let $K = \widetilde{k}$. In this case set $g = b''$ if (i) holds and $g = a$ if (iii) holds. Thus, we have $d(g) = m_i d_i$ in the considered cases.

LEMMA 2. Let $K = \overline{k}$. Let $u, v \in \Lambda_i'$ be nonzero elements and $t \in K_i$. Then $d(u+tv) \leq \min\{d(u), d(v)\}$ for all excepting of at most $\mathcal{P}(n)$ elements $t \in K_i$ for some polynomial $\mathcal{P}$.

PROOF. Let $K((T))$ be the field power series in T with algebraic closure $\overline{K((T))}$ and $\mathrm{ord}_T : \overline{K((T))} \to \mathbb{Q} \cup \{\infty\}$ be the order function such that $\mathrm{ord}_T(T) = 1$. Set $K_1 = \overline{K((T))}$. There exists an irreducible over K_1 factor $\widetilde{\chi}$, $\mathrm{lc}(\widetilde{\chi}) = 1$ of the characteristic polynomial of the element $(j \otimes_K K_1)(u + Tv)$ such that $\mathrm{ord}_T(a) > 0$ for every coefficient a of the polynomial $\chi - \widetilde{\chi}$. So if Δ is a nonzero minor (i.e. submatrix with nonzero determinant) of the maximal order of the matrix $\chi(u)$ then the corresponding minor $\widetilde{\Delta}$ of the matrix $\widetilde{\chi}(u + Tv)$ is also nonzero. Therefore, $d(u + Tv) \leq d(u)$. From here by specialization we get that $d(u + tv) \leq d(u)$ for all excepting of at most $P_1(n)$ elements $t \in K_i$ for some polynomial P_1 Similarly considering over series in $1/T$ we get that $d(u + tv) \leq d(v)$ for all excepting of at most $P_2(n)$ elements $t \in K_i$ for some polynomial P_2. The Lemma is proved.

Now let $K = \overline{k}$. Let $b'' = \sum_{1 \leq j \leq n_i} b''_j \lambda_{i,j} \in \Lambda'_i$, $b''_j \in k_i$. Using Lemma 2 replace successively the coefficients $b''_1, b''_2, \ldots$ by coefficients $a'_1, a'_2, \ldots \in H_0$ with $l(a'_j) < \mathcal{O}(\log n)$ such that for every $1 \leq s \leq n_i$ it is satisfied

$$d(\sum_{1 \leq j \leq s} a'_j \lambda_{i,j} + \sum_{s < j \leq n_i} b''_j \lambda_{i,j}) \leq d(b'').$$

Set $a' = \sum_{1 \leq j \leq n_i} a'_j \lambda_{i,j}$. Now return to the beginning of the procedure described where the element a was chosen. Replace a by a' and apply this procedure recursively. Hence, finally we shall construct an element a as above such that $d(a) = m_i$. Set $g = a$.

Thus, we have $d(g) = m_i d_i$ in all the considered cases. Replace a by g in our considerations above and conserve all other denotations. Choose an arbitrary element $0 \neq w \in W'(\chi)$ and construct the K_i–basis of the module $(\Lambda'_i \otimes_{k_i} K_i)w$. Show that $U'_i = (\Lambda'_i \otimes_{k_i} K_i)w$ is a simple $\Lambda'_i \otimes_{k_i} K_i$–module and $U'_i \otimes_{K_i} K$ is a simple Λ_i–module. Indeed, it is sufficient to prove the last statement. We have $\dim_{D_i} U_i(\chi) = 1$, i.e. $U_i(\chi)$ is one dimensional right vector space over D_i. Therefore, all nonzero elements of $U_i(\chi)$ have the same annulator $\mathfrak{m} \subset \Lambda_i$ and generate the simple module U_i. Hence, all nonzero elements of $W(\chi) = U_i(\chi)^{m_i}$ have the annulator $\mathfrak{m}$. Thus, $U'_i \otimes_{K_i} K \simeq \Lambda_i/\mathfrak{m} \simeq U_i$ and our assertion is proved. Additionally it is proved that U_i is defined over the field K_i.

Thus, we have constructed the module U_i in the case when $K = \overline{k}$. Consider the case when $K = \widetilde{k}$. If (ii) holds then Λ'_i is k'_i algebra and Λ_i is $k'_i \otimes_{k_i} K$–algebra and $k'_i \otimes_{k_i} K \simeq \overline{k}$. So applying the algorithm from the case when $K = \overline{k}$, see above, we shall construct the simple Λ_i–module U_i also when (ii) holds. If (i) or (iii) holds then set $\Lambda''_i = \Lambda'_i \otimes_{k_i} k_i[\sqrt{-1}]$. We have $K[\sqrt{-1}] = \overline{K}$, the $\overline{K}$–algebra $\Lambda''_i \otimes_{k_i[\sqrt{-1}]} \overline{K}$ is simple. Apply the algorithm from the case when $K = \overline{k}$, see above, replacing Λ'_i, k_i, ζ, χ, $W'(\chi)$ by Λ''_i, $k_i[\sqrt{-1}]$, ζ'', χ'', $W''(\chi'')$. So we shall construct a nonzero element $a \in \Lambda'_i \subset \Lambda''_i$ and corresponding linear polynomial χ'', $\mathrm{lc}(\chi'') = 1$, such that $\dim_{k_i[\sqrt{-1}][\zeta'']} W''(\chi'') = \sqrt{n_i}$. If $\zeta'' \in K$ then (i) holds, set $g = a$ and construct as it was above for the element g the simple module U_i. If $\zeta'' \notin K$ then denote by $\overline{\chi}''$ the conjugate over K polynomial to χ. Set $\chi = \chi''\overline{\chi}''$ and construct the field K_i generated by the coefficients of χ. Then χ is a polynomial

with coefficients from K and $\dim_{K_i} W'(\chi) = \dim_{k_i[\sqrt{-1}][\zeta'']}(W''(\chi'') + W''(\overline{\chi}'')) = 2\dim_{k_i[\sqrt{-1}][\zeta'']} W''(\chi'') = 2\sqrt{n_i}$. Therefore, $d(a) \leq 2\sqrt{n_i}$. Compute $d(a)$, see above. If $d(a) < 2\sqrt{n_i}$ then again (i) holds, set $g = a$ and construct as it was above for the element g the simple module U_i. If $d(a) = 2\sqrt{n_i}$ then apply to a the algorithm described for the case $K = \widetilde{k}$. Thus, we have finished the description of the algorithm for constructing the simple module U_i.

Compute the annulator $\mathfrak{m}' \subset \Lambda_i' \otimes_{k_i} K_i$ of the module U_i'.

Now let be given a Λ–module V, see Introduction. Our aim is to construct an isomorphism $\Lambda_i V \simeq U_i^{s_i}$ defined over the field K_i. First of all note that $\Lambda_i V \simeq ((\Lambda_i' \otimes_{k_i} K_i)(V' \otimes_k K_i)) \otimes_{K_i} K$ and therefore the module $\Lambda_i V$ is defined over K_i. Construct a K_i–basis of the $\Lambda_i' \otimes_{k_i} K_i$–module $V'' = (\Lambda_i' \otimes_{k_i} K_i)(V' \otimes_k K_i) \subset V' \otimes_k K_i$. Set $V''(\mathfrak{m}') = \{v \in V'' : \mathfrak{m}'v = \{0\}\}$ and compute a K_i–basis $f_1, \ldots, f_{s_i}$ of $V''(\mathfrak{m}')$. Then $\Lambda_i f_v \simeq U_i$ for every $1 \leq v \leq s_i$ and $V'' = \sum_{1 \leq v \leq s_i} (\Lambda_i' \otimes_{k_i} K_i) f_v$, $V = \sum_{1 \leq v \leq s_i} \Lambda_i f_j$. Compute the minimal set $I_i \subset \{1, \ldots, s_i\}$ such that $V'' = \sum_{v \in I_i} (\Lambda_i' \otimes_{k_i} K_i) f_v$. Then $\Lambda_i V = \oplus_{j \in I_i} \Lambda_i f_v$ is the required decomposition into the direct sum of simple modules.

For every ring A denote by A° the ring with the opposite multiplication, i.e. there exists an isomorphism of additive groups $A \to A^\circ$, $a \mapsto a^\circ$ such that $(ab)^\circ = b^\circ a^\circ$ for all $a, b \in A$. We can identify $(\mathrm{Hom}_{\Lambda_i}(U_i, U_i))^\circ = D_i$. Construct the algebra $(\mathrm{Hom}_{\Lambda_i'}(U_i', U_i'))^\circ = D_i'$. So D_i' is a division algebra over K_i and $D_i' \otimes_{K_i} K \simeq D_i$.

In the case when K is a real field the vectors f_v, $v \in I_i$ can be chosen more canonically. Namely, let $d = d_i = \dim_K D_i$. Note that $V''(\mathfrak{m}')$ is a right vector space over D_i. Construct an orthonormal K_i–basis $f_1, \ldots, f_{s_i}$ of $V''(\mathfrak{m}')$ such that $f_{jd+1}, f_{jd+2}, \ldots, f_{(j+1)d}$ is a basis of $f_{jd+1} D_i'$ for every $0 \leq j < s_i/d$. The required set $I_i = \{1, d+1, 2d+1, \ldots, (s_i/d-1)+1\}$. We shall suppose later that the vectors f_v, $v \in I_i$ are chosen in such a way when K is a real field.

We shall suppose further without loss of generality that if $V = \Lambda$ then $f_1 = w$ and $1 \in I_i$, i.e. f_1 is a generator of U_i. Further, the idempotent $e_i = \sum_{j \in I_i} e_{i,v}$ where idempotents $e_{i,v} \in \Lambda_i f_v$. Hence $e_{i,v} \in \Lambda_i' \otimes_{k_i} K_i$ for all v. Denote $e^{(i)} = e_{i,1} \in U_i$. So $U_i = \Lambda e^{(i)}$. Denote by $\gamma_{i,v} : U_i \to \Lambda_i f_v$, the constructed isomorphism which is given by the formula $\lambda f_1 \mapsto \lambda f_v$ for $\lambda \in \Lambda$. Set $e_v^{(i)} = \gamma_{i,v}(e^{(i)})$ for all $v \in I_i$, $i \in I$. So $e_v^{(i)} \in \Lambda_i f_v$ is an idempotent which has the same annulator as $e^{(i)}$, $v \in I_i$, $i \in I$.

REMARK 5. Suppose that $V = \Lambda$ then if $K = \overline{k}$, $i, j \in I$ and $\sigma : k_i \to K$ is an embedding over k such that $i^\sigma = j$ then, see Remark 2, it follows from Remark 4 and the described algorithm that there exists an embedding $\sigma_1 : K_i \to K$ over k which extends σ such that $e_{i,v}^{\sigma_1} = e_{j,v}$ and $\gamma_{i,v}^{\sigma_1} = \gamma_{j,v}$ (in the sense that $\gamma_{i,v}(x)^{\sigma_1} = \gamma_{j,v}(x^{\sigma_1})$ for all $x \in U_i'$) for all v. In particular $(e^{(i)})^{\sigma_1} = e^{(j)}$

Show that the natural projection $V \to \Lambda_i V$ is defined over the field K_i. Indeed, the module $\sum_{j \in I, j \neq i} \Lambda_j$ is defined over the field k_i as it was proved above. Hence, the module $(\sum_{j \in I, j \neq i} \Lambda_j) V \simeq \sum_{j \in I, j \neq i} \Lambda_j V$ is defined over the field K_i. The required assertion follows from here immediately.

Note also that one can construct within the polynomial time the isomorphism $\Lambda_i \simeq M_{m_i}(D_i)$. Indeed, we can identify $(\mathrm{Hom}_{\Lambda_i}(U_i, U_i))^\circ = D_i$ and therefore,

$$\Lambda_i \simeq (\mathrm{Hom}_{\Lambda_i}(\Lambda_i, \Lambda_i))^\circ \simeq (\mathrm{Hom}_{\Lambda_i}(U_i^{m_i}, U_i^{m_i}))^\circ \simeq$$
$$(M_{m_i}(\mathrm{Hom}_{\Lambda_i}(U_i, U_i)))^\circ \simeq M_{m_i}((\mathrm{Hom}_{\Lambda_i}(U_i, U_i))^\circ) = M_{m_i}(D_i).$$

The fourth isomorphism in this sequence is induced by transposition of matrices. These natural isomorphisms are defined over the field K_i. Therefore, they can be constructed within the polynomial time.

2 Algorithms for projective modules over algebras

Our aim is to prove Theorem 3 and construct an algorithm for decomposition of projective modules into the direct sum of indecomposable.

Let Λ and Λ' be as in the Introduction. Compute, see [?], [?] the radical $\mathfrak{R}' = \mathfrak{R}(\Lambda')$ of the algebra Λ'. Then the algebra $\Lambda'/\mathfrak{R}(\Lambda')$ is semisimple and hence, the algebra $\Lambda/(\mathfrak{R}' \otimes_k K) \simeq (\Lambda'/\mathfrak{R}') \otimes_k K$ is also semisimple, see e.g. [?]. Denote by $\mathfrak{R} = \mathfrak{R}(\Lambda)$ the radical of the algebra Λ. Then $\mathfrak{R} = \mathfrak{R}' \otimes_k K$ under our identifications of tensor products with subspaces of Λ, see Section 1.

Compute the semisimple algebra $\overline{\Lambda}' = \Lambda'/\mathfrak{R}'$ i.e. compute a k–basis of this algebra with its multiplication table, c.f. Introduction. This basis is simultaneously a basis of K–algebra $\overline{\Lambda} = \Lambda/\mathfrak{R}$ under our identifications. Denote by $\pi : \Lambda \to \lambda/\mathfrak{R}$ the natural projection.

Apply the algorithm from Section 1 to the semisimple algebra $\overline{\Lambda}'$ and construct the decomposition

$$\overline{\Lambda} = \oplus_{i \in I} \overline{\Lambda}_i \tag{5}$$

similar to (1) where the simple algebra $\overline{\Lambda}_i$ is defined over the field k_i, see Section 1. Further, construct an isomorphism

$$\overline{\Lambda}_i \simeq \oplus_{i \in I} U_i^{m_i}. \tag{6}$$

similar to (2) with V replaced by $\overline{\Lambda}_i$. So U_i is a simple $\overline{\Lambda}_i$–module defined over a field K_i, see Section 1. Denote $\overline{P}_i = U_i$ for every $i \in I$.

According to the construction from Section 1 the module $\overline{R}_i = \sum_{j \in I,\, j \neq i} \overline{\Lambda}_j \oplus U_i^{\varepsilon_i - 1}$ is defined over the field K_i and $\overline{P}_i \oplus \overline{R}_i \simeq \overline{\Lambda}$. The module $\overline{R}_i$ defined by its K_i–structure and the isomorphism $\overline{P}_i \oplus \overline{R}_i \simeq \overline{\Lambda}$ can be constructed within the polynomial time, see Section 1. Further we shall suppose without loss of generality that $\overline{P}_i \oplus \overline{R}_i = \overline{\Lambda}$, i.e. that $\overline{P}_i$ and $\overline{R}_i$ are submodules of Λ defined over K_i.

We need an auxiliary algorithm. In input of this algorithm a finite extension L of the field k, an idempotent $q \in \Lambda' \otimes_k L$, idempotents $\overline{q}_i \in \overline{\Lambda}' \otimes_k L$, $1 \leq i \leq r$ are given such that $\overline{q}_{i_1} \overline{q}_{i_2} = 0$ for any different $1 \leq i_1 \neq i_2 \leq r$ and $\overline{q} = q \mod \mathfrak{R} = \sum_{1 \leq i \leq r} \overline{q}_i$. Hence, see [?], $W = \Lambda q$ is projective ideal of Λ defined over L, the modules $\overline{Q}_i = \overline{\Lambda} \overline{q}_i$

are projective ideals of $\overline{\Lambda}$, $1 \leq i \leq r$, and we have the decomposition $W/\mathfrak{R}W = \oplus_{1 \leq i \leq r} \overline{Q}_i$ of the module $\overline{W} = W/\mathfrak{R}W$ into the direct sum of its submodules $\overline{Q_i}$, $1 \leq i \leq r$.

In output of this algorithm we get idempotents $q_i \in \Lambda' \otimes_k L$, $1 \leq i \leq r$ such that $q_{i_1} q_{i_2} = 0$ for any different $1 \leq i_1 \neq i_2 \leq r$, $q = \sum_{1 \leq i \leq r} q_i$ and $q_i \bmod \mathfrak{R} = \overline{q}_i$ for all $1 \leq i \leq r$. Hence, the modules $Q_i = \Lambda q_i$ are projective ideals of Λ, $1 \leq i \leq r$, and we have the decomposition $W = \oplus_{1 \leq i \leq r} Q_i$ of the module W into the direct sum of its submodules Q_i such that such that $\pi(Q_i) = Q_i/\mathfrak{R}Q_i = \overline{Q}_i$, $1 \leq i \leq r$.

The working time of this algorithm is polynomial in the size of input.

To describe this algorithm prove the following lemma.

LEMMA 3. Let $\mathfrak{r}_2 \subset \mathfrak{r}_1 \subset \mathfrak{R}$ be ideals of Λ and $\pi_1 : \Lambda/\mathfrak{r}_1 \to \overline{\Lambda}$, $\pi_{1,2} : \Lambda/\mathfrak{r}_2 \to \Lambda/\mathfrak{r}_1$ be natural projections. Let $\oplus_{1 \leq i \leq r} Q_{1,i} = W/\mathfrak{r}_1 W$ where $Q_{1,i}$ are submodules of $W/\mathfrak{r}_1 W$ defined over the field L and $\pi_1(Q_{1,i}) = \overline{Q}_i$ for $1 \leq i \leq r$.. Then there exist submodules $Q_{2,i}$ of $W/\mathfrak{r}_2 W$ defined over the field L such that $\oplus_{1 \leq i \leq r} Q_{2,i} = W/\mathfrak{r}_2 W$ and $\pi_{1,2}(Q_{2,i}) = Q_{1,i}$ for all $1 \leq i \leq r$.

PROOF. We shall suppose without loss of generality that $\mathfrak{r}_2 = \{0\}$. There exists, see e.g. [?], projective modules Q_i defined over L (i.e. their L–structures are projective modules) such that $Q_i/\mathfrak{R}Q_i \simeq \overline{Q}_i$ over L.

Show that there exists an isomorphism $W \to \oplus_{1 \leq i \leq r} Q_i$ defined over L. Indeed, since W and $\oplus_{1 \leq i \leq r} Q_i$ are projective modules defined over L and $\oplus_{1 \leq i \leq r} \overline{Q}_i = \overline{W}$ there exist homomorphisms $\alpha : W \to \oplus_{1 \leq i \leq r} Q_i$ and $\beta : \oplus_{1 \leq i \leq r} Q_i \to W$ defined over L such that $\alpha \circ \beta = 1 - \sigma_1$ and $\beta \circ \alpha = 1 - \sigma_2$ where 1 denotes here the identity isomorphisms of $\oplus_{1 \leq i \leq r} Q_i$ and W respectively, the images $\mathrm{Im}\sigma_1 \subset \mathfrak{R}(\oplus_{1 \leq i \leq r} Q_i)$, $\mathrm{Im}\sigma_2 \subset \mathfrak{R}W$. Therefore, σ_1 and σ_2 are nilpotent endomorphisms of $\oplus_{1 \leq i \leq r} Q_i$ and Λ respectively. Therefore, $\alpha \circ \beta$ and $\beta \circ \alpha$ are isomorphisms. Hence, the kernels $\mathrm{Ker}\alpha = \mathrm{Ker}\beta = \{0\}$ and the images $\mathrm{Im}\alpha = \oplus_{1 \leq i \leq r} Q_i$, $\mathrm{Im}\beta = W$. The required assertion is proved.

We shall suppose further without loss of generality that Q_i are submodules of Λ defined over L. We shall identify $W/\mathfrak{r}_1 W = \oplus_{1 \leq i \leq r} Q_i/\mathfrak{r}_1 Q_i$. Note that $Q_i/\mathfrak{r}_1 Q_i \simeq Q_{1,i}$ since these modules are projective $\Lambda/\mathfrak{r}_1$–modules and the reductions modulo $\mathfrak{R}/\mathfrak{r}_1$ of these modules coincide. Hence, there exists an isomorphism $\gamma_1 : \Lambda/\mathfrak{r}_1 \to \Lambda/\mathfrak{r}_1$ induced by the considered isomorphisms $Q_i/\mathfrak{r}_1 Q_i \simeq Q_{1,i}$, $1 \leq i \leq r$. There exists a homomorphism of modules $\gamma : W \to W$ such that $\gamma_1 \circ \pi_{1,2} = \pi_{1,2} \circ \gamma$. Analogously to that it was above for the homomorphism α it is proved that γ is an isomorphism. Now set $Q_{2,i} = \gamma(Q_i)$ for all $1 \leq i \leq r$. The lemma is proved.

Now let $1 \leq j \in \mathbb{Z}$. Consider the natural projection $\pi_j : \Lambda/\mathfrak{R}^j \to \overline{\Lambda}$. Let $1 \leq j_0 \in \mathbb{Z}$ be maximal such that $\mathfrak{R}^{j_0 - 1} \neq \{0\}$. Our aim is to construct consequently for $j = 1, 2, \ldots, j_0$ submodules $Q_{i,j} \subset W/\mathfrak{R}^j W$ defined over the field L such that $\oplus_{1 \leq i \leq r} Q_{i,j} = \Lambda/\mathfrak{R}^j$ and $\pi_j(Q_{i,j}) = \overline{Q}_i$, $1 \leq i \leq r$. Let $q \bmod \mathfrak{R}^j = \sum_{1 \leq i \leq r} q_{i,j} \in \Lambda/\mathfrak{R}^j$ where $q_{i,j} \in Q_{i,j}$, $1 \leq i \leq r$. Then $(\Lambda/\mathfrak{R}^j) q_{i,j} = Q_{i,j}$ and $q_{i,j} \in \Lambda/\mathfrak{R}^j$

are idempotents such that $q_{i_1,j}q_{i_2,j} = 0$ for any different $1 \le i_1 \ne i_2 \le r$, see [?]. Conversely, if $q_{i,j} \in \Lambda/\mathfrak{R}^j$ are idempotents such that $q \bmod \mathfrak{R}^j = \sum_{1\le i\le r} q_{i,j}$, $q_{i_1,j}q_{i_2,j} = 0$ for any different $1 \le i_1 \ne i_2 \le r$ and $\pi_j(q_{i,j}) = q_{i,1}$ then we can set $(\Lambda/\mathfrak{R}^j)q_{i,j} = Q_{i,j}$ for all $1 \le i \le r$. So it is sufficient to construct idempotents $q_{i,j} \in \Lambda/\mathfrak{R}^j$ such that $q \bmod \mathfrak{R}^j = \sum_{1\le i\le r} q_{i,j}$, $q_{i_1,j}q_{i_2,j} = 0$ for any different $1 \le i_1 \ne i_2 \le r$ and $\pi_j(q_{i,j}) = q_1$ for all $1 \le i \le r$.

Construct for $j = 1, 2, \ldots$ the factor algebras $\Lambda/\mathfrak{R}^j$ and compute j_0. Note that $Q_{i,1} = \overline{Q}_i$. Hence, construct $q_{i,1}$ for all $1 \le i \le r$. We shall construct for every $0 \le j < j_0$, $1 \le i \le r$ elements $\varepsilon_{i,j} \in \mathfrak{R}^j$ (one have $\mathfrak{R}^0 = \Lambda$) such that $q_{i,j} = \sum_{0\le s<j} \varepsilon_{i,s} \bmod \mathfrak{R}^j$ for every $1 \le j \le j_0$, $1 \le i \le r$. Solving a linear system over the field L construct elements $\varepsilon_{i,0} \in \Lambda$ such that $q_{i,1} = \varepsilon_{i,0} \bmod \mathfrak{R}$. Now suppose that $q_{i,j-1}$ and all $\varepsilon_{i,s}$, $0 \le s < j-1$, $1 \le i \le r$ are constructed for some $1 < j \le j_0$ and show how to construct $q_{i,j}$ and $\varepsilon_{i,j-1}$.

By Lemma 3 applied to $\mathfrak{r}_1 = \mathfrak{R}^{j-1}$, $\mathfrak{r}_2 = \mathfrak{R}^j$ and by the described above connection between idempotents and projective modules there exist $u_i \in \mathfrak{R}^{j-1}$, $1 \le i \le r$ such that

$$
\begin{aligned}
(\sum_{0\le s<j-1} \varepsilon_{i_1,s} + u_{i_1})(\sum_{0\le s<j-1} \varepsilon_{i_2,s} + u_{i_2}) \in \mathfrak{R}^j, \quad & 1 \le i_1 \ne i_2 \le r,\\
(\sum_{0\le s<j-1} \varepsilon_{i,s} + u_i)^2 - \sum_{0\le s<j-1} \varepsilon_{i,s} - u_i \in \mathfrak{R}^j, \quad & 1 \le i \le r,\\
\sum_{1\le i\le r} (\sum_{0\le s<j-1} \varepsilon_{i,s} + u_i) - q \in \mathfrak{R}^j. &
\end{aligned}
$$

Hence, equivalently

$$
\begin{aligned}
\varepsilon_{i_1,0}u_{i_2} + u_{i_1}\varepsilon_{i_2,0} = - \sum_{0\le s_1,s_2<j-1, s_1+s_2\le j-1} \varepsilon_{i_1,s_1}\varepsilon_{i_2,s_2} \bmod \mathfrak{R}^j,\\
1 \le i_1 \ne i_2 \le r;\\
\varepsilon_{i,0}u_i + u_i\varepsilon_{i,0} - u_i = - \sum_{0\le s_1,s_2<j-1, s_1+s_2\le j-1} \varepsilon_{i,s_1}\varepsilon_{i,s_2} + \sum_{0\le s<j-1} \varepsilon_{i,s} \bmod \mathfrak{R}^j,\\
1 \le i \le r;\\
\sum_{1\le i\le r} u_i = q - \sum_{1\le i\le r} \sum_{0\le s<j-1} \varepsilon_{i,s} \bmod \mathfrak{R}^j
\end{aligned}
$$

in $\Lambda/\mathfrak{R}^j$. Solving a linear system over the field L compute some elements $u_i \bmod \mathfrak{R}^j$, $1 \le i \le r$. Solving a linear system over the field L compute the required elements $\varepsilon_{i,j-1} \in \mathfrak{R}^{j-1}$ by the condition $u_i = \varepsilon_{i,j-1} \bmod \mathfrak{R}^j$, $1 \le i \le r$. It follows immediately by induction from the construction described that the size $L(\varepsilon_{i,j}) < (j-1)\mathcal{P}_1(M_1d_1n) + \mathcal{P}_2(M_1d_1n)$ for all i, j for some polynomials $\mathcal{P}_1, \mathcal{P}_2$. Therefore, all $\varepsilon_{i,j}$ and $q_{i,j}$ can be constructed within the polynomial time.

Now construct the required modules $Q_i = \Lambda q_{i,j_0}$ defined by their L–structures. The auxiliary algorithm is described.

Now apply the auxiliary algorithm to the decomposition $\overline{P}_i \oplus \overline{R}_i = \overline{\Lambda}$, $i \in I$ where $\overline{P}_i$ and $\overline{R}_i$ are submodules of Λ defined over K_i, see above. So construct the

decomposition $P_i \oplus R_i = \Lambda$ where P_i and Q_i are projective ideals of Λ defined over the field K_i such that $\pi(P_i) = P_i/\mathfrak{R}P_i = \overline{P}_i$ and $\pi(R_i) = R_i/\mathfrak{R}R_i = \overline{R}_i$ for all $i \in I$ and an idempotent $e^{(i)} \in \Lambda' \otimes_K K_i$ such that $P_i = \Lambda e^{(i)}$, $R_i = \Lambda(1 - e^{(i)})$. The K_i–structure of P_i is $P_i' == \Lambda' e^{(i)}$.

REMARK 6. We shall suppose that by solving linear systems in the described construction we take conjugated solutions for systems with conjugated coefficients. Therefore, if $K = \overline{k}$, the dices $i, j \in I$, an embedding $\sigma : k_i \to K$ over k , an embedding $\sigma_1 : K_i \to K$ over k are such that (see Remark 5) $i^\sigma = j$ and σ_1 extends σ then $\left(e^{(i)}\right)^{\sigma_1} = e^{(j)}$.

Now let V be an arbitrary Λ–module from Introduction defined by its k–structure V'. Our aim is to decide whether V is a projective Λ–module and if it is the fact to construct an isomorphism

$$V \simeq \oplus P_i^{\varepsilon_i}.$$

Construct the epimorphism $\pi_V : \Lambda^m \to V$ defined over the field k. This is possible since the generators $\{v_j\}_{1 \le j \le m}$ of V' are known, see Introduction. Solving a linear system construct a basis over k of the space of homomorphisms

$$\mathrm{Hom}_{\Lambda'}(V', V') = \{\tau \in \mathrm{Hom}_k(V', V') \ : \ \tau(\lambda_i v_j) = \lambda_i \tau(v_j) \forall 1 \le i \le n,\ 1 \le j \le m\}.$$

Hence, the space of homomorphisms $\mathrm{Hom}_\Lambda(V, V) = \mathrm{Hom}_{\Lambda'}(V', V') \otimes_k K$. Similarly construct a basis over k of the space of homomorphisms $\mathrm{Hom}_{\Lambda'}(V', (\Lambda')^m)$. Hence $\mathrm{Hom}_\Lambda(V, \Lambda^m) = \mathrm{Hom}_{\Lambda'}(V', (\Lambda')^m) \otimes_k K$. Therefore, $\mathrm{Hom}_\Lambda(V, V)$, and $\mathrm{Hom}_\Lambda(V, \Lambda^m)$ are defined over k. Further construct the homomorphism defined over k

$$\pi_{V*} : \mathrm{Hom}_\Lambda(V, \Lambda^m) \to \mathrm{Hom}_\Lambda(V, V)$$

induced by π_V.

Now V is projective if and only if the identity isomorphism 1_V of V belongs to $\mathrm{Im}\,\pi_{V*}$. Solving a linear system over k we can decide whether $1_V \in \mathrm{Im}\,\pi_{V*}$ and if it is the fact construct an element $\sigma \in \pi_{V*}^{-1}(1_V)$. Thus we can decide within the polynomial time whether V is projective.

Let V be a projective module. Using Section 1 construct the isomorphism $\overline{\gamma} : V/\mathfrak{R}V \simeq \oplus_{i \in I} \overline{P}_i^{\varepsilon_i}$ and the natural projections $\overline{\gamma}_i : V/\mathfrak{R}V \to \overline{P}_i^{\varepsilon_i}$ defined over the field K_i, see Section 1. Consider the natural homomorphism defined over the field K_i

$$\rho : \mathrm{Hom}_\Lambda(V, P_i^{\varepsilon_i}) \to \mathrm{Hom}_\Lambda(V/\mathfrak{R}V, \overline{P}_i^{\varepsilon_i}).$$

Since V is a projective module there exists a homomorphism $\gamma_i : V \to P_i^{\varepsilon_i}$ such that $\gamma_i \bmod \mathfrak{R} = \overline{\gamma}_i$, i.e. $\gamma_i \in \rho^{-1}(\overline{\gamma}_i)$. Solving linear systems over the fields K_i construct homomorphisms γ_i for all $i \in I$.

We claim that the homomorphisms γ_i, $i \in I$ define the isomorphism $\gamma : V \to \oplus_{i \in I} P_i^{\varepsilon_i}$. Indeed, we have $\gamma \bmod \mathfrak{R} = \overline{\gamma}$. Now similarly to that it was in the proof

of Lemma 3 for the isomorphism of Λ and $P_i \oplus Q_i$ we get that γ is an isomorphism (defined over the composite of all fields K_i, $i \in I$).

Now let be given two projective modules V_1 and V_2 defined over the field k. Construct for them the isomorphisms $\gamma_j : V_j \simeq \oplus_{i \in I} P_i^{\varepsilon_{j,i}}$, $j = 1, 2$. The modules V_1 and V_2 are isomorphic over K if and only if $\varepsilon_{1,i} = \varepsilon_{2,i}$ for all $i \in I$ and if it is the case we have the isomorphism between them $\gamma_2^{-1} \circ \gamma_1$ defined over the composite of all fields K_i, $i \in I$. We shall show later in Section 5 how to obtain the isomorphism between these modules defined over the field k.

3 Decomposition of an algebra into the direct sum of projective ideals which is good with respect to the action of the Galois group.

Let Λ be as in previous Section and (5), (6) are satisfied and constructed.

We shall suppose that the set of indices I has the structure described in Section 1, i.e. that

$$I = \bigcup_{i \in I_1} H_i \text{ if } K = \overline{k}, \tag{7}$$

$$I = \bigcup_{i \in I_1} (H_i' \cup \bigcup_{j \in J_i} \Xi_j) \text{ if } K = \widetilde{k}, \tag{8}$$

and

$$I = \bigcup_{i \in I_1} E_i \tag{9}$$

where $E_i = H_i' \cup \cup_{j \in J_i} \Xi_j$ for every $i \in I_1$. Further, the sets H_u, $u \in I_1$ can be constructed within the polynomial time. Denote the central idempotents corresponding to the elements of $i \in H_u$ or $i \in I$ by $\overline{e}_i$ (in Section 1 they were denoted e_i). If $u \in I_1$ then the algebra $\overline{\Lambda}_u$ is constructed and defined by the central idempotent $\overline{e}_u = \sum_{i \in H_u} \overline{e}_i = \sum_{i \in E_u} \overline{e}_i$. The algebra $\overline{\Lambda}_u$ is defined over the field k for every $u \in I_1$. Denote the idempotents corresponding to the elements of $v \in I_i$, $i \in I$ by $\overline{e}_{i,v}$, $\overline{e}_v^{(i)}$ (in Section 1 they were denoted $e_{i,v}$, $e_v^{(i)}$) and the modules corresponding to $\Lambda_i f_v$ by $\overline{W}_{i,v}$. In particular denote by $\overline{e}^{(i)} = \overline{e}_{i,1}$ the idempotent defining the module $\overline{P}_i$. The isomorphisms $\overline{P}_i \to \overline{W}_{i,v}$ constructed in Section 1 denote by $\overline{\gamma}_{i,v}$ (in Section 1 they were denoted $\gamma_{i,v}$).

Note that now $\#I_i = \varepsilon_i$ and we shall suppose that $I_i = \{1, \ldots, \varepsilon_i\}$. We conserve other denotations from Section 1 and Section 2.

We have $\Lambda = \Lambda' \otimes_k K$ and $\Lambda \otimes_K \overline{K} = \Lambda' \otimes_k \overline{K}$. Hence, the Galois group $\mathrm{Gal}(K/k)$ acts in the natural way on Λ and the Galois group $\mathrm{Gal}(\overline{K}/k)$ acts on $\Lambda \otimes_K \overline{K}$. These actions are trivial on Λ'.

Now let A' be an L–structure of a submodule A (of Λ) defined over the field L which is an extension of k. Then every embedding $\sigma : L \to K$ over k is extended

uniquely till the embedding $A' \to \Lambda$ which we shall also denote without ambiguity by σ. This embedding $\sigma : A' \to \Lambda$ is such that $\sigma(a) = a^{\widetilde{\sigma}}$ for $a \in A'$ where $\widetilde{\sigma} \in \mathrm{Gal}(K/k)$ is an arbitrary element for which the restriction $\widetilde{\sigma}|_L = \sigma$. The embedding $\sigma : A' \to \Lambda$ does not depend on the choice of $\widetilde{\sigma}$ since A' is invariant relatively to the Galois group $\mathrm{Gal}(K/L)$.

In Section 2 the projective ideals P_i of an algebra Λ and an an isomorphism

$$\gamma : \Lambda \to \oplus_{i \in I} P_i^{\varepsilon_i} \tag{10}$$

(one should set here $V = \Lambda$) were constructed.

The aim of this section is to construct projective ideals $W_{i,v}$, $1 \le v \le \varepsilon_i, i \in I$ of Λ satisfying to the following properties. that

(i) $W_{i,v}$ is defined over the field K_i for all $1 \le v \le \varepsilon_i, i \in I$.

(ii) the isomorphisms $\gamma_{i,v} : P_i \to W_{i,v}$ defined over the field K_i are constructed for all $1 \le v \le \varepsilon_i, i \in I$.

(iii) $\Lambda = \sum_{1 \le v \le \varepsilon_i, i \in I} W_{i,v}$ as a sum of submodules of Λ (it follows from (10) by comparison of dimensions over K that this sum is a direct sum of submodules).

(iv) Let $1 = \sum_{1 \le v \le \varepsilon_i, i \in I} e_{i,v} \in \Lambda$, where $e_{i,v} \in W_{i,v}$. Denote also $\sum_{1 \le v \le \varepsilon_i} e_{i,v} = e_i$ for every $i \in I$ and $\sum_{i \in E_u} e_i = e_u$ for every $u \in I_1$. Then

  (a) $e_{i,v} \in \Lambda' \otimes_k K_i$ and $e_{i,v} \bmod \mathfrak{R} = \overline{e}_{i,v}$ for all $1 \le v \le \varepsilon_i, i \in I$, hence $W_{i,v}/W_{i,v} \cap \mathfrak{R} = \overline{W}_{i,v}$;

  (b) if $K = \overline{k}$, the indices $i, j \in I$, an embedding $\sigma : k_i \to K$ over k , an embedding $\sigma_1 : K_i \to K$ over k are such that (see Remark 5) $i^\sigma = j$, $\overline{e}_{i,v}^{\sigma_1} = \overline{e}_{j,v}$ for all v and σ_1 extends σ then $e_{i,v}^{\sigma_1} = e_{j,v}$ for all $1 \le v \le \varepsilon_i$, and $\gamma_{i,v}^{\sigma_1} = \gamma_{j,v}$, i.e. $\gamma_{j,v}(x^{\sigma_1}) = \gamma_{i,v}(x)^{\sigma_1}$ for every $x \in P_i'$;

  (c) $e_i \in \Lambda' \otimes_k k_i$ and $e_i \bmod \mathfrak{R} = \overline{e}_i$ for every $i \in I$, therefore the ideal $W_i = \sum_{1 \le v \le \varepsilon_i} W_{i,v} = \Lambda e_i$ is defined over the field k_i and $W_i/W_i \cap \mathfrak{R} = \overline{\Lambda}_i$

  (d) if $i, j \in I$ and an embedding $\sigma : k_i \to K$ of fields over k are such that $j = i^\sigma$, see Remark 2, then $e_j = e_i^\sigma$;

  (e) $e_u \in \Lambda'$ and $e_u \bmod \mathfrak{R} = \overline{e}_u$ for every $u \in I_i$, therefore the ideal $W_u = \sum_{i \in E_u} W_i = \Lambda e_u$ is defined over the field k, and $W_u/W_u \cap \mathfrak{R} = \overline{\Lambda}_u$.

To effect this construction at first apply the auxiliary algorithm to the decomposition $\overline{\Lambda} = \oplus_{u \in I_1} \overline{\Lambda}_u$, i.e. to the idempotents $1 \in \Lambda$ and $\overline{e}_u \in \overline{\Lambda}$ $u \in I_1$, and construct all the required in (e) ideals W_u defined over k and idempotents $e_u \in \Lambda'$ such that $W_u = \Lambda e_u$ and $e_u \bmod \mathfrak{R} = \overline{e}_u$ for all $u \in I_1$.

Consider at first the case when $K = \overline{k}$.

Now for every $u \in I_1$ and a fixed index $i_0 \in H_u$ denote $\overline{q}_{i_0} = \sum_{i \in H_u, i \ne i_0} \overline{e}_i \in \overline{\Lambda}$, $\overline{S}_{i_0} = \oplus_{i \in H_u, i \ne i_0} \overline{\Lambda}_i = \overline{\Lambda} q_{i_0}$. Hence, the idempotents $\overline{e}_{i_0}, \overline{q}_{i_0} \in \overline{\Lambda}' \otimes_k k_{i_0}$ and the

modules $\overline{\Lambda}_{i_0}$, $\overline{S}_{i_0}$ are defined over the field k_{i_0}. Apply the auxiliary algorithm to to the module W_u and the decomposition $\overline{\Lambda}_u = \overline{\Lambda}_{i_0} \oplus \overline{S}_{i_0}$, i.e. to the idempotents $e_u \in \Lambda$, $\overline{e}_{i_0}, \overline{q}_{i_0} \in \overline{\Lambda}' \otimes_k k_{i_0}$ and construct the idempotents $\widetilde{e}_{i_0}, q_{i_0} \in \Lambda$ such that $e_u = \widetilde{e}_{i_0} + q_{i_0}$, $\overline{e}_{i_0} = \widetilde{e}_{i_0} \bmod \mathfrak{R}$, $\overline{q}_{i_0} = q_{i_0} \bmod \mathfrak{R}$.

Set $\widetilde{W}_{i_0} = W_u\widetilde{e}_{i_0} = \Lambda\widetilde{e}_{i_0}$. $S_{i_0} = W_u q_{i_0} = \Lambda q_{i_0}$. So we get the decomposition $W_u = \widetilde{W}_{i_0} \oplus S_{i_0}$ where $\widetilde{W}_{i_0}$ and S_{i_0} are defined over the field k_{i_0}.

Set $\widetilde{e}_i = \widetilde{e}_{i_0}^{\sigma}$, $q_i = q_{i_0}^{\sigma}$ and $\widetilde{W}_i = W_u\widetilde{e}_i = \Lambda\widetilde{e}_i$. $S_{i_0} = W_u q_{i_0} = \Lambda q_{i_0}$ for every $i \in H_u$ and an embedding $\sigma : k_{i_0} \to K$ of fields over k such that $i = i_0^{\sigma}$. So we have the isomorphism $W_u = \widetilde{W}_i \oplus S_i$ and natural projections $\widetilde{\pi}_i : W_u \to \widetilde{W}_i$ and $\pi_i' : W_u \to S_i$ defined over the field k_i for every $i \in H_u$, $u \in I_1$.

We can not claim now that the sum of projective ideals $\sum_{i\in H_u} \widetilde{W}_i$ is a direct sum. But still similarly to that it was for the isomorphism γ there exists an isomorphism

$$\gamma_u : W_u \to \oplus_{i\in H_u} \widetilde{W}_i \tag{11}$$

which is induced by the natural projections $W_u \to \widetilde{W}_i$, $i \in H_u$ (the direct sum here is an external abstract direct sum).

Now our aim is to construct using (11) the required in (c) ideals W_i satisfying to (d). Define the action of the Galois group $\mathrm{Gal}(\overline{K}/k)$ on the module $\oplus_{i\in H_u}\widetilde{W}_i$ in the following way if $(\lambda_i)_{i\in H_u} \in \oplus_{i\in H_u}\widetilde{W}_i$ and $\tau \in \mathrm{Gal}(\overline{K}/k)$ then set

$$(\lambda_i)_{i\in H_u}^{\tau} = (\lambda_{i^{\tau^{-1}}}^{\tau})_{i\in H_u}.$$

Thus γ_u is invariant relative to the action of the Galois group $\mathrm{Gal}(\overline{K}/k)$, i.e. $\gamma(\lambda^{\tau}) = \gamma(\lambda)^{\tau}$ for any $\lambda \in W_u$ and $\tau \in \mathrm{Gal}(\overline{K}/k)$.

Consider the natural projection

$$\pi_i : W_u \to \oplus_{j\in H_u, j\neq i}\widetilde{W}_j.$$

Set $\mathrm{Ker}\pi_i = W_i$. Then $W_i^{\tau} = W_i$ for every $\tau \in \mathrm{Gal}(\overline{K}/k_i)$. Therefore, W_i is defined over the field k_i for every $i \in H_u$. Besides that, $W_i/W_i \cap \mathfrak{R} = \overline{\Lambda}_i$. Further, $\sum_{i\in H_u} W_i = W_u$ and this sum of submodules is a direct sum since γ_u is an isomorphism. Note that $\sum_{j\in H_u, j\neq i} W_j = S_i = \mathrm{Ker}\widetilde{\pi}_i$ for every $i \in H_u$. So we have $W_u = W_i \oplus S_i$ as a direct sum of submodules.

Denote by W_i' (respectively S_i') the k_i–structure of W_i (respectively S_i) and by W_u' the k–structure of W_u for every $i \in H_u$. Then we have

$$W_i' = (\bigcap_{j\in H_u, j\neq i} \mathrm{Ker}\widetilde{\pi}_j) \cap (W_u' \otimes_k k_i) =$$
$$\bigcap_{j\in H_u, j\neq i} ((S_j \otimes_{k_j} k[i,j]) \cap (W_u' \otimes_k k_i))$$

Here $k[i,j]$ is a composite of the fields $k_i = k[i]$ and $k_j = k[j]$ over k and $S_j \otimes_{k_j} k[i,j]$, $W_u' \otimes_k k_i$ are subspaces of $W_u' \otimes_k k[i,j]$ considered as vector space over k. Thus, compute all the different non–isomorphic over k_i composites $k[i,j]$ of the fields

$k_i = k[i]$ and $k_j = k[j]$ over k and all the different subspaces $(S_j \otimes_{k_j} k[i,j]) \cap (W'_u \otimes_k k_i) \subset W'_u \otimes_k k_i$. Finally computing their intersection obtain the required W'_i for all $i \in H_u$, $u \in I_1$.

Compute the idempotents $e_i \in W_i$ and $e'_i \in S_i$ from the condition $e_i + e'_i = e_u$ for all $i \in H_u$, $u \in I_1$.

Thus, we have by the construction described $e_i \in \Lambda' \otimes_k k_i$ and $e_i \bmod \mathfrak{R} = \overline{e}_i$ for every $i \in I$, the ideal $W_i = \Lambda e_i$ is defined over the field k_i and $W_i / W_i \cap \mathfrak{R} = \overline{\Lambda}_i$. Further, if $i, j \in I$ and an embedding $\sigma : k_i \to K$ of fields over k are such that $j = i^\sigma$, then $e_j = e_i^\sigma$ for all $i \in H_u$, $u \in I_1$. Hence, W_i and e_i satisfy to (c) and (d) for all $i \in H_u$, $u \in I_1$. Besides that, $\sum_{i \in H_u} e_i = e_u$ for all $u \in I_1$.

So for every $u \in I_1$ fix an index $i \in H_u$ and apply the auxiliary algorithm to the idempotents $e_i \in \Lambda$, $\overline{e}_i, \overline{e}_{i,v}$, $1 \le v \le \varepsilon_i$ which define the decomposition

$$\overline{\Lambda}_i = \oplus_{1 \le v \le \varepsilon_i} \overline{W}_{i,v}.$$

Thus, construct the idempotents $e_{i,v} \in \Lambda' \otimes_k K_i$ such that $\sum_{1 \le v \le \varepsilon_i} e_{i,v} = e_i$ and $e_{i,v} = \overline{e}_{i,v} \bmod \mathfrak{R}$ for all $1 \le v \le \varepsilon_i$. Set $W_{i,v} = W_i e_{i,v} = \Lambda e_{i,v}$ for all $1 \le v \le \varepsilon_i$. So we obtain the decomposition

$$W_i = \oplus_{1 \le v \le \varepsilon_i} W_{i,v}$$

where all $W_{i,v}$ are defined over the field K_i.

Similarly to how it was for the isomorphism γ in Section 2 construct the required isomorphisms $\gamma_{i,v}$ from the condition that $\gamma_{i,v} \bmod \mathfrak{R} = \overline{\gamma}_{i,v}$.

If $j \in I$, an embedding $\sigma : k_i \to K$ over k , an embedding $\sigma_1 : K_i \to K$ over k are such that $i^\sigma = j$, $\overline{e}_{i,v}^{\sigma_1} = \overline{e}_{j,v}$ for all v and σ_1 extends σ then set $e_{i,v}^{\sigma_1} = e_{j,v}$, $\gamma_{i,v}^{\sigma_1} = \gamma_{j,v}$ for all $1 \le v \le \varepsilon_i$.

Thus (a), (b), (c), (d) and (e) are satisfied. Hence, (i), (ii), (iii), (iv) are satisfied. The construction for the case $K = \overline{k}$ is completed.

Now consider the case when $K = \widetilde{k}$. Apply the algorithm for the case $K = \overline{k}$ to the algebra $\Lambda \otimes_K \overline{K}$ and the corresponding idempotents $\overline{e}_u$, $\overline{e}_i$, $u \in I_1$, $i \in H_u$. So we get the idempotents e_u, e_i, $u \in I_1$, $i \in H_u$. Now for every $j \in J_u$, $u \in I_1$ set $e_j = e_{i_1} + e_{i_2}$ if and only if $j = i_1 + i_2 + z i_1 i_2$ for $i_1, i_2 \in H_u$, see (8) and Section 1. The idempotent $e_j \in \Lambda' \otimes_k k[i_1, i_2]$ and it is invariant relatively to the action of the Galois group $\mathrm{Gal}(k[i_1, i_2]/k_j)$. Hence, $e_j \in \Lambda' \otimes_k k_j$. Define $W_u = \Lambda e_u$, $W_i = \Lambda e_i$, for all $i \in E_u$, $u \in I_1$.

Now for every $i \in E_u$, $u \in I_1$ apply the auxiliary algorithm to the idempotents $e_i \in \Lambda$, $\overline{e}_i, \overline{e}_{i,v}$, $1 \le v \le \varepsilon_i$ which define the decomposition

$$\overline{\Lambda}_i = \oplus_{1 \le v \le \varepsilon_i} \overline{W}_{i,v}.$$

Thus, construct the idempotents $e_{i,v} \in \Lambda' \otimes_k K_i$ such that $\sum_{1 \le v \le \varepsilon_i} e_{i,v} = e_i$ and $e_{i,v} = \overline{e}_{i,v} \bmod \mathfrak{R}$ for all $1 \le v \le \varepsilon_i$. Set $W_{i,v} = W_i e_{i,v} = \Lambda e_{i,v}$ for all $1 \le v \le \varepsilon_i$. So we obtain the decomposition

$$W_i = \oplus_{1 \le v \le \varepsilon_i} W_{i,v}$$

where all $W_{i,v}$ are defined over the field K_i.

Similarly to how it was for the isomorphism γ in Section 2 construct the required isomorphisms $\gamma_{i,v}$ from the condition that $\gamma_{i,v} \bmod \mathfrak{R}(\overline{e}^{(i)}) = \overline{e}_v^{(i)}$.

Thus (a), (c), (d) and (e) are satisfied. Hence, (i), (ii), (iii), (iv) are satisfied. The construction for the case $K = \widetilde{k}$ is also completed.

4 Decomposition into the direct sum of indecomposable modules.

Let V be a Λ–module defined over the field k, see Introduction. Our aim is to construct the decomposition

$$V \simeq \sum_{i \in I} V_i^{\varepsilon_i} \tag{12}$$

from Theorem 1 and to prove it. By the Krull–Schmidt theorem, see e.g. [?], this isomorphism is unique up to isomorphisms and a permutation of direct summands.

Construct the algebra of endomorphisms of the module V

$$E = \mathrm{Hom}_\Lambda(V, V) \subset \mathrm{Hom}_K(V, V)$$

defined by its k–structure

$$E' = \mathrm{Hom}_{\Lambda'}(V', V') \subset \mathrm{Hom}_k(V', V').$$

Apply the construction from Sections 3 and 4 to the algebra E. So we get the projective ideals and idempotents of E. We change Λ for E and use other denotations from (i)–(iv), (a)–(e) of Section 4 for these projective ideals and idempotents of E.

Thus the family of orthogonal idempotents $e_{i,v}$, $1 \le v \le \varepsilon_i$, $i \in I$ is a family of orthogonal projections, i.e. this family defines the isomorphism of Λ–modules

$$V \to \oplus_{i \in I} \oplus_{1 \le v \le \varepsilon_i} V_{i,v} \tag{13}$$

where $V_{i,v} = e_{i,v}(V)$ and (13) is induced by the projections $e_{i,v} : V \to e_{i,v}(V)$, $1 \le v \le \varepsilon_i$, $i \in I$. The direct sum in (13) is a sum of submodules of V.

Each module $V_{i,v}$ is defined over the field K_i. Each module $V_{i,v}$ is indecomposable, $1 \le v \le \varepsilon_i$, $i \in I$. Indeed, if $V_{i,v} = V' \oplus V''$ is a direct sum of submodules V' and V'' of V then the projections to V' and V'' define the idempotents $e', e'' \in E$ such that $e_{i,v} = e' + e''$. This defines the decomposition of the E–module $W_{i,v} \simeq P_i$

into the direct sum of two its submodules. But P_i is an indecomposable projective module. Therefore, $e' = 0$ or $e'' = 0$ and then $V' = 0$ or $V'' = 0$, i.e. V is indecomposable as it was required.

We shall show that $V_{i_1,v_1} \simeq V_{i_2,v_2}$ if and only if $i_1 = i_2$ and construct this isomorphism. Suppose that $i_1 = i_2 = i$. Set $v_1 = v$. Recall that $P_i = Ee^{(i)}$ for the idempotent $e^{(i)}$. Denote by p_i (respectively $p_{i,v}$) the projection $E \to P_i$, $\lambda \mapsto \lambda e^{(i)}$ (respectively $E \to W_{i,v}$, $\lambda \mapsto \lambda e_v^{(i)}$). Set also $V_i = e^{(i)}(V)$.

Show how to construct an isomorphism $V_i \simeq V_{i,v}$.

Since P_i and $W_{i,v}$ are isomorphic projective modules the projective E–modules $E(1-e^{(i)})$ and $E(1-e_v^{(i)})$ are also isomorphic and defined over the field K_i. So we can construct an isomorphism $\delta_{i,v}$ between $E(1-e^{(i)})$ and $E(1-e_v^{(i)})$ similarly to that it was for the isomorphism γ in Section 2. Further, construct an isomorphism μ of the module E which is the direct sum of $\gamma_{i,v}$ and $\delta_{i,v}$. So $\gamma_{i,v} \circ p_i = p_{i,v} \circ \mu$ and $\mu|_{P_i} = \gamma_{i,v}$.

Hence

$$e^{(i)}\mu(1) = \mu(e^{(i)}) = \gamma_{i,v}(e^{(i)}) = (\gamma_{i,v} \circ p_i)(1) = (p_{i,v} \circ \mu)(1) = \mu(1)e_v^{(i)}$$

where $1 \in E$ is identity isomorphism of V. Note that $\mu(1)$ is invertible element of E since μ is an isomorphism of the E–module E to itself. So $e_v^{(i)} = \mu(1)^{-1}e^i\mu(1)$.

Now define an isomorphism $\nu_{i,v} : V_i \to V_{i,v}$ by the formula $v \mapsto \mu(1)^{-1}(v)$ for $v \in V_i$. The isomorphism $\nu_{i,v}$ is defined over the field K_i. Similarly the isomorphism ν_{i_2,v_2} is constructed. Therefore $V_{i_1,v_1} \simeq V_{i_2,v_2} \simeq V_i$ over the field K_i if $i_1 = i_2 = i$.

REMARK 7. One can construct similarly to Section 3 the isomorphisms $\nu_{i,v}$ satisfying additionally to the following property. If $K = \overline{k}$, $i, j \in I$, an embedding $\sigma : k_i \to K$ over k , an embedding $\sigma_1 : K_i \to K$ over k are such that $i^\sigma = j$, $\overline{e}_{i,v}^{\sigma_1} = \overline{e}_{j,v}$ for all v and σ_1 extends σ then $\nu_{i,v}^{\sigma_1} = \nu_{j,v}$.

Conversely, suppose that there exists an isomorphism $\nu : V_{i_1,v_1} \to V_{i_2,v_2}$ of Λ–modules. Then there exists an isomorphism $\widetilde{\nu} : V \to V$ of the Λ–module V which is a direct sum of ν and another isomorphism (similarly to that it was for μ) Hence, $\widetilde{\nu} \circ e_{v_1}^{(i_1)} = e_{v_2}^{(i_2)} \circ \widetilde{\nu}$ and $\widetilde{\nu}|_{e_{v_1}^{(i_1)}(V)} = \nu$. Define the isomorphism of E-modules $\mu : E \to E$ by the condition $\mu(1) = \widetilde{\nu}^{-1}$. One see immediately that $\mu(W_{i_1,v_1}) = W_{i_2,v_2}$, i.e. E–modules W_{i_1,v_1} and W_{i_2,v_2} are isomorphic. Therefore $P_{i_1} \simeq P_{i_2}$ and hence $i_1 = i_2$, see Section 2.

Thus we have constructed the required isomorphism (12).

5 Algorithms for the problem of the isomorphism of modules.

¿From the Krull–Schmidt theorem an the result of the previous section we get the following criteria of the isomorphism of two Λ–modules V_1 and V_2 defined over the field k such as in the Introduction.

Construct isomorphisms

$$V_1 \simeq \sum_{i \in I} V_i^{\varepsilon_i} \tag{14}$$

and

$$V_1 \oplus V_2 \simeq \sum_{j \in J} V_j^{\varepsilon_j}. \tag{15}$$

The modules V_1 and V_2 are isomorphic if and only if $\#I = \#J$ and there exists a bijection $\tau : I \to J$ such that $\varepsilon_{\tau(i)} = 2\varepsilon_i$. An isomorphism between V_1 and V_2 (if they are isomorphic) defined over a composite of fields of definition of all V_i, $i \in I$ and V_j, $j \in J$ can be also constructed. But we shall construct more than that.

By the Deuring–Noether theorem [?] if V_1 and V_2 are isomorphic over an algebraic extension of the field k then there exists an isomorphism $V_1 \simeq V_2$ defined over k. Our aim now is to construct such an isomorphism if it exists and to prove Theorem 2.

Construct the algebra of endomorphisms of the module V_1

$$E = \mathrm{Hom}_\Lambda(V_1, V_1) \subset \mathrm{Hom}_K(V_1, V_1)$$

defined by its k–structure

$$E' = \mathrm{Hom}_{\Lambda'}(V_1', V_1') \subset \mathrm{Hom}_k(V_1', V_1').$$

Further, construct the space of homomorphisms

$$V = \mathrm{Hom}_\Lambda(V_2, V_1) \subset \mathrm{Hom}_K(V_2, V_1)$$

which is a E–module defined over k by its k–structure

$$V' = \mathrm{Hom}_{\Lambda'}(V_2', V_1') \subset \mathrm{Hom}_k(V_2', V_1').$$

If $V_1 \simeq V_2$ then $E \simeq V$ as E–module.

LEMMA 4. If $V_1 \simeq V_2$ and $\delta : E \to V$ is an isomorphism of E–modules defined over k then $\delta(1) : V_2 \to V_1$ is an isomorphism of Λ–modules defined over k.

PROOF. Denote $C' = \mathrm{Ker}\delta(1)$ and $C'' = \mathrm{Im}\delta(1)$. We have the exact sequence

$$0 \to C' \to V_2 \to C'' \to 0$$

which gives the exact sequence

$$0 \to \mathrm{Hom}_\Lambda(C'', V_2) \to \mathrm{Hom}_\Lambda(V_2, V_2) \to \mathrm{Hom}_\Lambda(C', V_2).$$

In this sequence the homomorphism $\mathrm{Hom}_\Lambda(V_2, V_2) \to \mathrm{Hom}_\Lambda(C', V_2)$ is nonzero if C' is nonzero. Therefore, $\dim_K \mathrm{Hom}_\Lambda(C'', V_2) \le \dim_K \mathrm{Hom}_\Lambda(V_2, V_2)$ and the equality takes place if and only if $C' = \{0\}$, i.e. if and only if $\delta(1)$ is an isomorphism.

Each homomorphism $\beta \in \mathrm{Hom}_\Lambda(V_2, V_1)$ can be uniquely represented in the form $\beta = \alpha \circ \delta(1)$ where $\alpha \in \mathrm{Hom}_\Lambda(V_1, V_1)$. Hence the honomorhism $\mathrm{Hom}_\Lambda(V_2, V_1) \to \mathrm{Hom}_\Lambda(C'', V_1)$, $\beta \mapsto \alpha|_{C''}$ is an embedding. Further, we have

$$\mathrm{Hom}_\Lambda(V_2, V_2) \simeq \mathrm{Hom}_\Lambda(V_1, V_1) \simeq \mathrm{Hom}_\Lambda(V_2, V_1) \hookrightarrow \mathrm{Hom}_\Lambda(C'', V_1) \simeq \mathrm{Hom}_\Lambda(C'', V_2)$$

where the first isomorphism takes place since $V_1 \simeq V_2$, the second since δ is an isomorphism and the third since $V_1 \simeq V_2$. Hence, $\dim_K \mathrm{Hom}_\Lambda(C'', V_2) \geq \dim_K \mathrm{Hom}_\Lambda(V_2, V_2)$. Thus $\delta(1)$ is an isomorphism. The lemma is proved.

Using the algorithm described in Section 2 decide whether V is a projective E-module. If V is not a projective E–module than $E \not\simeq V$ and hence $V_1 \not\simeq V_2$. If V is a projective E–module then decide using the algorithm from Section 2 whether there exists an isomorphism of E–modules $E \simeq V$. By the Deuring–Noether theorem if such an isomorphism exists then there exists also an isomorphism of E–modules $E \simeq V$ defined over k. If $E \not\simeq V$ then $V_1 \not\simeq V_2$. If $E \simeq V$ then our aim till the end of the Section will be to construct such an isomorphism $\delta : E \to V$ defined over the field k. Further, if $\delta(1)$ is not an isomorphism then $V_1 \not\simeq V_2$ by Lemma 4. Otherwise, $\delta(1)^{-1} : V_1 \to V_2$ is the required isomorphism.

Thus we can suppose that $E \simeq V$ and our aim is to construct such an isomorphism defined over k. Denote by $\mathfrak{R}$ the radical of E and compute $\mathfrak{R}$. Note that it is sufficient to construct an isomorphism $E/\mathfrak{R} \simeq V/\mathfrak{R}V$ defined over the field k. Indeed, if such an isomorphism is constructed then since E and V are projective modules we can lift this isomorphism till an isomorphism $E \to V$, similarly to that it was for the isomorphism γ in Section 2. So construct $E/\mathfrak{R}$ and $V/\mathfrak{R}V$. We shall suppose further without loss of generality that $\mathfrak{R} = \{0\}$, i.e. that E is a semisimple algebra over the field k.

At first we shall describe a direct method for constructing an isomorphism defined over the field k of two E–modules W_1 and W_2 defined over the field k when E is a semisimple algebra. Let E', W_1' and W_2' be the k–structures of E, W_1 and W_2. Compute a nonzero element $h \in \mathrm{Hom}_{E'}(W_1', W_2')$. Since E' is a semisimple algebra the modules $\mathrm{Im}\, h$ and $\mathrm{Coker}\, h$ are projective. Therefore, $W_1 \simeq \mathrm{Ker}\, h \oplus \mathrm{Im}\, h$ and $W_2 \simeq \mathrm{Im}\, h \oplus \mathrm{Coker}\, h$. Construct these isomorphisms using the algorithm from Section 2. Since E' is semisimple the modules $W_1' \simeq W_2'$ if and only if $\mathrm{Ker}\, h \simeq \mathrm{Coker}\, h$. To obtain an isomorphism $W_1' \simeq W_2'$ it is sufficient now to construct an isomorphism $\mathrm{Ker}\, h \simeq \mathrm{Coker}\, h$. But $\dim_k \mathrm{Ker}\, h < \dim_k W_1'$, $\dim_k \mathrm{Coker}\, h < \dim_k W_2'$. So we can apply the algorithm under description recursively to $\mathrm{Ker}\, h$ and $\mathrm{Coker}\, h$ instead of W_1' and W_2'. The description of this direct method is completed. This algorithm works in the polynomial time if the field k is finite.

In the case of an infinite field k one should estimate the growth of coefficients from k in the described construction. But instead of that for the case when k is infinite we shall describe an algorithm for constructing an isomorphism between E and V.

Consider the case when k is an infinite field. Set $K = \overline{k}$ and effect all the construction of Section 1 for the algebra E and the module V. Change everywhere in Section 1 Λ for E including the denotations with indices and conserve all the other denotations from this Section (one should not confuse these denotations with ones from Section 3).

For every $i \in H_u$, $I \in I_1$ construct the isomorphisms $E_i \simeq U_i^{e_i}$ and $V_i \simeq U_i^{e_i}$ defined over the field K_i are constructed. These isomorphisms induce the isomorphism

$$\rho_i : E_i \to V_i$$

defined over the field K_i for every $i \in H_u$, $I \in I_1$. Besides that, see Remark 5, the isomorphisms ρ_i satisfy to the following property. If $i, j \in H_u$, an embedding $\sigma : k_i \to K$ over k, an embedding $\sigma_1 : K_i \to K$ over k which extends σ are such that $i^\sigma = j$, $e_{i,v}^{\sigma_1} = e_{j,v}$ then $\rho_i^{\sigma_1} = \rho_j$ in the sense that $\rho_i(x)^{\sigma_1} = \rho_j(x^{\sigma_1})$ for every $x \in E_i' \otimes_{k_i} K_i$ (recall that E_i' is the k_i–structure of E_i).

We have the isomorphisms $E_u \simeq \oplus_{i \in H_u} E_i$ and $E_u V \simeq \oplus_{i \in H_u} E_i V$ which are given by the same formula $z \mapsto (e_i z)_{i \in H_u}$ for $z \in E_u$ or $z \in E_u V$. These isomorphisms induce the isomorphism

$$\theta : \mathrm{Hom}_E(E_u, E_u V) \to \oplus_{i \in H_u} \mathrm{Hom}_E(E_i, E_i V).$$

The isomorphism θ defines the projection

$$\theta_i : \mathrm{Hom}_E(E_u, E_u V) \to \mathrm{Hom}_E(E_i, E_i V)$$

for every $i \in H_u$. The projection θ_i is defined over the field k_i since it is induced by the projection $E_u V \to E_i V$, $z \mapsto e_i z$ and the inclusion $E_i \to E_u$, $z \mapsto z$ which are defined over the field k_i.

Denote by E_u' (respectively E_i') the k–structure (respectively k_i–structure) of E_u (respectively E_i). Then $E_u' V'$, $\mathrm{Hom}_{E'}(E_u', E_u' V')$ (respectively $E_i' V' \otimes_k k_i$, $\mathrm{Hom}_{E' \otimes_k k_i}(E_i', E_i'(V' \otimes_k k_i))$ is the k–structure (respectively k_i–structure) of $E_u V$ (respectively $E_i V$, $\mathrm{Hom}_E(E_i, E_i V)$). It follows immediately from the considered construction that if $i, j \in H_u$ and an embedding $\sigma : k_i \to K$ over k, the element $z \in \mathrm{Hom}_{E'}(E_u', E_u' V')$ are such that $i^\sigma = j$ then $\theta_i(z)^\sigma = \theta_j(z)$ in the sense that $\theta_i(z)(y)^\sigma = \theta_j(z)(y^\sigma)$ for every $y \in E_i'$.

For every $u \in I_1$ effect the following. Fix an index $i \in H_u$. Construct the vector spaces of homomorphisms $\mathrm{Hom}_{E'}(E_u', E_u' V')$ and $\mathrm{Hom}_{E' \otimes_k k_i}(E_i', E_i'(V' \otimes_k k_i))$. Denote by $\phi_w, 1 \le w \le a$ the k–basis of $\mathrm{Hom}_{E'}(E_u', E_u' V')$ which is constructed. Construct $\theta_i(\phi_w) \in \mathrm{Hom}_{E' \otimes_k k_i}(E_i', E_i'(V' \otimes_k k_i))$ for all $1 \le w \le a$. The elements $\theta_i(\phi_w)$, $1 \le w \le a$ generate the K_i–vector space

$$\mathrm{Hom}_{E' \otimes_k k_i}(E_i', E_i'(V' \otimes_k k_i)) \otimes_{k_i} K_i =$$
$$\mathrm{Hom}_{E' \otimes_k K_i}(E_i' \otimes_{k_i} K_i, (E_i' \otimes_{k_i} K_i)(V' \otimes_k K_i))$$

since θ_i is an epimorphism. So solving a linear system compute a representation

$$\rho_i = \sum_{1 \le w \le a} \lambda_w \theta_i(\phi_w)$$

where $\lambda_w \in K_i$ for all w.

Now construct integers $\widetilde{\lambda}_w$, $1 \leq w \leq a$ in the following way, c.f. Lemma 2. Let $\widetilde{\lambda}_w$ are constructed for $0 \leq w < j \leq a$. Show how to construct $\widetilde{\lambda}_j$. Enumerate $t = 1, 2, \ldots$. For the considered value of t compute

$$\rho_{i,j}(t) = (\sum_{1 \leq w < j} \widetilde{\lambda}_w \theta_i(\phi_w)) + t\theta_i(\phi_j) + (\sum_{j < w \leq a} \lambda_j \theta_i(\phi_w)).$$

Decide whether $\rho_{i,j}(t)$ is an isomorphism. If $\rho_{i,j}(t)$ is an isomorphism set $\widetilde{\lambda_j} = t$, otherwise, go to the consideration of the next value of t. Note that $\widetilde{\lambda}_j \leq 1 + \dim_{k_i} V_i'$ since the determinant of the square matrix corresponding to $\rho_{i,j}(t)$ considered as a polynomial in t has at most $\dim_{k_i} V_i'$ zeros.

Set

$$\widetilde{\rho}_i = \sum_{1 \leq w \leq a} \widetilde{\lambda}_w \theta_i(\phi_w)$$

where $\lambda_w \in K_i$ for all w. Thus, $\widetilde{\rho}_i$ is an isomorphism. Set

$$\widetilde{\rho}_u = \sum_{1 \leq w \leq a} \widetilde{\lambda}_w \phi_w.$$

Then $\theta_j(\widetilde{\rho}_u)$ is an isomorphism for every $j \in H_u$ since $\theta_j(\widetilde{\rho}_u) = \theta_i(\widetilde{\rho}_u)^\sigma = \widetilde{\rho}_i^\sigma$ for the embedding $\sigma : k_i \to K$ over k such that $j = i^\sigma$. Hence, $\theta(\widetilde{\rho}_u)$ is an isomorphism. Therefore, $\widetilde{\rho}_u$ is an isomorphism for every $u \in I_1$.

We have the isomorphisms $E \simeq \oplus_{u \in I_1} E_u$ and $V \simeq \oplus_{u \in I_1} E_u V$ defined over the field k and given by the same formula $z \mapsto (e_u z)_{u \in I_1}$ for $z \in E$ or $z \in V$. Finally, using these isomorphism and the direct sum of isomorphisms $\widetilde{\rho}_u$, $u \in I_1$ construct the required isomorphism $\widetilde{\rho} : E \simeq V$ defined over the field k. The case of an infinite field k is considered completely. The description of the algorithm of this Section is completed.

6 The problem of similarity of families of matrices.

Our aim is to prove Theorem 4 from the Introduction. Denote by $M_r(k)$ the algebra of $r \times r$ matrices with coefficients from the field k. Compute the k–algebra

$$\Lambda' = \{C \in M_r(k) : CA_i = A_i C,\ 1 \leq i \leq m\}$$

and Λ'–module

$$V' = \{C \in M_r(k) : CB_i = A_i C,\ 1 \leq i \leq m\}.$$

LEMMA 5. The existence of the matrix S from the formulation of Theorem 4 is equivalent to two conditions

(a) there exists an isomorphism $\mu_0 : \Lambda' \to V'$ is of Λ'–modules

(b) for every isomorphism $\mu : \Lambda' \to V'$ of Λ'–modules $\mu(1)$ is an invertible matrix.

Besides that if these conditions are satisfied then one can take $S = \mu(1)$ in the formulation of Theorem 4.

PROOF. If S exists then then we have the required isomorphism $\mu_0 : \Lambda' \to V'$ defined by the condition $S = \mu_0(1)$. Hence (a) is fulfilled. If μ is an arbitrary isomorphism then $S = C\mu(1)$ for some matrix $C \in \Lambda'$ since $S \in V'$. Therefore $\mu(1)$ is invertible. Hence (b) is fulfilled. Conversely, suppose that (a) and (b) are satisfied. Set $S = \mu(1)$. Then S is the required in the formulation of Theorem 4 matrix. The lemma is proved.

Now set $K = \overline{k}$, $\Lambda = \Lambda' \otimes_k K$ and $V = V' \otimes_k K$. So Λ is an algebra defined over k and V is a Λ–module defined over k. Apply the algorithm from Section 5 to the Λ-modules Λ and V defined over k and decide whether these modules are isomorphic over k. Further if it is the fact construct an isomorphism $\mu : \Lambda \to V$ defined over the field k. Construct the matrix $\mu(1)$. Decide whether $\mu(1)$ is an invertible matrix. If $\mu(1)$ is an invertible matrix then set $S = \mu(1)$. By Lemma 5 S is the required matrix and, conversely, the required matrix S exists only if there exists μ and $\mu(1)$ is invertible. The algorithm for Theorem 4 is described completely.

7 The problem of similarity of families of matrices relatively to the orthogonal group

Our aim is to prove Theorem 5 from the Introduction. Denote by $M_r(k)$ the algebra of $r \times r$ matrices with coefficients from the field k. Denote by T the operation of transposition of matrices.

Show how to compute the k–subalgebras Λ'_1 (respectively Λ'_2) of the algebra $M_r(k)$ generated by the matrices E, A_1, $A_1^T, \ldots, A_m$, A_m^T (respectively E, B_1, $B_1^T, \ldots, B_m$, B_m^T). Here E denotes the unity element of $M_r(k)$. The algorithm for constructing Λ'_1 is the following. Set L_1 to be the vector subspace of $M_r(k)$ generated by the matrices E, A_1, $A_1^T, \ldots, A_m$, A_m^T and compute the basis $l_{1,j}$, $1 \leq j \leq r_1$ of L_1 consisting of some elements of the sequence E, A_1, $A_1^T, \ldots, A_m$, A_m^T. Further, recursively for $i \geq 1$ suppose that L_i with its k–basis $l_{i,j}$, $1 \leq j \leq r_i$ is constructed. Then if $L_i \neq L_{i-1}$ of $i = 1$ construct the subspace $L_{i+1} = L_1 L_i + L_i L_1$ with its k–basis $l_{i+1,j}$, $1 \leq j \leq r_{i+1}$. Namely, set $l_{i+1,j} = l_{i,j}$ if $1 \leq j \leq r_i$ and choose as $l_{i+1,j}$ for $r_i + 1 \leq j \leq r_{i+1}$ some products $l_{1,j_1} l_{i,j_2}$ or $l_{i,j_2} l_{1,j_1}$ for $1 \leq j_1 \leq r_1$, $1 \leq j_2 \leq r_i$. If $L_i = L_{i-1}$ then set $\Lambda'_1 = L_i$, $i_0 = i$. Note that each $l_{i,j}$ is a product of no more than i elements of the sequence E, A_1, $A_1^T, \ldots, A_m$, A_m^T and these expressions of $l_{i,j}$ as products can be obtained from the algorithm. Similarly the algebra Λ'_2 is constructed.

Show how to decide whether there exists an isomorphism $\mu : \Lambda'_1 \to \Lambda'_2$ such that $\mu(A_i) = B_i$ and $\mu(A_i^T) = B_i^T$ for all $1 \leq i \leq m$. This siomorphism exists if and only if the two conditions are satisfied

(a) the basis $l_{i_0,j}$, $1 \le j \le r_{i_0}$, of Λ'_2 can be obtained by substituting in expressions of $l_{i_0,j}$, $1 \le j \le r_{i_0}$, as products of some elements of the sequence E, A_1, $A_1^T, \ldots, A_m$, A_m^T corresponding elements of the sequence E, B_1, $B_1^T, \ldots, B_m$, B_m^T;

(b) the multiplication tables of the basises $l_{i_0,j}$, $1 \le j \le r_{i_0}$, and $l'_{i_0,j}$, $1 \le j \le r_{i_0}$, coincide.

So we can construct μ if it exists. If μ does not exist then also there exists no matrix S from the formulation of Theorem 5. So we shall suppose further that μ exists and constructed explicitely.

Set $K = \widetilde{k}$, $\Lambda_j = \Lambda'_j \otimes_k K$, $j = 1, 2$. Not that if C belongs to Λ'_j (respectively Λ_j) then C^T also belongs to Λ'_j (respectively Λ_j), $j = 1, 2$. We have the scalar product on algebras Λ'_j and Λ_j, $j = 1, 2$. Namely, if x, y belong to Λ'_j or Λ_j then their scalar product is $\mathrm{tr}(xy^T)$.

LEMMA 6. The k–algebras Λ'_j are semisimple for $j = 1, 2$. Therefore the K–algebras Λ_j are also semisimple for $j = 1, 2$.

PROOF. Let $x \in \mathfrak{R}'$ where $\mathfrak{R}'$ is the radical of Λ'_j. Then xx^T is nilpotent. Therefore, the trace $\mathrm{tr}(xx^T) = 0$. Hence, $x = 0$ since k is a real field. The lemma is proved.

Using the algorithm from Section 1 construct the isomorphisms

$$\Lambda_j \simeq \oplus_{i \in I} \Lambda_{j,i},\ j = 1, 2 \tag{16}$$

where $\Lambda_{j,i} \subset \Lambda_j$ are simple algebras over K. Besides that $\Lambda_{j,i}$ is defined over the field k_i which is constructed and has the k_i–structure $\Lambda'_{j,i}$ such $(\mu \otimes_k k_i)(\Lambda'_{1,i}) = \Lambda'_{2,i}$. Factually it is sufficient to construct (16) for $j = 1$ and then apply the isomorphism $\mu \otimes_k K$.

LEMMA 7. The sum in (16) is a direct orthogonal sum of subspaces.

PROOF. Denote by $e_{j,i}$ the central idempotent defining $\Lambda_{j,i}$, i.e. $\Lambda_{j,i} = \Lambda e_{j,i}$. Then the idempotent $e_{j,i}^T \in \Lambda_{j,i}$ and also $\Lambda_{j,i} = \Lambda e_{j,i}^T$. Therefore $e_{j,i} = e_{j,i}^T$ for all j, i. Therefore, if $x_1 \in \Lambda_{j,i_1}$, $x_2 \in \Lambda_{j,i_2}$ than $\mathrm{tr}(x_1 x_2^T) = \mathrm{tr}(x_1 e_{j,i_1}(x_2 e_{j,i_2})^T) = \mathrm{tr}(x_1 e_{j,i_1} e_{j,i_2}^T x_2^T) = \mathrm{tr}(x_1 e_{j,i_1} e_{j,i_2} x_2^T) = \mathrm{tr}(0) = 0$. The lemma is proved.

Denote by V the space of columns K^r which is Λ_j–module, $j = 1, 2$. The scalar product of $w_1, w_2 \in V$ is equal to $w_1^T w_2$. Construct the isomorphisms

$$V \simeq \sum_{i \in I} \Lambda_{j,i} V,\ j = 1, 2. \tag{17}$$

The similar computation as it was in Lemma 7 for (16) shows that the sum in (17) is a direct orthogonal sum of subspaces.

Denote by D_i the division algebra such that $\Lambda_{j,i} = M_{m_i}(D_i)$ by the Wedderbarn theorem, see Section 1. Using the algorithm from Section 1 construct for the algebras $\Lambda_{j,i}$ simple module $U_{j,i} \subset \Lambda_{j,i}$ defined over the field K_i with the annulator $\mathfrak{m}_{j,i}$

also defined over the field K_i for all i and $j = 1, 2$. Besides that, the K_i–structure of $U_{j,i}$ (respectively $\mathfrak{m}_{j,i}$) is $U'_{j,i}$ (respectively $\mathfrak{m}'_{j,i}$) and $(\mu \otimes_k K_i)(U'_{1,i}) = U'_{2,i}$, $(\mu \otimes_k K_i)(\mathfrak{m}'_{1,i}) = \mathfrak{m}'_{2,i}$. Factually it is sufficient to construct everything for $j = 1$ and then apply the isomorphism $\mu \otimes_k K$.

Construct the isomorphisms

$$\Lambda_{j,i}V = \sum_{1 \le v \le e_{j,i}} \Lambda_{j,i} f_{j,i,v},\ i \in I,\ j = 1, 2 \tag{18}$$

where $\Lambda_{j,i}f_{j,i,v}$ is a simple $\Lambda_{j,i}$–module defined over the field K_i; $f_{j,i,v} \in (\Lambda_{j,i} \otimes_{k_i} K_i)(V'_j \otimes_k K_i)$, $1 \le v \le e_{j,i}$ is an orthonormal system of vectors with the same annulator $\mathfrak{m}_{j,i} \subset \Lambda_{j,i}$ which is given by the K_i–structure $\mathfrak{m}'_{j,i}$. Besides that,

$$\sum_{1 \le v \le e_{j,i}} f_{j,i,v} D_i = \{v \in \Lambda_{j,i}V : \mathfrak{m}'v = \{0\}\} = V''_{j,i}$$

and $\sum_{1 \le v \le e_{j,i}} f_{j,i,v} D_i$ is an orthogonal direct sum of subspaces $f_{j,i,v}D_i$, see Section 1.

LEMMA 8. The sum in (18) is a direct orthogonal sum of subspaces.

PROOF. The orthogonal complement $(\Lambda_{j,i}f_{j,i,v})^\perp \subset \Lambda_{j,i}V$ is an ideal since if $w_1 \in (\Lambda_{j,i}f_{j,i,v})^\perp$, $w_2 \in \Lambda_{j,i}f_{j,i,v}$, $\lambda \in \Lambda$ then $\lambda^T \in \Lambda$ and $(\lambda w_1)^T w_2 = w_1^T(\lambda^T w_2) = 0$. We have the decomposition into the direct sum

$$V''_{j,i} = (\Lambda_{j,i}f_{j,i,v} \cap V''_{j,i}) \oplus ((\Lambda_{j,i}f_{j,i,v})^\perp \cap V''_{j,i}).$$

But $\Lambda_{j,i}f_{j,i,v} \cap V''_{j,i} = f_{j,i,v}D_i$. Therefore,

$$(\Lambda_{j,i}f_{j,i,v})^\perp \cap V''_{j,i} = \sum_{1 \le v_1 \le e_{j,i},\ v_1 \ne v} f_{j,i,v_1} D_i$$

since $\sum_{1 \le v_1 \le e_{j,i},\ v_1 \ne v} f_{j,i,v_1} D_i = (f_{j,i,v}D_i)^\perp$ in $V''_{j,i}$. Thus $f_{j,i,v_1} \in (\Lambda_{j,i}f_{j,i,v})^\perp$ for every $v_1 \ne v$.

Therefore for every $v_1 \ne v$ we have $\Lambda_{j,i}f_{j,i,v_1} \subset (\Lambda_{j,i}f_{j,i,v})^\perp$. Hence, the sum

$$\sum_{1 \le v_1 \le e_{j,i}, v_1 \ne v} \Lambda_{j,i} f_{j,i,v_1} \subset (\Lambda_{j,i}f_{j,i,v})^\perp.$$

Thus,

$$\sum_{1 \le v_1 \le e_{j,i}, v_1 \ne v} \Lambda_{j,i} f_{j,i,v_1} = (\Lambda_{j,i}f_{j,i,v})^\perp$$

since the dimensions of the both sides coincide. The lemma is proved.

Now we get immediately that for the existence of the matrix S required in the formulation of Theorem 5 it is necessary that $e_{1,i} = e_{2,i}$ for all $i \in I$.

Show that this condition is also sufficient. So we shall suppose further that $e_{1,i} = e_{2,i} = e_i$ for all $i \in I$. Construct the isomorphism $\nu_{i,v} \in \mathrm{Hom}_K(\Lambda_{1,i}f_{1,i,v}, \Lambda_{2,i}f_{2,i,v})$, defined over the field K_i such that $\nu_{i,v}(\lambda f_{1,i,v}) = \mu(\lambda) f_{2,i,v}$ for every $\lambda \in \Lambda$ which exists according to described above.

LEMMA 9. The homomorphism $\nu_{i,v}$ conserve scalar product, i.e. for every $w_1, w_2 \in \Lambda_{1,i}V$ we have $w_1^T w_2 = (\nu_{i,v}(w_1))^T \nu_{i,v}(w_2)$

PROOF. Let $\mathbf{e}_j$ be an orthonormal basis of $\Lambda_{1,i}f_{j,i,v}$ such that $f_{j,i,v}$ is the first of its elements, $j = 1, 2$. It is sufficient to prove that the matrix ψ of $\nu_{i,v}$ in the basises $\mathbf{e}_1, \mathbf{e}_2$ is an orthogonal matrix. Let $\lambda \in \Lambda_{j,i}$. Denote by $\varphi_1(\lambda)$ (respectively $\varphi_2(\lambda)$) the matrix of the homomorphism $\Lambda_{1,i}f_{1,i,v} \to \Lambda_{1,i}f_{1,i,v}$, $z \mapsto \lambda z$ (respectively $\Lambda_{2,i}f_{2,i,v} \to \Lambda_{2,i}f_{2,i,v}$, $z \mapsto \mu(\lambda)z$). Then

$$\psi\varphi_1(\lambda) = \varphi_2(\lambda)\psi \tag{19}$$

for every $\lambda \in \Lambda$ by the definition of μ. Further we have $\varphi_j(\lambda^T) = \varphi_j(\lambda)^T$ for every $\lambda \in \Lambda$ since the matrix $\varphi_j(\lambda)$ is a submatrix of the block–diagonal matrix $\mathrm{diag}(\varphi_j(\lambda), \varphi'_j(\lambda))$ which is obtained from λ by the the orthogonal transformation of similarity corresponding to the decomposition (18) into the orthogonal direct sum. Hence

$$\psi\varphi_1(\lambda)^T = \varphi_2(\lambda)^T\psi$$

for every $\lambda \in \Lambda$. Therefore,

$$\psi^T\varphi_2(\lambda) = \varphi_1(\lambda)\psi^T \tag{20}$$

for every $\lambda \in \Lambda$. Now (19) and (20) give

$$\psi^T\psi\varphi_1(\lambda) = \varphi_1(\lambda)\psi^T\psi$$

for every $\lambda \in \Lambda$. Hence $\psi^T\psi$ is a matrix of some homomorphism

$$\mu_1 \in \mathrm{Hom}_{\Lambda_1}(\Lambda_{1,i}f_{1,i,v}, \Lambda_{1,i}f_{1,i,v}).$$

But $\Lambda_{1,i}f_{1,i,v}$ is a simple Λ_1–module. Therefore, $\mathrm{Hom}_{\Lambda_1}(\Lambda_{1,i}f_{1,i,v}, \Lambda_{1,i}f_{1,i,v}) \simeq D_i$. Thus, the minimal polynomial of the matrix $\psi^T\psi$ over K is linear or square with a negative discriminant. But all the eigenvalues of the symmetric and therefore diagonalizable matrix $\psi^T\psi$ with coefficients from k are non–negative elements of k. Hence, the minimal polynomial of the matrix $\psi^T\psi$ over K is linear. Finally, $\psi^T\psi$ is the identity matrix since the first column of ψ is $(1, 0, \ldots, 0)^T$ due to the fact that $\nu_{i,v}(f_{1,i,v}) = f_{2,i,v}$. Thus ψ is an orthogonal matrix. The lemma is proved.

Now set the isomorphism $\nu \in \mathrm{Hom}_K(V, V)$ to be the direct sum of isomorphisms $\nu_{i,v}$ for $i \in I$, $1 \le v \le e_i$. By Lemma 9 this homomorphism has an orthogonal matrix in any orthogonal basis of V. We have $\nu(\lambda w) = \mu(\lambda)\nu(w)$ or $\mu(\lambda)w = \nu(\lambda\nu^{-1}(w))$ for all $\lambda \in \Lambda$ and $w \in V$. So one can take as S the matrix of the linear homomorphism ν. Theorem 5 is proved.

REMARK 8. It follows from the construction described that the matrix S can be represented as a product of three orthogonal matrices $S = S_1S_2S_3$ such that each coefficient of S_1, S_2, S_3 is from the extension of k of the degree bounded from above by a polynomial in n, m, r (though the field generated by coefficients of each of these matrices is of exponential degree in n, m, r in the general case).

REMARK 9. One can describe in a similar way the algorithms for the problem of similarity of families of matrices relatively to the unitary and simplectic groups.

References

[1] **Pierce R. S.:** *"Associative algebras"*, Springer-Verlag, 1982

[2] **Rónyai L.:** *"Computations in Associative algebras"*, DIMACS SERIES in Discrete Math. 11, 1993, AMS. pp. 221-243.

[3] **Eberly W. M.:** *"Decomposition of algebras over finite fields and number fields"*, Computational Complexity. 1, 1991, 179–206.

[4] **Eberly W. M.:** *"Decompositions of algebras over* **R** *and* **C***"*, Computational Complexity. 1, 1991, 207–230.

[5] **Babai L., Rónyai L.:** *"Computing irreducible representations of finite groups"*, Mathematics of Computation. 192, 1990, 705–722.

[6] **Bochnak J., Coste M., Roy M.–F.:** *"Géométrie algébrique réelle"*, Springer–Verlag, Berlin, Heidelberg, New York, 1987.

[7] **Chistov A. L.:** *"Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), pp. 124–188 (Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

[8] **Dickson L.E.:** *"Algebras and their arithmetics"*, University of Chicago, 1923.

[9] **Rónyai L.:** *"Computing the structure of finite algebras"*, Journal of Symbolic Computation. 9, 1990, 355–373.

[10] **Curtis C. W., Reiner I.** *"Representation theory of finite groups and associative algebras"* John Wiley and Sons, 1966.