CIS-TR-85-03

Polynomial time solutions of some problems in computational algebra*

Katalin Friedl
Computer and Automation Institute
Hungarian Academy of Sciences
Budapest, Hungary

Lajos Rónyai
Computer and Automation Institute
Hungarian Academy of Sciences
Currently visiting CIS Department,
University of Oregon, Eugene, OR

*This paper has been accepted for publication in the Proceedings of the 17th Annual ACM Symposium on Theory of Computing (May 6-8, 1985 Providence, Rhode Island).

Polynomial time solutions of some problems in computational algebra

by

Katalin Friedl and Lajos Rónyai*

Computer and Automation Institute
Hungarian Academy of Sciences
Budapest, Hungary

Abstract. The first structure theory in abstract algebra was that of finite dimensional Lie algebras (Cartan-Killing), followed by the structure theory of associative algebras (Wedderburn-Artin). These theories determine, in a non-constructive way, the basic building blocks of the respective algebras (the radical and the simple components of the factor by the radical). In view of the extensive computations done in such algebras, it seems important to design efficient algorithms to find these building blocks.

We find polynomial time solutions to a substantial part of these problems. We restrict our attention to algebras over finite fields and over algebraic number fields. We succeed in determining the radical (the "bad part" of the algebra) in polynomial time, using (in the case of prime characteristic) some new algebraic results developed in this paper. For associative algebras we are able to determine the simple components as well. This latter result generalizes factorization of polynomials over the given field. Correspondingly, our algorithm over finite fields is Las Vegas.

Some of the results generalize to fields given by oracles.

Some fundamental problems remain open. An example: decide whether or not a given rational algebra is a noncommutative field.

1. Introduction.

We address computational problems in matrix algebras, finite dimensional associative algebras and Lie algebras over a field F. Analogous problems for finite permutation groups have been considered by W. M. Kantor and E. M. Luks (see Babai-Kantor-Luks [1]). For the basic definitions see Section 2.

1.1. Building blocks.

The classical structure theories of associative and Lie algebras (see Jacobson [8], Herstein [7]) describe the basic building blocks of these algebras. The "bad part" is the *radical*. The factor by the radical is *semisimple* and a semisimple associative algebra is a direct sum of *simple* algebras.

The textbook proofs of these results are not constructive. They mostly start by picking "any minimal right ideal". But the minimal right ideals may not cover more than a tiny fragment of the algebra and might be quite difficult to find. (In fact, this problem is still open and is related to 1.6 below.)

1.2. The significance of the results.

Finding the radical and the simple factors of the radical quotient are as essential to computational algebra as factoring integers and finding composition factors are to computational number theory and group theory, resp. (A polynomial time algorithm to find the composition factors of permutation groups has recently been given by E. M. Luks, cf. [1].)

In addition, such results (on algebras) are likely to have applications to computational group theory as well since group representations are a major source of problems on matrix algebras, both associative and Lie. For instance the (open) problem of finding an invariant subspace for a group representation is a matrix algebra problem closely related to those discussed here.

1.3. The basic problem.

We want to find the building blocks (radical, simple factors) of a finite dimensional (associative or Lie) algebra in polynomial time.

We note that no such algorithms seem to appear in the literature on computational algebra (except for the trivial problem of finding the radical of an algebra of characteristic zero). Thus, we had to find new algorithms rather than just analyse existing ones. Some of the algorithms require new theoretical results in algebra (see Section 5).

1.4. Connection with factoring polynomials.

The case of commutative associative algebras generalizes the problem of factoring polynomials over F. Indeed, let $f \in F[x]$ and let $f = g_1^{a_1} \dots g_k^{a_k}$ where the g_j are irreducible over F. Consider the commutative associative algebra $R = F[x]/(f)$. (Computing with polynomials *mod f*.) The radical of R comes from the "degeneracy" of f, i.e. the presence of multiple factors: $Rad(R)$ is generated (as an ideal of R) by $h = g_1 \dots g_k$. The quotient $R/Rad(R)$ is isomorphic to $F[x]/(h)$. This in turn is the direct sum of its simple components, i. e. the fields $F[x]/(g_j)$ $(j=1,\dots,k)$. Finding these components is equivalent to factoring f.

Partly for this reason we restrict our base field F to be a *finite field* or an *algebraic number field* (finite extension of the rationals). Some of the results, however, generalize to fields given by appropriately restricted oracles.

1.5. The main results.

A/. *The radical.* We find it in deterministic polynomial time, both for associative and Lie algebras. We note that the difficult case is when F has characterisic p.

B/. *The simple components* of an associative semisimple algebra. We find them

both in characteristic zero and in characteristic p. Since the algorithm involves factoring over F (and over finite extensions of F), our algorithm is deterministic polynomial time in the former case and polynomial time Las Vegas in the latter.

1.6. Open problems.

A simple associative algebra is isomorphic to a full matrix algebra over a possibly noncommutative field.

The main open problem remaining is to find an explicit isomorphism with such a full matrix algebra. This would involve finding minimal right ideals.

In particular, we are unable to determine whether or not a given rational algebra is a skew field.

Another important problem is to find the composition factors of a (semisimple) Lie algebra.

1.7. Acknowledgements.

The authors are indebted to L. Babai for suggesting the problem. Helpful discussions with S. Becker and E. M. Luks are also acknowledged.

2. Definitions.

A is an *associative algebra* (or *algebra* for short) over the field F if

i) A is a vector space over F

ii) A is equipped with a multiplication $*$ such that $<A,+,*>$ is an associative ring

iii) $\lambda(x*y)=(\lambda x)*y=x*(\lambda y)$ holds for every $x,y\in A$ and $\lambda\in F$.

For the sake of simplicity we shall write xy instead of $x*y$. A nonempty subset B of A is a *subalgebra* if it is both a subring and a subspace of A. Similarly, a subspace B is an ideal if it is a ring ideal of A. If B is an ideal of A then we may take the *factor algebra* A/B in the standard way. The algebra A is *simple* if it has only trivial ideals (i.e. (0) and A) and $AA\neq(0)$. We say that the algebra A is the direct sum of its ideals $A_1,A_2,...,A_k$ (written as $A_1+...+A_k$) if A is the vector-space direct sum of the subspaces A_i.

Here we consider finite dimensional algebras only.

The *center* $Z(A)$ of the algebra A is defined as

$$Z(A)=\{\ x\in A\ ;\ xy=yx \text{ for every } y\in A\ \}.$$

If $Z(A)=A$ then A is a *commutative* algebra.

Examples:

i) If the field F' is a finite algebraic extension of the field F then F' is a finite dimensional simple algebra over F.

ii) $M_n(F)$, the algebra of all n by n matrices over F, is a simple algebra of dimension n^2. Its center is F.

iii) Subalgebras of $M_n(F)$.

These latter examples are typical as the following well-known representation theorem shows:

Theorem 1.1. If A is an algebra over F and $dim_F A=n$ then A is isomorphic to a subalgebra of $M_{n+1}(F)$. Moreover if A has an identity element then it is isomorphic to a subalgebra of $M_n(F)$.

This statement is easily proved using the *regular representation* of A: for each $x\in A$ we may define a linear transformation $R_x: A\to A$ as follows: $R_x(y)=xy$ for every $y\in A$. It is easy to see that the mapping R is an algebra homomorphism. If A has an identity element then R is injective.

An element $x\in A$ is *nilpotent* if $x^m=0$ for some positive integer m. An element x is *strongly nilpotent* if xy is nilpotent for every $y\in A$. The *radical* $Rad(A)$ is the set of strongly nilpotent elements of A. The algebra A is *semisimple* if it contains no strongly nilpotent elements, i.e. $Rad(A)=0$.

$Rad(A)$ is an ideal of A and $A/Rad(A)$ is a semisimple algebra. Semisimple algebras obey a very nice structure theorem due to *Wedderburn* and *Artin*: if A is a semisimple algebra over the field F then A is isomorphic to a direct sum of simple algebras:

$$A=A_1+A_2+\ldots+A_k,$$

where the A_i are the (uniquely determined) minimal ideals of A. Moreover, each A_i is isomorphic to a full matrix algebra $M_{n_i}(F_i)$ where F_i are (not necessarily commutative) fields containing F in their centers. In particular, if A is commutative then $n_i=1$, i. e. $F_i=A_i$.

L is a *Lie algebra* over the field F if L is a vector space over F equipped by an F-bilinear multiplication $[\,]$ for which the following identities are valid:

i) $[xx]=0$ for every $x\in L$

ii) $[[xy]z]+[[yz]x]+[[zx]y]=0$ for every $x, y, z\in L$.

We can define the notions *subalgebra*, *ideal*, *factoralgebra* in the usual way. The *derived series* of L is the sequence of ideals of L defined by $L^{(0)}=L, \ldots, L^{(i)}=[L^{(i-1)}L^{(i-1)}]$. L is *solvable* if $L^{(n)}=0$ for some n. It is known (Jacobson [8]) that if L is a finite dimensional Lie algebra then it has a unique maximal solvable ideal $R(L)$, the *radical* of L.

The *descending central series* of L is the sequence of ideals of L defined as $L^0=L,\ldots,L^i=[L\,L^{i-1}]$. L is called *nilpotent* if $L^n=0$ for some n. Every finite dimensional Lie algebra L contains a unique maximal nilpotent ideal $N(L)$, the *nilradical* of L (see Jacobson [8]).

Example:

If $A, B \in M_n(F)$ then we can define $[AB]$ as $[AB]=AB-BA$. It is easy to see that this operation satisfies the requiremnts i) - ii), so if L is a subspace of $M_n(F)$ and closed under the operation [ ], then it is a *linear Lie algebra.*

There is a simple, but usually not faithful representation of abstract Lie algebras as linear Lie algeras. The *adjoint representation* $ad(L)$ of a Lie algebra L is defined as the linear Lie algebra of linear transformations of $ad(x)$ of L where $x \in L$ and

$ad(x)y=[xy]$ for every $y \in L$.

We remark that a deeper result of Ado and Iwasawa [8, chapter 6] says that every finite dimensional Lie algebra is actually isomorphic to a linear Lie algebra, but we shall not need this fact.

Now we specify our input. An algebra A (associative or Lie) can be given by *structure constants.* If the elements $a_1,...,a_n$ form a (linear) basis of A, then by the distributive law, it is enough to know the elements $a_i \bigcirc a_j$, $i,j=1,...,n$, where $\bigcirc$ stands for the multiplication in question. We can express these products as linear combinations of the a_i.

$$a_i \bigcirc a_j = \sum_{k=1}^{n} \gamma_{ijk} a_k$$

for $i,j=1,...,n$. The coefficients γ_{ijk} are called the structure constants.

We also need a representation of the field F. We assume that F is a finite extension of its prime field P (P is either a field of prime order or the field of rationals). Therefore F is a finite dimensional algebra over P. Thus F can be represented by specifying the structure constants over P with respect to some basis of F over P. If $dim_P F=n$ then F is the extension of P by a single generating element α of degree n. This fact gives rise to a particularly convenient basis, $\{1,\alpha,\alpha^2, \cdots ,\alpha^{n-1}\}$. To specify the structure constants with respect to this basis one only has to list the coefficients of the minimum polynomial of α over P.

3. Controlling sizes

In this section we describe some algorithmic tools we shall extensively use in the sequel. The main purpose of the results of this section is to guarantee that the size of the numbers involved in our computations will not blow up.

The *size* $|x|$ of an object x (such as a rational or algebraic number, vector, field, algebra, element of an algebra) is the length of the string we use to encode x.

We shall solve various systems of linear equations. It is known that this task can be done in time polynomial in the input size. The proof of the following observation is a routine exercise.

Proposition 3.1. Let F be either a finite field or an algebraic number field of size K. Suppose that we have m linear equations with n variables and with

coefficients from F. Suppose further that the size of the coefficients is not greater than N. Then this system of linear equations can be solved in time polynomial in N, m, n and K. In particular, the result has size polynomial in these parameters.

Corollary 3.2. Let F and K be as above. Suppose we have subspaces $V_1,...,V_l$ of F^n represented by bases. Suppose that the size of the coordinates of these vectors is not greater than M. Then we can compute a basis of the subspace $V_1 \cap V_2 \cap ... \cap V_l$ in time polynomial in K,M,n,l. In particular, this subspace can be represented by vectors having polynomial size coordinates.

Proof. First we compute a 'dual basis' for every subspace V_i (i.e. a maximal linearly independent set of linear equations for V_i). By Proposition 3.1 this can be done in time poynomial in K,M,n,l. Then form the union U of these sets of equations and compute a 'dual basis' for U. To do this, we have to solve another linear system whose input size is polynomial in K,M,n,l, so we may use Proposition 3.1. again. It is obvious that the vectors obtained form a basis of $V_1 \cap V_2 \cap ... \cap V_l$.

We shall have to compute the minimum polynomial $minpol_a(x)$ of the element $a \in A$.

Proposition 3.3. Let A be an associative algebra with identity element over the field F, with basis $a_1,...,a_n$ and structure constants γ_{ijk}. Here F is either finite or an algebraic number field. Suppose that the description of F has size M. Suppose that $|\gamma_{ijk}| \leq K$ for every i,j,k. Let $a = \sum_1^n \lambda_i a_i$ be an element of A and suppose that $|\lambda_i| \leq N$ hold for every coefficient λ_i. Then there is an algorithm which computes $minpol_a(x)$ over F in time, polynomial in M,n,N and K. In particular, the output (and the intermediate results) have size polynomial in M,n,N and K.

Proof. (i) We successively compute the first n powers of a. This task can be done in polynomial time and the size of the coefficients remains polynomial in M,n,N and K.
(ii) We determine 1,the identity element of A.We have to solve a system of n linear equations with coefficients of size polynomial in n and K.
(iii) Finally for $i=1,2,...,n$ we test the linear independence of 1 and the first i powers of a until we find a linear dependence. In each step we solve a system of linear equations whose input is polynomial in M,n,N and K. The first linear dependence gives the coefficients of $minpol_a(x)$.

4. The radical

In this section we first sketch how finding the radical of a Lie algebra can be reduced to the associative case. Subsequently we describe the algorithm for finding the radical of an associative algebra.

4.1. Reduction of $R(L)$ to $N(L)$. In the infinite case $R(L)$ can be computed

directly, by solving a system of linear equations (cf. Beck-Kolman-Stewart [2, section 5]), derived from a classic trace condition similar to Dickson's theorem (see Theorem 4.2 below). In the finite case $R(L)$ can be computed by repeated application of an $N(L)$ procedure. The reason is that $N(L) \subset R(L)$ and $R(L) \neq 0$ implies that $N(L) \neq 0$ because the next to last term J of the derived series of $R(L)$ is an abelian (i.e $[JJ]=0$) hence a nilpotent ideal. After finding the nilradical of L, we repeat this for the factor algebra $L_1 = L/N(L)$ and so on. This process terminates when we have a Lie algebra L_i such that $N(L_i)=0$. Now L_i is isomorphic to $L/R(L)$ and we can easily poduce a basis for $R(L)$ by keeping track of the preimages of the ideals we factored out during the process.

4.2. Reduction of $N(L)$ to the associative case. A theorem of Jacobson allows us to reduce the problem of computing $N(L)$ to the problem of computing the radical in an associative algebra.

Theorem 4.1. (Jacobson [8, p.36].) Let L^* denote the associative (matix-) algebra generated by $ad(L)$. Then an element $x \in L$ is in $N(L)$ if and only if $ad(x) \in Rad(L^*)$.

This theorem shows that given $Rad(L^*)$, $N(L)$ can be computed by solving a system of linear equations.

4.3. Associative algebras: reduction to prime fields. By our assumption, the field F is a finite extension of its prime field P. Let d be the dimension of F over P and n the dimension of A over F. Then A can be viewed as an algebra of dimension nd over P. Moreover, the definition of the radical as the set of strongly nilpotent elements does not depend on the ground field. Henceforth we assume $F=P$.

4.4. Characteristic zero. If $F=Q$ then we may use the following characterization of the radical due to Dickson.

Theorem 4.2. (Dickson [6],pp. 106-108.) Let A be a subalgebra of $M_n(F)$ where $charF=0$. Then $x \in Rad(A)$ if and only if $Tr(xy)=0$ for every $y \in A$.

Corollary 4.3. Let F be a field of characteristic zero and A a matrix algebra over F. Let the elements $a_1, a_2, \ldots, a_n$ form a linear basis of A over the field F. Then $x \in Rad(A)$ if and only if $Tr(xa_i)=0$ for $i=1,\ldots,n$.

This statement shows that $Rad(A)$ can be obtained by solving a system of linear equations with small and easily computable coefficients.

4.5. Prime characteristic. This is the difficult case to which the rest of this section and the entire next section will be devoted. For this case, we had to develop an apparently new, tractable construction of the radical. Let $F=GF(p)$, $A \subseteq M_n(p)$ a matrix algebra with $dim_F A = n$ *or* $n-1$ and let l be the integer defined by the inequalities $p^l \leq n < p^{l+1}$. Let A^* denote the *set* of matrices obtained by adjoining I the identity matrix of $M_n(p)$ to A.

We shall find ideals $I_{-1}, I_0, \ldots, I_l$ and functions $g_i : I_{i-1} \rightarrow GF(p)$ for $0 \leq i \leq l$ with the

following properties:

1. $I_1=A$ and $I_l=Rad(A)$.

2. g_i is a linear function on I_{i-1}.

3. $I_i=\{\ x\in I_{i-1}\ ;\ g_i(xy)=0$ for *every* $y\in A^*\ \}$.

4. $g_i(x)$ can be computed in time polynomial in n and $log(p)$ for every $x\in A$.

These properties immediately show that if a basis of I_{i-1} is given then a basis of I_i can be obtained by solving a system of linear equations over $GF(p)$. The coefficients of these equations can be obtained in polynomial time and we obtain the radical after $l\leq log(n)$ such steps.

In order to compute $g_i(x)$ we shall under certain circumstances *divide mod p residue classes by p.* More precisely, the function g_i is defined as follows. Let X be an integral matrix and $x=X\ mod\ p$. Compute the integer $u=Tr(X^{p^i})$. It will turn out that for $x\in I_{i-1}$ this number will be divisible by p^i. Let $g_i(x) = u/p^i\ \ mod\ p$.

This somewhat mysterious definition clearly justifies the above claim of fast computability but it leaves a lot to be proved. The justification follows in the next section.

5. Approximating the radical

In this section we prove the claims made in the previous section.

Let p denote a prime number and n a positive integer. Let M_n and $M_n(p)$ denote the rings of all n by n matrices over the integers Z and over the p-element field Z_p, respectively. ϕ will denote the ring homomorphism from M_n to $M_n(p)$ induced by the $Z\rightarrow Z_p$ epimorphism.

Matrices over Z will be denoted by capitals (A,B,X,Y); the corresponding l. c. letters will indicate matrices over Z_p.

We want to speak about $Tr(a^{p^i})mod(p^{i+1})$ where $a\in M_n(p)$ simply by choosing an arbitrary matrix $A\in M_n$ for which $\phi(A)=a$ and taking $Tr(A^{p^i})mod(p^{i+1})$. This procedure is justified by the following lemma.

Lemma 5.1. If $A\equiv B\ \ mod\ p$ where $A,B\in M_n$ and i is an arbitrary nonnegative integer then

$$Tr(A^{p^i})\equiv Tr(B^{p^i})\ mod\ (p^{i+1}).$$

Proof. Let $P=B-A$. Here every entry of the integral matrix P is divisible by p. First we notice that if $B_1,\ldots,B_k$ are integer matrices and m of them equal P then every element of the product matrix $B=B_1B_2\ldots B_k$ is divisible by p^m. In particular, $Tr(B)\equiv 0 mod(p^m)$.

Now if we expand the left hand side of the stated congruence we obtain

$$Tr(B^{p^i})=Tr((A+P)^{p^i})=\sum Tr(Z_1Z_2\ldots Z_{p^i})$$

where $Z_i=A$ or $Z_i=P$ and the summation ranges over all the 2^{p^i} such products. If $G=<\pi>$ denotes the cyclic group of order p^i then we may define an action of G on these words by setting

$$\pi(Z_1Z_2\ldots Z_{p^i})=Z_{p^i}Z_1\ldots Z_{p^i-1}.$$

i.e. π acts as a cyclic shift. Clearly if V and W are two products from the same G-orbit then $Tr(V)=Tr(W)$ because $Tr(XY)=Tr(YX)$ for any $X, Y\in M_n$. If the orbit of the product V has p^j elements then the contribution of this orbit to the sum is $p^jTr(V)$. But, in this case π^{p^j} leaves V fixed, i.e. V can be obtained as the p^{i-j}-th power of the product of its first p^j factors.
If V is not A^{p^i} then at least p^{i-j} of the matrices Z_k is P. Now using the trivial inequality $p^{i-j}\geq i-j+1$, we conclude that every element and hence the trace of V is divisible by p^{i-j+1} and the contribution of the orbit is divisible by p^{i+1}. On the other hand A^{p^i} forms a one element orbit, proving the Lemma.

The following result provides a tool for inductive proofs.

Lemma 5.2. Let H be a multiplicatively closed subset of M_n, and k a positive integer and suppose that $Tr(X^{p^i})$ is divisible by p^{i+1} for every $X\in H$ and $0\leq i<k$. Then for every $X,Y\in H$

$$Tr((X+Y)^{p^k})\equiv Tr(X^{p^k})+Tr(Y^{p^k})\ mod\ (p^{k+1}).$$

Proof. We expand the left hand side of the congruence as in Lemma 5.1 and obtain that

$$Tr((X+Y)^{p^k})=\sum Tr(Z_1Z_2\ldots Z_{p^k})$$

where $Z_i=X$ or $Z_i=Y$ and the summation ranges over all of the 2^{p^k} such products. Again, we consider the orbits of the cyclic shifts. If the orbit of the product V has p^j elements then the contribution of this orbit to the sum is $p^jTr(V)$. But, in this case, as in Lemma 5.1, the matrix V can be obtained as the p^{k-j}-th power of the product of its first p^j factors. Using our assumption, if $j\neq 0$ then $Tr(V)$ is divisible by p^{k-j+1} .On the other hand, $V\in H$ thus the sum of the orbit is divisible by p^{k+1}. The one-element orbits correspond to the right hand side of the congruence.

Let now F be a field and $f\in F[x]$ a monic polynomial:

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n.$$

If $\alpha_1,\alpha_2,\ldots,\alpha_n$ are the roots of f (in an appropriate extension of F) then let

$$s_i=\sum_{j=1}^n\alpha_j^i$$

for $i=1,2,...,n$. The elements s_i can be expressed by $a_1,a_2,...,a_n$ using the well-known Newton - Girard identities:

$$s_1+a_1=0$$

$$s_2+a_1s_1+2a_2=0$$

$$s_3+a_1s_2+a_2s_1+3a_3=0$$

$$\vdots$$

$$s_n+a_1s_{n-1}+...+a_{n-1}s_1+na_n=0.$$

The next two results establish a trace condition for nilpotence.

Lemma 5.3. Let H be a multiplicatively closed subset of M_n and suppose that for every $X\in H$, $Tr(X^{p^l})$ is divisible by p^{l+1} where l is defined by the inequalities $p^l \leq n < p^{l+1}$. Then $\phi(X)$ is nilpotent for every $X\in H$.

Proof. It suffices to prove that $\phi(X)^{p^l}=\phi(X^{p^l})$ is nilpotent. If f is the characteristic polynomial (with leading coefficient one) of $Y=X^{p^l}$ over the rationals then $\phi(Y)$ is nilpotent if and only if every a_i is divisible by p. We shall use the Newton - Girard identities for the polynomial f. Using the fact that $s_i=Tr(Y^i)=Tr((X^i)^{p^l})$ and $X^i\in H$ we conclude that s_i is divisible by p^{l+1}. Now from the Newton - Girard formulae we obtain that

$$ia_i\equiv 0 \ mod(p^{l+1}) \qquad \text{for every } 0<i\leq n.$$

On the other hand, from the definition of l it follows that i is not divisible by p^{l+1} hence a_i is divisible by p, and the statement follows.

Lemma 5.4. Let $X\in M_n$ be a matrix for which $\phi(X)$ is nilpotent. Then for every $i\geq 0$

$$Tr(X^{p^i})\equiv 0 mod\,(p^{i+1}).$$

Proof. If $\phi(X)$ is nilpotent then it is similar (over Z_p) to a strictly upper triangular matrix. Or, in terms of integer matrices, there exist $A,B,P,R,U\in M_n$ such that if I is the identity matrix in M_n then

$$AXB=U+P \ , \ BA=I+R \ , \ U^n=O \text{ and}$$

$$\phi(P)=\phi(R)=O \ .$$

Now using Lemma 5.1

$$0=Tr(U^{p^i})\equiv Tr((U+P)^{p^i})=Tr((AXB)^{p^i})$$

where the congruence is $mod(p^{i+1})$. Similarly,

$$Tr((AXB)^{p^l})=Tr((BAX)^{p^l})=Tr((X+RX)^{p^l}).$$

Observing that $\phi(RX)=O$, we may use Lemma 5.1 again and we obtain that

$$Tr((X+RX)^{p^l})\equiv Tr(X^{p^l}) \ mod(p^{i+1}).$$

Combining these equalities and congruences we see that

$$Tr(X^{p^l})\equiv 0 mod\,(p^{i+1}).$$

Now suppose that A is a subalgebra of $M_n(p)$. Our aim here is to construct a descending chain of ideals of A,
$A=I_{-1}\supseteq I_0\supseteq\cdots\supseteq I_l=Rad(A)$
such that given I_i the ideal I_{i+1} is computable in time polynomial in n and $\log p$.
For $0\leq i\leq l$ let

$$I_i=\{\ x\in A\ ;\ Tr((xy)^{p^l})\equiv 0 mod(p^{j+1}) \text{ for every } y\in A^* \text{ and for every } 0\leq j\leq i\ \}.$$

For the definition of A^* see section 4.5. We remark that for $u\in A$ the residue $Tr(u^{p^l})mod(p^{j+1})$ is $Tr(U^{p^l})mod(p^{j+1})$ where U is an arbitrary integer matrix for which $\phi(U)=u$. (See Lemma 5.1.)

From the definition it is immediate that

$$A=I_{-1}\supseteq I_0\supseteq\ldots\supseteq I_l.$$

Using our lemmas, we can prove the following:

Theorem 5.5. *I_k is an ideal of A for every k $(-1\leq k\leq l)$ and $I_l=Rad(A)$.*

Proof. I_{-1} is obviously an ideal, so we may suppose that $k\geq 0$. If $x\in I_k$ and $u\in A^*$ then obviously $xu\in I_k$. In order to prove $ux\in I_k$ we observe that

$$Tr(((UX)Y)^{p^l})=Tr((X(YU)^{p^l}).$$

Now we have to prove that I_k is an additive subgroup of A. This is true for I_0 because Tr is a linear function. So we may suppose that $k>0$. As I_k is multiplicatively closed, the same is true for its preimage J_k in M_n:

$$J_k=\{\ X\in M_n\ ;\ \phi(X)\in I_k\ \}.$$

We shall apply Lemma 5.2 for $H=J_k$. Let $X,Y\in J_k$ and for and $U\in M_n$ such that $\phi(U)\in A^*$. Now for any $0\leq j\leq k$ we have

$$Tr(((X+Y)U)^{p^l})=Tr((XU+YU)^{p^l})\equiv$$
$$\equiv Tr((XU)^{p^l})+Tr((YU)^{p^l})\equiv 0 \ mod(p^{j+1}).$$

The last congruence follows from

$$Tr((XU)^{p^l})\equiv 0 \ mod(p^{j+1})$$

and

$$Tr((YU)^{p^i})\equiv 0 \ mod(p^{i+1}).$$

Finally we show that $I_l=Rad(A)$. Indeed, if $x\in Rad(A)$ then xy is nilpotent for every $y\in A^*$. If U is an arbitrary integral matrix for which $\phi(U)=xy$ then U is nilpotent $mod(p)$ and from Lemma 5.4 we obtain that

$$Tr((xy)^{p^i})\equiv 0 mod(p^{i+1})$$

for every $i\geq 0$, i.e. $x\in I_l$. The reverse containment immediately follows from Lemma 5.3 if we define H to be $H=J_l$ and the proof is complete.

For $0\leq i\leq l$ we define the function $f_i : M_n\to Q$ by

$$f_i(X)=\frac{Tr(X^{p^i})}{p^i}.$$

Let

$$J_i = \{X\in M_n | \phi(X)\in I_i\}.$$

If $X\in J_{i-1}$ then $f_i(X)$ is an integer and if $X,Y\in J_{i-1}$ then

(1) $\quad f_i(X+Y)\equiv f_i(X)+f_i(Y) \ mod(p).$

Indeed, if $i=0$ then this is immediate and if $i>0$ then we may use Lemma 5.2.

Now for $0\leq i\leq l$ we define the functions $g_i : I_{i-1}\to Z_p$ as follows:

$$g_i(x)=f_i(X) \ mod(p)$$

where X is an arbitrary integer matrix for which $\phi(X)=x$. The definition is obviously unambiguous if $i=0$. To see this for $i>0$, let X,Y integral matrices for which $\phi(X)=\phi(Y)=x$ then Lemma 5.1. implies that

$$Tr(X^{p^i})\equiv Tr(Y^{p^i}) mod(p^{i+1}).$$

But now $X,Y\in J_{i-1}$, so p^i divides $Tr(X^{p^i})$ and $Tr(Y^{p^i})$ hence

$$\frac{Tr(X^{p^i})}{p^i}\equiv\frac{Tr(Y^{p^i})}{p^i} mod(p).$$

Now we summarize these facts in the following:

Theorem 5.6.
(i) The functions g_i are Z_p-linear on I_{i-1} for every $0\leq i\leq l$.
(ii) $\quad I_i=\{ x\in I_{i-1};\ g_i(xy)=0$ *for every* $y\in A^* \}$.

Proof. (i) Immediate consequence of (1).
(ii) This is a simple reformulation of the definition of I_i. Indeed, $g_i(xy)=0$ if and only if $Tr((xy)^{p^i})$ is divisible by p^{i+1}.

Theorems 5.5. and 5.6. together with our remarks in Subsection 4.5 immediately imply the following result.

Theorem 5.7. Let A be an associative algebra of dimension n over the field $GF(p)$ given by structure constants. Then we can compute a basis of $Rad(A)$ in time polynomial in n and $\log p$.

Proof. First we compute the regular representation of A (cf. Theorem 2.1). Now we have a matrix algebra over $GF(p)$ and we can successively determine the ideals I_j by solving systems of linear equations over $GF(p)$.

6. Fields, polynomials, commutative algebras

In this section we establish effective versions of some the basic facts from algebra needed for the decomposition of semisimple associative algebras. First we deal with fields of characteristic zero. Q will denote the field of rational numbers. If α is an element of an algebra over the field F then $minpol_\alpha(x)$ will denote the defining polynomial of α (i.e. the smallest degree polynomial $f\in F[x]$ with leading coefficient 1 for which $f(\alpha)=0$). The field F in consideration will be clear from the context.

Proposition 6.1. Let F,F' be isomorphic (field-) extensions of the field Q. Suppose that we have elements $a_1,a_2,\ldots,a_n\in F$ and $b_1,b_2,\ldots,b_n\in F'$ such that

a) $lin_Q<a_1,\ldots,a_n>=F$ and

$lin_Q<b_1,\ldots,b_n>=F'$

b) there is no field isomorphism $\phi: F\to F'$ for which

$\phi(a_i)=b_i$ for every $i=1,2,\ldots,n$.

Then there exist integers $\alpha_1,\ldots,\alpha_n$ such that $0\leq\alpha_i\leq 2n$ and over the field Q

$$minpol_{\sum_1^n\alpha_ia_i}(x)\neq minpol_{\sum_1^n\alpha_ib_i}(x).$$

Proof. By contradiction. If the assertion is false then for every such choice of the integer vector $\vec{\alpha}=(\alpha_1,\ldots,\alpha_n)$ there is an isomorphism ϕ (depending on $\vec{\alpha}$) for which $\phi(\sum_1^n\alpha_ia_i)=\sum_1^n\alpha_ib_i$. In this case we say that the isomorphism ϕ belongs to the vector $\vec{\alpha}$. We choose a prime p, $2n\geq p>n$ and consider the vectors $\vec{\alpha}$ for which $0\leq\alpha_i<p$ hold for $i=1,\ldots,n$. As $dim_QF=dim_QF'\leq n$, there are at most n isomorphisms from F to F'. By our hypothesis, as every $\vec{\alpha}$ has at least one isomorphism belonging to it, there is an isomorphism ϕ which belongs to at least $\frac{p^n}{n}>\frac{p^n}{p}=p^{n-1}$

of these vectors. Every proper subspace has at most p^{n-1} elements, therefore these vectors cannot be in a proper subspace modulo p. So we may suppose that ϕ belongs to the modulo p independent vectors $\vec{\alpha}^1, \ldots, \vec{\alpha}^n$. These vectors are linearly independent over Q as well. Using the fact that

$$\phi: \sum_{i=1}^n \alpha_{ji} a_i \rightarrow \sum_{i=1}^n \alpha_{ji} b_i \qquad j=1,\ldots,n$$

we obtain the following system of linear equations

$$\sum_{i=1}^n \alpha_{ji}(\phi(a_i)-b_i)=0 \qquad \text{for } j=1,\ldots,n$$

the matrix of which is nonsingular. This implies that $\phi(a_i)=b_i$ for every $i=1,\ldots,n$, a contradiction.

It is a well known fact that finite extensions of fields of characteristic zero can be generated by a single element. The next proposition is an effective version of this.

Proposition 6.2. Let F be an algebraic number field with $dim_Q F=n$ and let $a_1,\ldots,a_m$ be a generating set of F over the rationals. Then there exist integers $\alpha_1, \ldots, \alpha_m$, $0 \leq \alpha_i \leq n^2$ such that $F=Q(\sum_1^m \alpha_i a_i)$.

Proof. The textbook proof of the theorem on simple extensions immediately gives the following fact.
If $Q(a)$ and $Q(b)$ are two simple algebraic extensions of Q with respective dimensions k,k' over Q then there exists an integer α, $0 \leq \alpha \leq kk'$ such that $Q(a,b)=Q(a+\alpha b)$.
Now let $F_i=Q(a_1,\ldots,a_i)$. Observing that $dim_Q F_i \leq n$ and $dim_Q Q(a_{i+1}) \leq n$, the result follows by induction on i.

The next corollary will guarantee that if A is isomorphic to a direct sum of algebraic number fields then A has "small" zero divisors.

Corollary 6.3. Let F,F^* be algebraic number fields. Suppose $a_1,\ldots,a_n$ is a linear generating set of F over Q and similarly let $b_1, \ldots, b_n$ be a linear generating set of F^*. Suppose further that there is no isomorphism $\phi : F \rightarrow F^*$ such that $\phi(a_i)=b_i$ for every $1 \leq i \leq n$. Then there exist integers $\alpha_1, \ldots, \alpha_n$, $0 \leq \alpha_i \leq max(n^2, 2n)$ such that

$$minpol_{\sum \alpha_i a_i}(x) \neq minpol_{\sum \alpha_i b_i}(x).$$

Proof. If F is not isomorphic to F^* then one of them (say F) is not isomorphic to a subfield of the other. By Proposition 6.2 there exists $a=\sum_1^n \alpha_i a_i \in F$ for which $F=Q(a)$ and $0 \leq \alpha_i \leq n^2$. Using these coefficients α_i the assertion follows in this case. If F is isomorphic to F^* then Proposition 6.1. gives the desired result.

Now suppose that A is a *semisimple commutative algebra* over the field F. Let $A=A_1+A_2+\ldots+A_k$ be the Wedderburn - Artin decomposition of A where the summands are fields and they are the minimal ideals of A. Every element b of A can uniquely be represented as

$$b=b_1+b_2+\ldots+b_k$$

where $b_j\in A_j$. In particular, we can represent the basis elements a_i as $a_i=a_{i1}+a_{i2}+\ldots+a_{ik}$ where a_{ij} belongs to A_j. A is a finite dimensional algebra over F,so every $b\in A$ is algebraic over F. As A is semisimple and commutative, it does not contain nilpotent elements. This immediately implies that $minpol_b(x)$, the minimum polynomial of b over F, has no multiple factors over F. The following two propositions establish a connection between factoring polynomials and decomposing algebras. They state well known facts. We include their proofs here because they contain ideas essential for our decomposition method.

Proposition 6.4. Let p be a polynomial with coefficients from F, A, b, b_i as above. Then
(i) $minpol_b(x)=$ l.c.m.$(minpol_{b_1}(x),\ldots,minpol_{b_k}(x))$.
(ii) If $p(b_i)$ is not zero then the ideal $p(b)A$ contains A_i.
(iii) If $p(b_i)=0$ then $p(b)A$ does not contain A_i.

Proof: (i) A is a direct sum of the subspaces A_i, hence $b=0$ if and only if $b_i=0$ for every i. The direct summands are ideals, thus if $x\in A_i$, $y\in A_j$ and $i\neq j$ then $xy=0$. The latter implies that for any polynomial p , $p(b)=\sum_1^k p(b_i)$, so $p(b)=0$ if and only if $p(b_i)=0$ for every i. Now the statement follows immediately.
(ii) $0\neq p(b)p(b_i)\in A_i$ and A_i is a minimal ideal.
(iii) For each $x\in A$ the i-th component of $xp(b)$ is 0.

Proposition 6.5. Let A be as above. Let $b\in A$ and suppose that $minpol_b(x)=f(x)g(x)$ where $f,g\in F[x]$ nonconstant relatively prime polynomials. Then A can be decomposed as a direct sum of ideals $A=I+J$ where $I=f(b)A$ and $J=g(b)A$. Moreover these ideals also have identity elements.

Proof. It is immediate that I and J are ideals and $f(b)\neq 0, g(b)\neq 0$ imply that $I\neq(0)$ and $J\neq(0)$. Now let $u,v\in F[x]$ such that $fu+gv=1$. Then

$$f(b)u(b)+g(b)v(b)=1 \tag{2}$$

holds (here 1 is the identity element of A). First we observe that $e=f(b)u(b)$ is the identity element of I. Indeed, $e\in I$ and multiplying (2) by $f(b)$ we obtain $ef(b)=f(b)$. If $x\in I$ then $x=f(b)y$ for some $y\in A$ and $ex=ef(b)y=f(b)y=x$. Similarly, $d=g(b)v(b)$ is the identity element of J. Now using the fact that $de=0$ we deduce that if $x\in I\cap J$ then $x=ex=edx=0$ hence $I\cap J=(0)$. Finally if $x\in A$ then from (2) we obtain that $ex+dx=x$, where the fist term is from I and the second is from J, i.e. I and J generate A. The proposition is proved.

7. Semisimple associative algebras

7.1. Reduction to the commutative case. If A is a semisimple associative algebra then first we compute B, the center of A. A basis of B can be obtained

by solving a system of linear equations. The center is a commutative semisimple algebra, more precisely, it is a direct sum of fields.

Suppose that we are able to find the Wedderburn-Artin decomposition of B to its simple components (fields B_i):

$$B=B_1+B_2+...+B_k.$$

Then it is easy to see that A is the direct sum of the simple ideals B_iA , $i=1,2,...,k$ and these components can be computed effectively.

7.2. Finding the decomposition over Q

In this section we outline a deterministic polynomial time algorithm that computes the minimal ideals of a given semisimple commutative algebra over Q. Let A be a semisimple commutative algebra over Q, with basis $a_1,...,a_n$ and structure constants γ_{ijk} .Suppose that $|\gamma_{ijk}|\leq K$ for every i,j,k.
Let $A_1,A_2,...,A_k$ denote the minimal ideals of A. Every element $b\in A$ can be uniquely represented as a sum

$$(3) \qquad b=b_1+b_2+...+b_k$$

where $b_i\in A_i$. In particular, we can represent the basis elements of A as

$$a_i=a_{i1}+a_{i2}+...+a_{ik} \qquad a_{ij}\in A_j$$

For any fixed j the elements $a_{1j},a_{2j},...,a_{nj}$ generate A_j as a linear subspace.
Let $e_1,e_2,...,e_k$ denote the primitive idempotents of A (i.e. the identity elements of the fields $A_1,A_2,...,A_k$). We can express them as rational linear combinations of $a_1,...,a_n$:

$$e_i=e_{i1}a_1+e_{i2}a_2+...+e_{in}a_n.$$

First we prove that the result of the decomposition process can be represented in polynomial size.

Proposition 7.1. The coefficients e_{ij} have size polynomial in n and K.

Proof: Without loss of generality we may assume that $i=1$. For each $r,r=2,...,k$, there exists an element b (depending on r) such that
i) the coefficients of b are polynomially bounded in n and
ii) if we consider the representation (3) of b then $minpol_{b_1}(x)$ and $minpol_{b_r}(x)$ are different.
Indeed, we use Cor. 6.3 for the fields A_1, A_r and for their linear generating sets $a_{11},...,a_{1n}$ and $a_{r1},...,a_{rn}$ respectively. As A_1 and A_r are fields, these are different irreducible polynomials over Q. Now we notice that if p_r denotes $minpol_{b_r}(x)$ then then $p_r(b_1)$ is not zero,hence the ideal $B_r=p_r(b)A$ contains A_1 but it does not contain A_r, by Prop. 6.4. On the other hand from Cor. 6.3 it follows that $p_r(x)$ is a factor of $minpol_b(x)$ so it has "small" coefficients (in terms of n and K) hence $p_r(b)$

and B_r can be represented by vectors with small coordinates. As $A_1=B_2\cap B_3\cap...\cap B_k$, A_1 can also be represented by small vectors. e_1 is the identity element of A_1 hence it can be obtained by solving the system of linear equations:

$$e_1c_1=c_1$$
$$\vdots$$
$$e_1c_l=c_l$$

where the elements $c_1,...,c_l$ form a Q-basis of A_1. The size of input is polynomial in n and K thus the coefficients $e_{11},...,e_{1n}$ are small as we wanted to show.

Corollary 7.2. Every idempotent of A has coefficients of size polynomial in n and K.

Proof. Every idempotent is a sum of at most n primitive idempotents. Now using Prop. 7.1 the statement follows.

Corollary 7.3. Suppose that I is an ideal of the algebra A and that I is given by a Q-linear basis $c_1,c_2,...,c_l$. Suppose that the size of the coefficients of c_i (with respect to the basis $a_1,...,a_n$) is bounded by N. Then there is a polynomial $p(x,y)$ and an algorithm (called *REDUCTION*() in the sequel) which runs in time polynomial in n, N and K and computes another basis of I. Moreover the coefficients of the new basis vectors have size less than $p(n,K)$.

Proof. The procedure *REDUCTION*(I) runs as follows:
i) First we compute e the identity element I as in Prop.7.1. This part of the algorithm runs in time, polynomial in n, N and K.
ii) Now, using the fact that $I=eA$, we select a maximal linearly independent set from the elements $ea_1,ea_2,...,ea_n$. These vectors obviously form a Q-basis of I and using Cor. 7.2 we obtain the result stated. We remark that this part of the algorithm also runs in time, polynomial in n and K.

Bases obtained via procedure *REDUCTION*() will be referred as ***standard*** bases.

To obtain succint representations of the intermediate fields we may encounter, we develop a simple procedure *PRIMELEM*() which computes a single generating element of a subfield of A. The subfield is given by two generating elements.
The input of *PRIMELEM*() is a Q-algebra A, and two elements $a,b\in A$ for which $Q(a,b)$ is a field. These elements are given as linear combinations of the basis vectors of A. The procedure outputs an element $c=a+\alpha b$ for which $Q(c)=Q(a,b)$ and α is an integer and $0\leq\alpha\leq n^2$. We shall employ an auxiliary integer variable j.

procedure *PRIMELEM*(A,a,b)

begin

j:=0;

for k=0 **to** n^2 **do begin**

Step 1. compute f the minimal polynomial of $a+kb$

Step 2. if $deg(f)>j$ then $j:=deg(f)$;

end for

return$(a+jb)$;

end procedure

Proposition 7.4. *PRIMELEM* is correct and terminates in time polynomial in the input size.

Proof. As we remarked in the proof of Prop. 6.2, such an element c exists. We know that for each k, $Q(a+kb)\subseteq Q(a,b)$, and $Q(a+kb)=Q(a,b)$ if and only if $dim_Q Q(a+kb)=dim_Q Q(a,b)$. But $dim_Q Q(a+kb)=deg(f)$, thus c generates $Q(a,b)$ if and only if $minpol_c(x)$ has maximal degree. From Prop. 3.3 it follows that *PRIMELEM* runs in time, polynomial in the input size.

Now we are in the position to describe our main subroutine *SPLIT*1(). Its input is a semisimple commutative algebra A and an ideal I of A given by a linear basis over Q. It tests whether I is indecomposable or not. In the latter case it finds a proper decomposition of I as a direct sum of ideals $I=I_1+I_2$ and returns a standard basis of I_1 and a standard basis of I_2. As mentioned in the Introduction, the algorithm will use a procedure for factoring over Q and its finite extensions. Such polynomial time algorithms exist (Lenstra-Lenstra-Lovász [12], Chistov-Grigoryev [5], Landau [10], A. K. Lenstra [11]).

procedure *SPLIT*1(A,I)

begin

Step 1.initialize variables $b_1,...,b_k$ to be the given basis vectors of I and let $var=1$ i.e. the identity element of I;

for $i:=1$ **to** k **do begin**

Step 2. compute f, the minimal polynomial of b_i over the field $Q(var)$;

Step 3. find the irreducible factors of f over $Q(var)$ using an appropriate factoring algorithm;

Step 4. **if** $f=gh$ is a proper factorization **then** return ideals *REDUCTION*$(Ag(b_i))$ and *REDUCTION*$(Ah(b_i))$ **else** let $var:=$*PRIMELEM*(A, var, b_i);
(* by semisimplicity, f cannot have multiple factors *)

end

Step 5. return the message " I is a field ";

end

Proposition 7.5. Suppose that I is represented by basis vectors whose coordinates have size less than N. Then *SPLIT*1 is correct and runs in time, polynomial in n, N, K.

Proof. First we notice that in each step I contains the field $Q(var)$ as a subalgebra (actually,I is an algebra over $Q(var)$) and if we passed the i-th cycle then $Q(var)$ contains the elements $b_1,b_2,...,b_i$ and if we terminate at Step 5 then I is a field. >From Prop. 6.5 it follows that if we terminate at Step 4 then *SPLIT*1 gives a proper decomposition of I, otherwise I is a field. The correctness is proved. As $k \leq n$, it is enough to show that each step takes only polynomial amount of time. This follows immediately from Prop. 3.3, Prop. 7.4, Cor. 7.3 provided that we have a polynomial bound on the sizes of elements stored in variable *var*. But these elements are always of the form $l_1b_1+l_2b_2+...+l_kb_k$ where the coefficients l_i are rational integers and for each i $|l_i| \leq n^2$.

Now we describe our program *MAIN*1(). The input of the program is an algebra A given by structure constants γ_{ijk} , where $i,j,k=1,...,n$. Its output is a list *MINID* whose elements are the minimal ideals of A represented by standard bases. It uses an auxiliary list *ID* which consist of the ideals to be decomposed and an auxiliary variable *id* of type "ideal".

program *MAIN*1(A)

begin

Step 1. initialize two empty lists *ID* and *MINID* respectively;

Step 2. put A on the list *ID*;

Step 3. **while** *ID* is not empty **do begin**

a) *id*:=first element of *ID*;

b) call *SPLIT*1(A,*id*);

c) **if** *id* was a field **then** put it on the list *MINID*;

d) **if** *SPLIT*1 returned two ideals **then** put them on the list *ID*;

end while

end program

Theorem 7.6. Let A, n, K be as above.Then *MAIN*1 gives us the Artin -

Wedderburn decomposition of A in time polynomial in n and K.

Proof. After each pass of the while loop we either get a minimal ideal of A or obtain a finer decompositon of A (the ideals on the two lists form a direct decomposition of A), so there are at most $2n-1$ passes. We have to prove only that each step takes a polynomial amount of time and this is immediate except for step b). The ideals in consideration are always stored by reduced bases so by Cor. 7.3 they have size polynomial in n and K and the rest of the statement follows from Prop. 7.5.

7.3. Finding the decomposition over finite fiels

As in the infinite case, it is enough to find the Wedderburn-Artin decomposition over the prime field, so we may suppose that A is an n dimensional algebra over the field $F=GF(p)$ for some prime p. The algebra A is given by structure constants γ_{ijl} where $\gamma_{ijl}\in F$ and $i,j,l=1,...,n$. We remark that in this case all subspaces of A have small representation in terms of $\log(p)$ and n, so we don't need procedures like *REDUCTION*. We may begin with *SPLIT*2(), the finite counterpart of *SPLIT*1().
The input of *SPLIT*2 is a pair A, I, where I is an ideal of A and it returns either
i) a proper direct sum $I=I_1+I_2$ or
ii) a message saying that I is a field.
The procedure uses an auxiliary variable *field* which stores a subfield of B given by a basis and structure constants over the prime field. We include here an informal description of *SPLIT*2. It is very similar to *SPLIT*1 except it is simpler because we don't have to worry about the size of representations of fields and subspaces constructed. It also employs a factoring procedure over finite fields. For example it may use the Las Vegas methods of Berlekamp [3], or Rabin [13] with expected running time polynomial in n and $log(p)$ or the deterministic algorithm of Berlekamp (cf. [3] and [9, section 4.6.2]) with running time polynomial in n and p.

procedure *SPLIT*2(A, I)

begin

Step 1.initialize variables $b_1,...,b_k$ to be the given basis vectors of I and let *field*:=F, the ground field of I;

(* I has an identity element, so we may suppose that it contains F *)

for i:=1 **to** k **do begin**

Step 2. compute f, the minimal polynomial of b_i over the field *field*;

Step 3. find the irreducible factors of f over *field* using an appropriate factoring algorithm;

Step 4. **if** $f=gh$ is a nontrivial factorization **then** return bases of ideals $Ig(b_i)$ and $Ih(b_i)$ **else** let $field:=field(b_i)$;
(* by semisimplicity, f cannot have multiple factors *)

end

Step 5. return the message " I is a field ";

end

Proposition 7.7. Procedure *SPLIT*2 is correct. It is either a polynomial time Las Vegas algorithm (polynomial in $log(p)$ and n, i.e. in the size of the input), or a deterministic algorithm, polynomial time in p and n, depending on the factoring method employed.

Proof. We notice that if we passed the i-th cycle then the field *field* contains the elements $b_1,...,b_i$. This implies that if we terminate at Step 5. then I is a field. From Prop. 6.5 it follows that if we terminate at Step 4. then we have a proper decomposition. The correctness is proved.
Step 3 runs in expected time, polynomial in n and $\log(p)$, or deterministic polynomial time in n and p depending on the factoring method we use. Prop. 3.3 implies that Step 2 runs in time, polynomial in n and $log(p)$. We can compute either a basis for $field(b_i)$ at Step 4. using a basis of *field* or bases for the ideals $Ig(b_i)$, $Ih(b_i)$ in time polynomial in n and $log(p)$. Observing that there are at most n cycles, the proposition is proved.

We have established a procedure which finds a proper decomposition into two direct summands if this is possible (i.e. if I is not a field). We can use this procedure to find the Wedderburn-Artin components in the same way as we did in the infinite case. Actually the same program *MAIN* will do the job if we replace *SPLIT*1 with *SPLIT*2. We summarize the results of this subsection in the following:

Theorem 7.8. There exists a Las Vegas algorithm for finding the Wedderburn-Artin decomposition of a finite dimensional commutative semisimple algebra A over a finite field $F=GF(q)$ in time polynomial in $dim_F A$ and $log(q)$.
Moreover the above problem can be solved deterministically in time, polynomial in $dim_F A$,p and m where $p=charF$ and $q=p^m$.

Proof. Using Prop. 7.7 in place of Prop. 7.5, we can conclude as in Theorem 7.6.

8. Fields given by oracles

Some of the above results extend to fields given by appropriate oracles. Suppose that we have an associative algebra A over the field of quotients of an integral domain D of characteristic zero. Let $l(x)$ denote the input length of an $x\in D$ in the given representation of D. Suppose that the following inequalities hold

for the length function l (see also Borodin-Cook-Pippenger [4]):
$l(x-y) \leq max\{ l(x), l(y)\} + O(1)$ and
$l(xy) \leq l(x) + l(y) + O(\log \max\{ l(x), l(y) \})$
for every $x,y \in D$. If we have oracles for subtraction and multiplication in D then we have a polynomial time oracle algorithm to compute $Rad(A)$. The main reason for this is that under these conditions we can effectively solve systems of linear equations, so we can use Cor. 4.3 as in the case of algebraic number fields.

REFERENCES

[1] L. Babai, W. M. Kantor, E. M. Luks, *Computational complexity and the classification of finite simple groups,* Proc. 24th IEEE Symp. Found. Comp. Sci., Tucson, Arizona, 1983, 162-171.

[2] R. E. Beck, B. Kolman, I. N. Stewart, *Computing the structure of a Lie algebra,* Computers in nonassociative rings and algebras, Academic Press, New York-San Francisco-London, 1977, 167-188.

[3] E. R. Berlekamp, *Factoring polynomials over large finite fields,* Math. Comp. 24 (1970), 713-715.

[4] A. Borodin, S. Cook, N. Pippenger, *Parallel computation for well-endowed rings and space-bounded probabilistic machines,* Information and Control 58 (1983), 113-136.

[5] A. L. Chistov, D. Yu. Grigoryev, *Polynomial-time factoring of the multivariable polynomials over a global field,* LOMI preprint, Leningrad 1982. (to appear in J. of Symbolic Computation)

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

[7] I. N. Herstein, *Noncommutative rings,* Math. Assoc. of America, 1968.

[8] N. Jacobson, *Lie algebras,* John Wiley, New York-London, 1962.

[9] D. E. Knuth, *The art of computer programming, Vol. 2, Seminumerical algorithms,* Addison-Wesley, Reading, 1981.

[10] S. Landau, *Factoring polynomials over algebraic number fields is in polynomial time,* SIAM J. Comp., 1985, to appear

[11] A. K. Lenstra, *Factoring polynomials over algebraic number fields,* in: Proc. Eurocal'83, Springer Lect. Notes in Comp. Sci. vol. 162, 245-254.

[12] A. K. Lenstra, H. W. Lenstra, L. Lovász, *Factoring polynomials with rational coefficients,* Math. Ann. 261 (1982), 515-534.

[13] M. O. Rabin, *Probabilistic algorithms in finite fields,* SIAM J. Comp. 9 (1980), 273-280.