comput complexity 3 (1993), 245–261 1016-3328/93/030245-17 $1.50+0.20

FINDING MAXIMAL ORDERS IN SEMISIMPLE ALGEBRAS OVER Q

Gábor Ivanyos and Lajos Rónyai

Abstract. We consider the algorithmic problem of constructing a maximal order in a semisimple algebra over an algebraic number field. A polynomial time ff-algorithm is presented to solve the problem. (An ff-algorithm is a deterministic method which is allowed to call oracles for factoring integers and for factoring polynomials over finite fields. The cost of a call is the size of the input given to the oracle.) As an application, we give a method to compute the degrees of the irreducible representations over an algebraic number field K of a finite group G, in time polynomial in the discriminant of the defining polynomial of K and the size of a multiplication table of G.

Subject classifications. 68Q40, 11Y40, 68Q25, 11Y16.

1. Introduction

Let R be a Dedekind domain, K be the field of quotients of R and let $\mathcal{A}$ be a finite dimensional semisimple algebra over K. An *R-order* in $\mathcal{A}$ is a subring $\Lambda \subseteq \mathcal{A}$ with the following properties:

- Λ is a finitely generated module over R.
- Λ has an identity element (this is necessarily the same as the identity element of $\mathcal{A}$ and R).
- Λ generates $\mathcal{A}$ as a linear space over K.

An R-order Λ in $\mathcal{A}$ is a *maximal R-order* if it is not a proper subring of any other R-order of $\mathcal{A}$.

In a previous paper (Rónyai 1992) we studied algorithmic problems related to maximal orders in the case when K is an algebraic number field and R is the ring of algebraic integers in K. Before discussing algorithmic problems, we specify some conventions concerning our input (and output) objects.

An algebra $\mathcal{A}$ over a field K can be described by *structure constants*. If $a_1, \ldots, a_m$ is a basis of $\mathcal{A}$ over K, then the products a_ia_j can be expressed as linear combinations of the a_i

$$a_ia_j = \gamma_{ij1}a_1 + \gamma_{ij2}a_2 + \cdots + \gamma_{ijm}a_m.$$

The elements $\gamma_{ijk} \in K$ are called structure constants. In this paper an algebra is considered to be given as a collection of structure constants. As an important special case, an algebraic number field K is given by the monic minimal polynomial $f(x) \in \mathbb{Z}[x]$ of an integral element $\alpha \in K$ over $\mathbb{Q}$ such that $K = \mathbb{Q}(\alpha)$. We shall also work with rings whose additive groups are finitely generated free Abelian groups. In this case the structure constants are integers given with respect to a basis over the integers $\mathbb{Z}$. Subrings and ideals will be represented by bases whose elements are linear combinations of basis elements of a larger structure.

The time complexity of an algorithm is described in terms of the size of the input. The size of a rational number p/q expressed in lowest terms is the number of bits of p and q. The size of compound objects (polynomials, vectors, matrices, etc.) is the sum of the sizes of their components. The size of an object X is denoted by size(X). In particular, we use the (somewhat ambiguous) notation size($\mathcal{A}$), size(S), where $\mathcal{A}$ is an algebra or S is a ring. This is understood to be the size of the representation of $\mathcal{A}$ or S as an input or an output of the algorithm considered.

An algebra $\mathcal{A}$ is *central* over K, if $C(\mathcal{A}) = K$ holds where $C(\mathcal{A})$ is the *center* of $\mathcal{A}$:

$$C(\mathcal{A}) = \{a \in \mathcal{A} : ab = ba \text{ for every } b \in \mathcal{A}\}.$$

If $\mathcal{A}$ is central simple over an algebraic number field K, then by a theorem of Wedderburn $\mathcal{A}$ is isomorphic to a full matrix algebra $M_k(E)$ where E is a central skewfield over K. We have $\dim_K E = d^2$ for some positive integer d and this d is called the *index* of $\mathcal{A}$. In Rónyai (1992) the following algorithmic problem was considered:

Problem INDEX
Instance: *A central simple algebra $\mathcal{A}$ over an algebraic number field K and a positive integer $d \leq \sqrt{\dim_K \mathcal{A}}$.*
Question: *Is the index of $\mathcal{A}$ equal to d?*

It was shown in Rónyai (1992), Theorem 1.1 that INDEX$\in$ $NP \cap$ co-NP. The proof is based on the fact that $\mathcal{A}$ contains a maximal D-order Λ (D is the ring of algebraic integers in K) which admits a short description and verification. To clarify the latter point, we introduce the notion of ff-algorithms. A deterministic algorithm is an *ff-algorithm* if it is allowed to call oracles for two types of subproblems. These are the problem of factoring integers and the problem of factoring polynomials over finite fields. At present, no deterministic polynomial time methods are known to solve these two problems. Similarly an *f-algorithm* is a deterministic method which is allowed to call an oracle only for factoring polynomials over finite fields. In both cases the cost of a call is the size of the input passed on to the oracle. The main technical contribution of Rónyai (1992) is a deterministic polynomial time ff-algorithm to check if a given $\mathbb{Z}$-module $\Lambda \subseteq \mathcal{A}$ is a maximal D-order in $\mathcal{A}$. On the other hand, it was pointed out that there exists a maximal D-order Λ such that size(Λ) = size$(\mathcal{A})^{O(1)}$. These two facts suggest the possibility of *constructing* a maximal D-order by a polynomial time ff-algorithm.

The main result of this paper is a polynomial time ff-algorithm for constructing a maximal D-order Λ in a semisimple algebra $\mathcal{A}$ over an algebraic number field K. As an application, we give a deterministic method to compute the degrees of the irreducible representations over an algebraic number field K of a finite group G given by a multiplication table. The algorithm runs in time polynomial in the size of a multiplication table of G and in $|d(f)|$, the discriminant of the given defining polynomial f of K. Such an algorithm apparently was not available before, even for the simplest case $K = \mathbb{Q}$.

The organization of the paper is as follows. Section 2 contains the basic statements from the theory of orders we need. In particular, Lemma 2.6 states that maximal D-orders and maximal $\mathbb{Z}$-orders coincide, while Propositions 2.4, 2.5, and 2.9 make it possible to reduce the problem of finding maximal $\mathbb{Z}$-orders to that of finding maximal orders over the discrete valuation rings $\mathbb{Z}_{(p)}$ for primes p dividing some starting discriminant. Most of the material can be found in Reiner (1975). Proofs are given only where a precise reference was hard to locate.

In Section 3 we collect some statements about the radicals of orders over discrete valuation rings. These play an important role in the study of extremal orders later on.

Section 4 and in particular Proposition 4.1 and Theorem 4.5 contain the statements which serve as the theoretical foundation for our algorithms. These two statements enable us to reduce the problem of finding maximal orders over discrete valuation rings to that of decomposing associative algebras over the residue class fields. The ideas presented here are not new. They were used by Jacobinski (see Jacobinski 1971 or Reiner 1975, Chapter 39) in his approach to the theory of hereditary orders. We include proofs because Jacobinski worked with complete local rings. In the statements here the completeness of R is not assumed. Also, largely due to the fact that weaker results are sufficient for our purposes, it was possible to simplify some of the original arguments.

Section 5 contains the algorithms. Theorem 5.1 provides the basic 'iteration step' of our subsequent methods for constructing maximal orders. We describe an algorithm that for a given $\mathbb{Z}$-order Λ constructs an order Γ properly containing Λ if such an order exists.

In Corollary 5.3 we give a polynomial time ff-algorithm for constructing a maximal D-order Λ in a semisimple algebra $\mathcal{A}$ over an algebraic number field K. This settles in the affirmative the question raised in Rónyai (1992). We remark at this point, that on the basis of the theory of hereditary orders (Harada 1963) it is possible to give a more direct, but theoretically much more complicated algorithm to construct maximal orders.

Perhaps the most interesting result of the paper is Corollary 5.6. We propose a new deterministic algorithm to compute the degrees of the irreducible representations over an algebraic number field K of a finite group G given by a multiplication table.

1.1. Notation and terminology. Throughout the paper we keep ourselves to the following notation and terminology:
R: a Dedekind ring, i.e., a Noetherian integrally closed domain in which the nonzero prime ideals are maximal,
K: the field of quotients of R,
P: the unique maximal ideal of R, if R is a discrete valuation ring,
π: a prime element of R when R is a discrete valuation ring R, i.e., an element $\pi \in R$ such that $(\pi) = P$,
$\mathcal{A}$: a finite dimensional semisimple algebra over K,
order: we use this term for an R-order in the K-algebra $\mathcal{A}$,
Γ, Λ: orders,
radical: the Jacobson radical of a ring or algebra, denoted by $\mathrm{Rad}(R)$, $\mathrm{Rad}(\Lambda)$, etc.

2. Basic facts about orders

In this section we collect the basic facts and some elementary results from the theory of orders we need later on. Most of the statements and proofs can be found in our principal reference Reiner (1975), Sections 9, 10. In this section we assume that $\mathcal{A}$ is a separable algebra, i.e., semisimple and the centers of its simple components are separable extensions of the ground field K.

2.1. Reduced trace forms and discriminants. First we introduce the *reduced trace* function of a semisimple algebra using a sequence of progressively more general definitions (for a central simple algebra, then a simple algebra, and finally for a semisimple algebra).

The *trace* $\mathrm{T}_{\mathcal{A}/K}(x)$ of an element $x \in \mathcal{A}$ over K is the trace of the K-linear transformation $L_x : \mathcal{A} \to \mathcal{A}$ defined by $L_x(a) = xa$ for $a \in \mathcal{A}$.

If $\mathcal{A}$ is a full matrix algebra over the field E, $\dim_E \mathcal{A} = n^2$, then there is another way to define traces of elements of $\mathcal{A}$. Namely, if we have an isomorphism $\phi\colon \mathcal{A} \cong \mathrm{M}_{n \times n}(E)$, then we can take $\mathrm{tr}_{\mathcal{A}/E}(x)$ as the trace of the matrix ϕx. This is independent of the choice of the isomorphism ϕ.

If $\mathcal{A}$ is a central simple K-algebra and $\dim_K \mathcal{A} = n^2$, then there exists an extension field E of K which splits $\mathcal{A}$, i.e., $E \otimes_K \mathcal{A} \cong \mathrm{M}_{n \times n}(E)$. It can be shown that $\mathrm{tr}_{\mathcal{A}/K}(x) := \mathrm{tr}_{E \otimes_K \mathcal{A}/E}(x \otimes 1) \in K$ is independent of the choice of the splitting field E and we have $n\, \mathrm{tr}_{\mathcal{A}/K}(x) = \mathrm{T}_{\mathcal{A}/K}(x)$. Consequently, if the characteristic of K is zero (or prime to n), then $\mathrm{tr}_{\mathcal{A}/K}(x) = \frac{1}{n}\mathrm{T}_{\mathcal{A}/K}(x)$.

If $\mathcal{A}$ is a simple K-algebra with center L, then we can take $\mathrm{tr}_{\mathcal{A}/K}(x) := \mathrm{T}_{L/K}\mathrm{tr}_{\mathcal{A}/L}(x)$. If $\mathcal{A}$ is a semisimple K-algebra with Wedderburn-decomposition $\mathcal{A} = \mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_k$, then we can define $\mathrm{tr}_{\mathcal{A}/K}(x) := \mathrm{tr}_{\mathcal{A}_1/K}(x_1) + \ldots + \mathrm{tr}_{\mathcal{A}_k/K}(x_k)$, where x_i is the image of x under the projection $\mathcal{A} \to \mathcal{A}_i$ onto the ith simple component of $\mathcal{A}$. We call $\mathrm{tr}_{\mathcal{A}/K}(x)$ the *reduced trace* of x over K. The map $\tau\colon \mathcal{A} \times \mathcal{A} \to K$ defined by $\tau(x,y) := \mathrm{tr}_{\mathcal{A}/K}(xy)$ is a K-bilinear function and is called the bilinear trace form of $\mathcal{A}$ over K. If $\mathcal{A}$ is *separable* over K then τ is a nondegenerate bilinear form. For the rest of this subsection we assume that $\mathcal{A}$ is separable over K.

We shall omit the subscript $\mathcal{A}/K$ from $\mathrm{T}_{\mathcal{A}/K}$ and $\mathrm{tr}_{\mathcal{A}/K}$ whenever $\mathcal{A}$ and K are clear from the context.

Let Λ be an R-order in $\mathcal{A}$. Then for every element $x \in \Lambda$, we have $\mathrm{tr}(x) \in R$ (Reiner 1975, Theorem 10.1). Let $n = \dim_K \mathcal{A}$. The *discriminant* of the order Λ is the ideal $\mathrm{d}(\Lambda)$ in R generated by the set

$$\{\det(\mathrm{tr}(x_i x_j))_{i,j=1}^{n} \mid (x_1, \ldots, x_n) \in \Lambda^n\}.$$

It is clear that if $\Lambda \subseteq \Gamma$, then $\mathrm{d}(\Gamma) \mid \mathrm{d}(\Lambda)$. Moreover we have

PROPOSITION 2.1. *Assume that* $\Lambda \subseteq \Gamma$. *Then* $\mathrm{d}(\Gamma) \mid \mathrm{d}(\Lambda)$ *and* $\Lambda = \Gamma$ *if and only if* $\mathrm{d}(\Gamma) = \mathrm{d}(\Lambda)$.

PROOF. Reiner (1975), Exercise 10.3 or 4.13. □

From a generating set of Λ as an R-module we can easily obtain a nonzero multiple of $\mathrm{d}(\Lambda)$: we select a subset $\{x_1, \dots, x_n\}$ of the generating set which is a K-basis of $\mathcal{A}$.

PROPOSITION 2.2. *Let $\{x_1, \dots, x_n\} \subseteq \Lambda$ be a K-basis of $\mathcal{A}$. Then the principal ideal generated by the nonzero determinant $d = \det(\mathrm{tr}(x_i x_j))_{i,j=1}^n$ is contained in the discriminant.*

PROOF. Obvious. □

PROPOSITION 2.3. *Let $\{x_1, \dots, x_n\}$ and d be as in Proposition 2.2. Let Γ be any order containing Λ. Then $d(\Gamma) \subseteq R\{x_1, \dots, x_n\} \subseteq \Lambda$.*

PROOF. The proof of Proposition 2.1 from Rónyai (1992) works for semisimple algebras as well. □

Note that if R is a principal ideal domain, then every R-order Λ admits an R-basis, say $\{x_1, \dots, x_n\}$, and the discriminant $\mathrm{d}(\Lambda)$ is the principal ideal generated by the determinant $\det(\mathrm{tr}(x_i x_j))_{i,j=1}^n$ (Reiner 1975, Theorem 10.2).

2.2. Localizations. If R is a Dedekind domain with quotient field K and P is a prime ideal in R, then the ring of quotients $R_P = (R \setminus P)^{-1} R \subset K$ is a discrete valuation ring. For an R-lattice M in $\mathcal{A}$ we can define the localization at P as follows: $M_P = R_P M \subset \mathcal{A}$. M_P is an R_P-lattice. If M is a full R-lattice in $\mathcal{A}$ (i.e., $KM = \mathcal{A}$), then M_P is a full R_P-lattice in $\mathcal{A}$. If Λ is an R-order, then Λ_P is an R_P-order. Moreover Λ is a maximal R-order if and only if Λ_P is a maximal R_P order for every prime ideal P of R. More generally, we have the following

PROPOSITION 2.4. *If Γ and Λ are R-orders in $\mathcal{A}$ such that $\Lambda \subset \Gamma$, then there exists a prime ideal P of R such that $\Lambda_P \subset \Gamma_P$.*

PROOF. Reiner (1975), Theorem 3.15. □

To be more specific, for a rational prime p let $\mathbb{Z}_{(p)}$ denote the ring

$$\mathbb{Z}_{(p)} = \{r/s \in \mathbb{Q};\ r, s \in \mathbb{Z},\ \gcd(p, s) = 1\}.$$

$\mathbb{Z}_{(p)}$ is a discrete valuation ring with unique maximal ideal $p\mathbb{Z}_{(p)}$. If Λ is a $\mathbb{Z}$-order, then we use the notation $\Lambda_{(p)} = \mathbb{Z}_{(p)}\Lambda$.

2.3. Orders over $\mathbb{Z}$ and $\mathbb{Z}_{(p)}$. There are some simple examples of orders. If M is a full R-lattice in $\mathcal{A}$ (i.e., $KM = \mathcal{A}$), then the left order of M defined by $\mathcal{O}_l(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$ is an R-order in $\mathcal{A}$ (Reiner 1975, p. 109). The right order is defined in a similar way. This type of construction is an important algorithmic tool for constructing orders:

PROPOSITION 2.5. *If $R = \mathbb{Z}$, and a full $\mathbb{Z}$-module M in the $\mathbb{Q}$-algebra $\mathcal{A}$ is given by a $\mathbb{Z}$-basis, then $\mathcal{O}_l(M)$ has a $\mathbb{Z}$-basis of size* $(\text{size}(\mathcal{A}) + \text{size}(M))^{O(1)}$, *and such a basis can be computed in time* $(\text{size}(\mathcal{A}) + \text{size}(M))^{O(1)}$.

PROOF. In Rónyai (1992), Theorem 3.2 the statement is proved for a simple algebra $\mathcal{A}$. The argument works in the more general case when $\mathcal{A}$ is semisimple. □

The next statement will be useful when we change the ring of coefficients from $\mathbb{Z}$ to D.

LEMMA 2.6. *Let K be an algebraic number field, $\mathcal{A}$ a finite dimensional semisimple algebra over K and let Λ be a $\mathbb{Z}$-order in $\mathcal{A}$. Let D be the ring of algebraic integers of K. Then $\Gamma = D\Lambda$ is a D-order containing Λ. As a consequence, a maximal $\mathbb{Z}$-order in $\mathcal{A}$ is a maximal D-order as well.*

PROOF. It is straightforward to check that $D\Lambda$ (the finite sums of the form $\sum \alpha_i x_i$, $\alpha_i \in D$, $x_i \in \Lambda$) is a ring which is a finitely generated D-module. Also we have $1_{\mathcal{A}} \in D\Lambda$. □

The following statement gives a tool to reduce the problem of enlarging a $\mathbb{Z}$-order to a similar problem for $\mathbb{Z}_{(p)}$-orders.

LEMMA 2.7. *Let p be a rational prime and Γ be a $\mathbb{Z}$-order. Suppose that $\mathcal{J}$ is an ideal of $\Gamma_{(p)}$ such that $\mathcal{J} \supseteq p\Gamma_{(p)}$ and $\mathcal{O}_l(\mathcal{J}) \supset \Gamma_{(p)}$. Let $\mathcal{I}$ denote the inverse image of $\mathcal{J}$ with respect to the embedding $\Gamma \to \Gamma_{(p)}$. Then we have $\mathcal{I} \supseteq p\Gamma$ and $\mathcal{O}_l(\mathcal{I}) \supset \Gamma$.*

PROOF. Clearly $\mathcal{I} \supseteq p\Gamma$ and $\mathcal{I}$ is an ideal of Γ. Let $a_1, a_2, \ldots, a_t$ be a generating set of $\mathcal{I}$, as a $\mathbb{Z}$-module. Then the images of the elements a_i (which will also be denoted by a_i) form a generating set of $\mathcal{J}$ as a $\mathbb{Z}_{(p)}$-module. Now let $a \in \mathcal{O}_l(\mathcal{J}) \setminus \Gamma_{(p)}$. Then for $i = 1, \ldots, t$ we have

$$aa_i = \frac{\alpha_{i1}}{\beta_{i1}}a_1 + \frac{\alpha_{i2}}{\beta_{i2}}a_2 + \cdots + \frac{\alpha_{it}}{\beta_{it}}a_t,$$

where $\alpha_{ij}, \beta_{ij} \in \mathbb{Z}$ and p does not divide β_{ij}. Now put $\beta = \prod_{i,j} \beta_{ij}$. Then it is straightforward to check that $\beta a \mathcal{I} \subseteq \mathcal{I}$ and consequently $\beta a \in \mathcal{O}_l(\mathcal{I})$. Finally we observe that $\beta a \notin \Gamma$, for otherwise we have $a \in \Gamma_{(p)}$. The proof is complete. □

The next statement demonstrates a simple but useful connection between the orders Λ and $\Lambda_{(p)}$.

PROPOSITION 2.8. *Let Λ be a $\mathbb{Z}$-order in $\mathcal{A}$. The map $\phi : x \mapsto x + p\Lambda_{(p)}$ ($x \in \Lambda$) induces an isomorphism of rings $\Lambda/p\Lambda \cong \Lambda_{(p)}/p\Lambda_{(p)}$.*

PROOF. Clearly $\phi : \Lambda \to \Lambda_{(p)}/p\Lambda_{(p)}$ is an epimorphism of rings. It is straightforward to check that $\ker(\phi) = p\Lambda$. □

The next statement provides a bound on the number of iterations in algorithms which successively increase orders until a maximal order is obtained.

PROPOSITION 2.9. *Assume that we have the strictly increasing chain $\Lambda_0 \subset \ldots \subset \Lambda_m$ of $\mathbb{Z}$-orders in $\mathcal{A}$. Let d_i be the positive integer generating the ideal* $\mathrm{d}(\Lambda_i)$, *for $0 \leq i \leq m$. Then*

$$m \leq \frac{1}{2}\log_2(d_0/d_m) \leq \frac{1}{2}\log_2 d_0.$$

PROOF. For each $i < m$, $d_i/d_{i+1} > 1$ is the square of an integer (namely of the determinant of the matrix transforming a $\mathbb{Z}$-basis of Λ_{i+1} to a $\mathbb{Z}$-basis of Λ_i). We obtain the statement by taking the logarithm of

$$\frac{d_0}{d_m} = \prod_{i=0}^{m-1} \frac{d_i}{d_{i+1}} \geq 2^{2m}. \quad \square$$

3. Radicals of orders over local rings

First we recall some basic facts about the Jacobson radical of rings. For proofs, see for example Reiner (1975), Section 6.a. Let S denote an arbitrary ring with an identity element. $\mathrm{Rad}(S)$, the Jacobson radical of S is the set of elements $x \in S$ such that $xM = (0)$ for all simple left (or, equivalently, $Mx = (0)$ for all simple right) modules M over S. $\mathrm{Rad}(S)$ is a two-sided ideal in S containing every nilpotent one-sided ideal of S. Also, $\mathrm{Rad}(S)$ can be characterized as the intersection of the maximal left ideals in S, and, equivalently, as the intersection of the maximal right ideals in S. If S is left or right Artinian (this holds for example if $\mathcal{S}$ is a finite dimensional algebra over a field) then $\mathrm{Rad}(\mathcal{S})$ is the maximal nilpotent ideal in $\mathcal{S}$.

After these preliminaries let us return to our rings of interest. We assume that R is a discrete valuation ring, P is the unique nonzero prime ideal of R, K is the field of quotients of R, and Λ is an R-order in a finite dimensional semisimple K-algebra $\mathcal{A}$.

Proposition 3.1. *The residue class ring $\bar{\Lambda} = \Lambda/P\Lambda$ is an algebra with identity element over the residue class field $\bar{R} = R/P$ and $\dim_K \mathcal{A} = \dim_{\bar{R}} \bar{\Lambda}$. If $\phi\colon \Lambda \to \bar{\Lambda}$ is the canonical epimorphism, then $P\Lambda \subseteq \mathrm{Rad}(\Lambda) = \phi^{-1}\mathrm{Rad}(\bar{\Lambda})$ and ϕ induces a ring isomorphism $\Lambda/\mathrm{Rad}(\Lambda) \cong \bar{\Lambda}/\mathrm{Rad}(\bar{\Lambda})$. As a consequence, a left (or right) ideal $\mathcal{I}$ of Λ is contained in $\mathrm{Rad}(\Lambda)$ if and only if $\mathcal{I}$ is nilpotent modulo $P\Lambda$, i.e., there exists a positive integer t such that $\mathcal{I}^t \subseteq P\Lambda$.*

Proof. Most of the statements are proved in Reiner (1975), Theorem 6.15. The claim about the dimensions follows directly from the fact that R is a principal ideal ring and Λ is a free R-module. As for the 'only if' part of the last statement, every nilpotent ideal of $\bar{\Lambda}$ is contained in $\mathrm{Rad}(\bar{\Lambda})$. □

Proposition 3.2. *If $\Lambda \subseteq \Gamma$ are R-orders, then there exists a positive integer s such that $\mathrm{Rad}(\Gamma)^s \subseteq \Lambda$. For any such s, $\mathrm{Rad}(\Gamma)^s \subseteq \mathrm{Rad}(\Lambda)$ is an ideal in Λ.*

Proof. (For a part of the argument below see Reiner 1975, Ex. 39.3.) Using that $\Gamma \supseteq \Lambda$ are full R-modules in $\mathcal{A}$ over a discrete valuation ring R, and Proposition 3.1, we infer that there exist positive integers u and t such that $P^u\Gamma \subseteq \Lambda$ and $\mathrm{Rad}(\Gamma)^t \subseteq P\Gamma$. Now $s = tu$ will suffice to prove the first claim. If for some s we have $\mathcal{I} = \mathrm{Rad}(\Gamma)^s \subseteq \Lambda$, then $\mathcal{I}$ is an ideal in Λ because $\Lambda\mathcal{I} \subseteq \Gamma\mathcal{I} = \mathcal{I}$ and $\mathcal{I}\Lambda \subseteq \mathcal{I}\Gamma = \mathcal{I}$. Finally, for the integers t and u we have

$$\begin{aligned} \mathcal{I}^{t(u+1)} &= \mathrm{Rad}(\Gamma)^{st(u+1)} \subseteq (P\Gamma)^{s(u+1)} \subseteq (P\Gamma)^{(u+1)} \\ &= P^{(u+1)}\Gamma = P \cdot P^u\Gamma \subseteq P\Lambda \end{aligned}$$

Proposition 3.1 implies that $\mathcal{I} \subseteq \mathrm{Rad}(\Lambda)$. □

The following observation plays an important role in Jacobinski's (1971) approach to hereditary orders.

Proposition 3.3. *Let $\Lambda \subseteq \Gamma$ be R-orders in $\mathcal{A}$ such that $\mathrm{Rad}(\Gamma) \subseteq \Lambda$. Then for any order Λ' such that $\Lambda \subseteq \Lambda' \subseteq \Gamma$ we have $\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda')$. The canonical map $\phi\colon \Gamma \to \bar{\Gamma} = \Gamma/\mathrm{Rad}(\Gamma)$ induces a bijection $\Lambda' \mapsto \Lambda'/\mathrm{Rad}(\Gamma)$ between the set of orders Λ' lying between Λ and Γ and the set of the subalgebras of the R/P-algebra $\bar{\Gamma}$ containing $\Lambda/\mathrm{Rad}(\Gamma)$. Moreover if $\Lambda \subseteq \Lambda' \subseteq \Gamma$, then we have $\mathrm{Rad}(\Lambda') = \phi^{-1}\mathrm{Rad}(\phi\Lambda')$.*

PROOF. We have $\mathrm{Rad}(\Gamma) \subseteq \Lambda \subseteq \Lambda'$. From this, Proposition 3.2 implies that $\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda')$. The statement about the correspondence of R-orders and R/P-subalgebras is obvious once we observe that any R-subalgebra Λ' such that $\Lambda \subseteq \Lambda' \subseteq \Gamma$ is actually an R-order. As for the last statement, we note that if $\mathcal{J}$ is a maximal left ideal of Λ', then $\mathrm{Rad}(\Gamma) \subseteq \mathcal{J}$, because we have $\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda')$. We infer that ϕ induces a bijection between the set of the maximal left ideals of Λ' and the set of the maximal left ideals of $\Lambda'/\mathrm{Rad}(\Gamma)$, and the statement follows. □

4. Extremal orders

In this section R is a discrete valuation ring. For R-orders in $\mathcal{A}$ we introduce the following partial ordering: Γ ***radically contains*** Λ if and only if $\Gamma \supseteq \Lambda$ and $\mathrm{Rad}(\Gamma) \supseteq \mathrm{Rad}(\Lambda)$. The orders maximal with respect to this partial ordering are called *extremal.* Maximal orders are obviously extremal. The notion of extremal orders has been introduced in Jacobinski (1971). The next statement is from Jacobinski (1971), Proposition 1. We note first that if Λ is an R-order, then $P\Lambda \subseteq \mathrm{Rad}(\Lambda)$, so that $\mathrm{Rad}(\Lambda)$ is a full R-lattice—therefore $\mathcal{O}_l(\mathrm{Rad}(\Lambda))$ is an R-order.

PROPOSITION 4.1. *For any R-order Λ, the order $\mathcal{O}_l(\mathrm{Rad}(\Lambda))$ radically contains Λ. Moreover, an R-order Λ of $\mathcal{A}$ is extremal if and only if $\Lambda = \mathcal{O}_l(\mathrm{Rad}(\Lambda))$ (if and only if $\Lambda = \mathcal{O}_r(\mathrm{Rad}(\Lambda))$).*

PROOF. Since $\mathrm{Rad}(\Lambda)$ is an ideal in Λ, $\Lambda \subseteq \mathcal{O}_l(\mathrm{Rad}(\Lambda))$. Also, $\mathrm{Rad}(\Lambda)$ is a left ideal in $\mathcal{O}_l(\mathrm{Rad}(\Lambda))$ and by Proposition 3.1 for some t we have $\mathrm{Rad}(\Lambda)^t \subseteq P\Lambda \subseteq P\mathcal{O}_l(\mathrm{Rad}(\Lambda))$, hence $\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{O}_l(\mathrm{Rad}(\Lambda)))$. This implies that $\mathcal{O}_l(\mathrm{Rad}(\Lambda))$ radically contains Λ. We infer that if Λ is extremal, then $\Lambda = \mathcal{O}_l(\mathrm{Rad}(\Lambda))$.

In the other direction, we suppose that $\Lambda = \mathcal{O}_l(\mathrm{Rad}(\Lambda))$ and Γ is an order radically containing Λ. By Proposition 3.2 there exists an integer $s > 0$ such that $\mathrm{Rad}(\Gamma)^s \subseteq \mathrm{Rad}(\Lambda)$. For any $s > 1$ with this property we have $\mathrm{Rad}(\Gamma)^{s-1}\mathrm{Rad}(\Lambda) \subseteq \mathrm{Rad}(\Gamma)^{s-1}\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda)$, implying that $\mathrm{Rad}(\Gamma)^{s-1} \subseteq \mathcal{O}_l(\mathrm{Rad}(\Lambda)) = \Lambda$. Proposition 3.2 implies that $\mathrm{Rad}(\Gamma)^{s-1} \subseteq \mathrm{Rad}(\Lambda)$. Continuing in this way we obtain $\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda)$ and consequently $\mathrm{Rad}(\Gamma) = \mathrm{Rad}(\Lambda)$. We conclude that $\Gamma \subseteq \mathcal{O}_l(\mathrm{Rad}(\Gamma)) = \mathcal{O}_l(\mathrm{Rad}(\Lambda)) = \Lambda$ and $\Gamma = \Lambda$. □

PROPOSITION 4.2. *Assume that $\Lambda \subseteq \Gamma$ are R-orders. Then $\Lambda + \mathrm{Rad}(\Gamma)$ is an R-order radically containing Λ.*

PROOF. It is straightforward to verify that $\Lambda' = \Lambda + \mathrm{Rad}(\Gamma)$ is an R-order containing Λ. Next, using the characterization of radical-ideals from Proposition 3.1, we obtain that $\mathrm{Rad}(\Lambda)+\mathrm{Rad}(\Gamma)$ is an ideal of Λ' and $\mathrm{Rad}(\Lambda)+\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda')$. □

PROPOSITION 4.3. *Let $\Lambda \subseteq \Gamma$ be R-orders and suppose that Λ is extremal. Then* $\mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda)$.

PROOF. An immediate consequence of Propositions 4.2 and 3.2. □

We remark that if Λ is an R-order in $\mathcal{A}$ such that $\mathrm{Rad}(\Lambda) = P\Lambda = \pi\Lambda$ then Λ is a maximal order. Indeed, $\mathcal{O}_l(\pi\Lambda) = \mathcal{O}_l(\Lambda) = \Lambda$, hence Λ is extremal by Proposition 4.1. If $\Gamma \supseteq \Lambda$, then by Proposition 4.3 we have $\pi\Gamma \subseteq \mathrm{Rad}(\Gamma) \subseteq \mathrm{Rad}(\Lambda) = \pi\Lambda$, implying that $\pi\Gamma = \pi\Lambda$ and $\Gamma = \Lambda$.

Theorem 4.5 plays a key role in our method for constructing a maximal R-order. The statement and the proof is a simplified version of Jacobinski (1971), Proposition 2. We need first an auxiliary lemma on semisimple algebras.

LEMMA 4.4. *Let $\mathcal{B}$ be a finite dimensional semisimple algebra over a field F. Let $\mathcal{C}$ be a maximal subalgebra of $\mathcal{B}$ such that* $\mathrm{Rad}(\mathcal{C}) \neq 0$. *Then there exists a two-sided ideal $\mathcal{J}$ of $\mathcal{C}$ minimal among those containing* $\mathrm{Rad}(\mathcal{C})$ *which is a left ideal of $\mathcal{B}$.*

PROOF. First we reduce the statement to the special case when $\mathcal{B}$ is simple. In general, by Wedderburn's theorem we have $\mathcal{B} = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_k$, where the direct summands $\mathcal{B}_i$ are simple algebras. We observe first that $\mathcal{C}$ contains the center $C(\mathcal{B})$ of $\mathcal{B}$. Indeed, for the algebra $\mathcal{C}' =< \mathcal{C}, C(\mathcal{B}) >$ we have $\mathcal{C}' \supseteq \mathcal{C}$. Also, it is straightforward to verify that an element $0 \neq c \in \mathrm{Rad}(\mathcal{C})$ generates a nilpotent left ideal in $\mathcal{C}'$ as well, therefore $\mathrm{Rad}(\mathcal{C}') \neq 0$. This implies that $\mathcal{C}' \subset \mathcal{B}$ and hence $\mathcal{C}' = \mathcal{C}$ and $\mathcal{C} \supseteq C(\mathcal{B})$.

We infer that $\mathcal{C}$ contains the identity elements $e_i \in \mathcal{B}_i$ of the ideals $\mathcal{B}_i$ and consequently we have $\mathcal{C} = e_1\mathcal{C} \oplus \cdots \oplus e_k\mathcal{C}$. Now the maximality of $\mathcal{C}$ implies the existence of an index i, such that $e_i\mathcal{C}$ is a maximal subalgebra of the simple algebra $\mathcal{B}_i$ and $e_j\mathcal{C} = \mathcal{B}_j$, if $j \neq i$. Clearly we have $\mathrm{Rad}(e_i\mathcal{C}) = \mathrm{Rad}(\mathcal{C}) \neq 0$. Now a two-sided ideal $\mathcal{J}_i$ of $e_i\mathcal{C}$ minimal among those containing $\mathrm{Rad}(e_i\mathcal{C})$ which is a left ideal of $\mathcal{B}_i$ will clearly suffice as $\mathcal{J}$.

For the rest of the proof we assume that $\mathcal{B}$ is a simple algebra. Let V be a simple left $\mathcal{B}$-module, and let D stand for the algebra of $\mathcal{B}$-endomorphisms of V. By Schur's lemma D is a division algebra over the field F and V is a right D-space. Moreover we have $\mathcal{B} = \mathrm{End}_D V$ and hence $\mathrm{Rad}(\mathcal{C})V \neq 0$.

We define the strictly decreasing chain of D-subspaces $V = V_0 \supset V_1 \supset V_2$ by $V_{i+1} = \mathrm{Rad}(\mathcal{C})V_i$, for $i = 0, 1$. From this chain of subspaces we obtain a decreasing chain of subalgebras $\mathcal{B} = \mathcal{B}_0 \supseteq \mathcal{B}_1 \supseteq \mathcal{B}_2$ by letting

$$\mathcal{B}_i = \{x \in \mathcal{B} \mid xV_j \subseteq V_j \text{ for } j = 0, \dots, i\}.$$

Here $\mathcal{B} \neq \mathcal{B}_1$ follows from $\mathcal{B} = \mathrm{End}_D V$. Moreover, $\mathcal{B}_2 \supseteq \mathcal{C}$ implies that $\mathcal{B}_1 = \mathcal{B}_2 = \mathcal{C}$. We infer that $V_2 = 0$ and $(\mathrm{Rad}(\mathcal{C}))^2 = 0$.

Then the annihilator $\mathcal{J} = \{x \in \mathcal{B} \mid xV_1 = 0\}$ is properly contained in $\mathcal{B}_1 = \mathcal{C}$, and in fact is a two-sided ideal of $\mathcal{C}$. It is also obvious that $\mathcal{J}$ is a left ideal of $\mathcal{B}$, and this implies that $\mathcal{J} \supset \mathrm{Rad}(\mathcal{C})$. From $\mathcal{B} = \mathrm{End}_D V$ we obtain that $\mathcal{C}/\mathrm{Rad}(\mathcal{C}) \cong \mathrm{End}_D V_1 \oplus \mathrm{End}_D V/V_1$. Thus, $\mathcal{C}/\mathrm{Rad}(\mathcal{C})$ is a semisimple algebra with exactly two minimal ideals, implying the minimality of $\mathcal{J}$ over $\mathrm{Rad}(\mathcal{C})$. □

THEOREM 4.5. *Let $\Lambda \subset \Gamma$ be R-orders in $\mathcal{A}$. Suppose that Λ is extremal and Γ is minimal among the R-orders properly containing Λ. Then there exists an ideal $\mathcal{I}$ of Λ minimal among those containing* $\mathrm{Rad}(\Lambda)$ *such that $O_l(\mathcal{I}) \supseteq \Gamma$.*

PROOF. By Propositions 4.3 and 3.3, we have that $\mathcal{C} = \Lambda/\mathrm{Rad}(\Gamma)$ is a maximal proper subalgebra of the semisimple $F = R/P$-algebra $\mathcal{B} = \Gamma/\mathrm{Rad}(\Gamma)$. Moreover $\mathrm{Rad}(\mathcal{C}) \neq 0$, since $\Lambda \subset \Gamma$ and Λ is extremal. We can apply Lemma 4.4. There exists a minimal ideal $\mathcal{J}$ of $\mathcal{C}$ above $\mathrm{Rad}(\mathcal{C})$ such that $\mathcal{J}$ is a left ideal in $\mathcal{B}$. Now $\mathcal{I}$, the inverse image of $\mathcal{J}$ with respect to the natural map $\Gamma \to \mathcal{B}$ clearly satisfies the requirements of the theorem. □

5. Algorithms

Let K be an algebraic number field, $\mathcal{A}$ a finite dimensional semisimple algebra over K and Λ be a $\mathbb{Z}$-order in $\mathcal{A}$. Let D stand for the ring of algebraic integers of K. Suppose that $\mathcal{A}$ is given by structure constants and Λ is given by a $\mathbb{Z}$-basis. Suppose further that we are given a set $S = \{p_1, p_2, \dots, p_r\}$ of rational primes such that $\Lambda_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$-order if $p \notin S$. By Proposition 2.3 the preceding condition is satisfied if S is the set of primes dividing a multiple of $d(\Lambda)$. For a finite set S of primes we write $k_S = \prod_{p \in S} p$.

THEOREM 5.1. *There exists an f-algorithm running in time* $(\mathrm{size}(\mathcal{A}) + \mathrm{size}(\Lambda) + \log k_S)^{O(1)}$ *that produces a $\mathbb{Z}$-basis of a $\mathbb{Z}$-order $\Gamma \supset \Lambda$, provided that such an order Γ exists. The f-oracle is employed to factor polynomials over $GF(p)$ for $p \in S$.*

PROOF. If Γ exists, then there must be an i, $1 \leq i \leq r$ such that $\Lambda_{p_i} \subset \Gamma_{p_i}$. We shall therefore test for $1 \leq i \leq r$ whether Λ is maximal at p_i. If Λ is maximal at every p_i, then Λ is a maximal $\mathbb{Z}$-order. Otherwise, at the first i such that Λ_{p_i} is not maximal, we construct a $\mathbb{Z}$-order Γ in $\mathcal{A}$ such that $\Lambda_{p_i} \subset \Gamma_{p_i}$ and therefore $\Lambda \subset \Gamma$. Clearly it suffices to show that a step of this iteration can be performed within the time bound stated because $r \leq \log_2 k_S$.

Let $p \in S$. We shall test first whether $\Lambda_{(p)}$ is an extremal $\mathbb{Z}_{(p)}$-order by checking if $\mathcal{O}_l(\text{Rad}(\Lambda_{(p)})) = \Lambda_{(p)}$. If not, then we construct a $\mathbb{Z}$-order $\Gamma \supset \Lambda$. If $\Lambda_{(p)}$ passes the test, then we use the test of Theorem 4.5. If there exists an ideal $\mathcal{J}$ minimal among the ideals properly containing $\text{Rad}(\Lambda_{(p)})$ such that $\mathcal{O}_l(\mathcal{J}) \supset \Lambda_{(p)}$, then we construct a $\mathbb{Z}$-order $\Gamma \supset \Lambda$. Otherwise we correctly conclude that Λ is maximal at p.

As for the first test, we compute the inverse image $\mathcal{I} \subseteq \Lambda$ of $\text{Rad}(\Lambda_{(p)})$ with respect to the embedding $\Lambda \to \Lambda_{(p)}$. By Lemma 2.7, Λ passes the first test if and only if $\mathcal{O}_l(\mathcal{I}) = \Lambda$. Otherwise, $\Gamma = \mathcal{O}_l(\mathcal{I})$ is an order strictly containing Λ.

We shall work with the finite algebra $\mathcal{B} = \Lambda/p\Lambda$ over $GF(p)$. We have $\dim_{GF(p)}\mathcal{B} = \dim_{\mathbb{Q}}\mathcal{A} = n$, and structure constants for $\mathcal{B}$ are easily obtained. We have $\text{size}(\mathcal{B}) = (\text{size}(\mathcal{A})+\text{size}(\Lambda)+\log p)^{O(1)}$. From Propositions 3.1 and 2.8 we infer that $\mathcal{I}$ is the inverse image of $\text{Rad}(\mathcal{B})$ with respect to the canonical map $\Lambda \to \mathcal{B}$. $\text{Rad}(\mathcal{B})$ can be computed in deterministic time $(n+\log p)^{O(1)}$ with the method of Rónyai (1990), Theorem 2.7. From a $GF(p)$-basis of $\text{Rad}(\mathcal{B})$ we can efficiently find a $\mathbb{Z}$-basis of $\mathcal{I}$. (Note that any $\mathbb{Z}$-submodule M such that $p\Lambda \subseteq M \subseteq \Lambda$ has a basis of size bounded by $(\text{size}(\Lambda) + \log p)^{O(1)}$). Also, by Proposition 2.5 we can compute $\mathcal{O}_l(\mathcal{I})$ efficiently. This finishes the description of the first test.

The second test can be treated in a similar way. Let $\mathcal{J}_1, \ldots, \mathcal{J}_m$ denote the minimal ideals of $\mathcal{B}$ which contain $\text{Rad}(\mathcal{B})$. Note that these ideals are the inverse images, with respect to the canonical map $\phi : \mathcal{B} \to \mathcal{B}/\text{Rad}(\mathcal{B})$, of the minimal ideals of the semisimple algebra $\mathcal{B}/\text{Rad}(\mathcal{B})$. We have $m \leq n$. Let $\mathcal{I}_i$ denote the inverse image in Λ of $\mathcal{J}_i$ with respect to the map $\Lambda \to \mathcal{B}$. Propositions 2.8 and 3.1 imply that $\mathcal{I}_1, \ldots, \mathcal{I}_m$ are also the inverse images of the minimal ideals of $\Lambda_{(p)}$ over $\text{Rad}(\Lambda_{(p)})$. As in the first case, we obtain that we have to compute the rings $\mathcal{O}_l(\mathcal{I}_i)$ for $1 \leq i \leq m$. We can stop when $\Lambda \subset \mathcal{O}_l(\mathcal{I}_i)$ is detected, because then we have an order properly containing Λ.

The ideals $\mathcal{J}_i$ are obtained by the deterministic f-algorithm of Friedl and Rónyai (see Rónyai 1990, Theorem 3.1). The time requirement is $(n+\log p)^{O(1)}$ and we call the f-oracle to factor polynomials over $GF(p)$. From the ideals $\mathcal{J}_i$, the ideals $\mathcal{I}_i$ and the rings $\mathcal{O}_l(\mathcal{I}_i)$ can be computed in deterministic time $(\text{size}(\mathcal{A}) + \text{size}(\Lambda) + \log p)^{O(1)}$. □

With the method of Theorem 5.1 we can construct a maximal $\mathbb{Z}$-order in $\mathcal{A}$ in ff-polynomial time. First we need a starting $\mathbb{Z}$-order. Let $a_1, \ldots, a_n$ be the input basis of $\mathcal{A}$ over $\mathbb{Q}$. Let d be the lowest common denominator of the structure constants with respect to this basis. Then the additive group Λ generated by $1_{\mathcal{A}}, da_1, \ldots, da_n$ is a $\mathbb{Z}$-order in $\mathcal{A}$. (This is a standard trick to make structure constants integral.) We put $k = \det(\mathrm{tr}_{\mathcal{A}/\mathbb{Q}}(d^2 a_i a_j)_{i,j=1}^n)$. By the results in Subsection 2.1, the elements $\mathrm{tr}_{\mathcal{A}/\mathbb{Q}}(a_i a_j)$ can be computed if we know the Wedderburn decomposition of $\mathcal{A}$ over $\mathbb{Q}$. The Wedderburn decomposition can be computed in deterministic polynomial time (Friedl & Rónyai 1985, Theorem 7.6). We have $\mathrm{size}(\Lambda) = \mathrm{size}(\mathcal{A})^{O(1)}$ and $\log k = \mathrm{size}(\mathcal{A})^{O(1)}$. Let S be the set of primes dividing k. We have $k_S \leq k$ and S is obtained by factoring k.

Repeated application of the algorithm of Theorem 5.1 gives a sequence of $\mathbb{Z}$-orders

$$\Lambda = \Gamma_0 \subset \Gamma_1 \subset \ldots \subset \Gamma_m$$

until a maximal $\mathbb{Z}$-order is obtained. By Proposition 2.9, $m \leq \frac{1}{2}\log_2 k$. We can control sizes during the iteration. By Proposition 2.3 we have $\Lambda \subseteq \Gamma_j \subseteq \frac{1}{k}\Lambda$, therefore Γ_j can be represented by a $\mathbb{Z}$-basis admitting a short description.

THEOREM 5.2. *Let $\mathcal{A}$ be a finite dimensional semisimple algebra over $\mathbb{Q}$ given by structure constants. Then a maximal $\mathbb{Z}$-order Λ can be constructed by an ff-algorithm running in time* $\mathrm{size}(\mathcal{A})^{O(1)}$. □

COROLLARY 5.3. *Let K be an algebraic number field, $\mathcal{A}$ a finite dimensional central simple algebra over K. Let D denote the ring of algebraic integers of K. Suppose that $\mathcal{A}$ is given by structure constants over K. Then a maximal D-order Λ in $\mathcal{A}$ can be constructed by an ff-algorithm running in time* $\mathrm{size}(\mathcal{A})^{O(1)}$.

PROOF. From K and the structure constants of $\mathcal{A}$ over K we can readily obtain structure constants of $\mathcal{A}$ over $\mathbb{Q}$. With the method of Theorem 5.2 we compute a $\mathbb{Z}$-basis of a maximal $\mathbb{Z}$-order Λ of $\mathcal{A}$. By Lemma 2.6 we conclude that Λ is a maximal D-order as well. □

Corollary 5.3 gives an affirmative answer to the question proposed at the end of Rónyai (1992).

Next we give an application to group representations. Suppose that K is an algebraic number field and D is the ring of algebraic integers of K. Let G be a finite group, $|G| = n$. We have the following theorem.

THEOREM 5.4. *Suppose that G is given by its multiplication table and D is given by a $\mathbb{Z}$-basis. Then in deterministic time* $(\mathrm{size}(K) + \mathrm{size}(D) + n)^{O(1)}$ *we can compute (a $\mathbb{Z}$-basis of) a maximal D-order Λ in KG which contains the group ring DG.*

PROOF. In Reiner (1975), Theorem 41.1 it is shown that if Λ is a D-order (and hence by Lemma 2.6 if Λ is a $\mathbb{Z}$-order) which contains $\Gamma = DG$, then $\Lambda \subseteq n^{-1}\Gamma$. This implies that $\Gamma_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$-order for every prime p not dividing n. Let S be the set of primes dividing n. As in the proof of Theorem 5.2 we compute a sequence of $\mathbb{Z}$-orders

$$\Gamma = \Gamma_0 \subset \Gamma_1 \subset \ldots \subset \Gamma_m$$

until a maximal $\mathbb{Z}$-order is obtained, by applying the method of Theorem 5.1. Since $\Gamma_m \subseteq n^{-1}\Gamma$, for the discriminants $d_m = d(\Gamma_m)$ and $d_0 = d(\Gamma_0)$ we have $d_0 \le n^{n \dim_{\mathbb{Q}} K} d_m$, and hence Proposition 2.9 implies that $m \le \frac{1}{2} n \dim_{\mathbb{Q}} K \log_2 n$.

Using the $\mathbb{Z}$-basis of D we have as part of the input, we can efficiently construct a $\mathbb{Z}$-basis of our starting order Γ. Since n counts in unary in the input size, we can afford to use trial division to construct S and to use the deterministic method of Berlekamp (1967) for factoring polynomials over finite fields at the second test. In this way we obtain the minimal ideals of $\mathcal{B}/\mathrm{Rad}(\mathcal{B})$ in deterministic time $(\dim_{\mathbb{Q}} K + n + p)^{O(1)}$ (note that the dimension over $\mathbb{Z}$ of DG is $n(\dim_{\mathbb{Q}} K)$). The statement follows from Theorem 5.1. □

COROLLARY 5.5. *Let K be an algebraic number field given by the monic minimal polynomial $f \in \mathbb{Z}[x]$ of an integral element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Let G be a finite group given by its multiplication table. Then in deterministic time* $(\mathrm{size}(f) + d(f) + |G|)^{O(1)}$ *we can construct a maximal D-order Λ in KG which contains DG.*

PROOF. We can factor the discriminant $d(f)$ by trial division. Once we have the primes dividing $d(f)$, we can compute a $\mathbb{Z}$-basis of the ring of algebraic integers of K in time $\mathrm{size}(f)^{O(1)}$ (cf. Zassenhaus 1967 and Pohst 1989). The rest follows from Theorem 5.4. □

The following statement seems to be new even in the case $K = \mathbb{Q}$.

COROLLARY 5.6. *Let K, f, G be as in the preceding statement. Then the degrees of the irreducible representations of G over K can be computed in deterministic time* $(\mathrm{size}(f) + d(f) + |G|)^{O(1)}$.

PROOF. We consider the Wedderburn decomposition of KG:

$$KG \cong \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_k,$$

where $\mathcal{A}_i \cong \mathrm{M}_{n_i \times n_i}(E_i)$ where n_i is a positive integer and E_i is a skewfield containing K in the center. Let F_i denote the center of $\mathcal{A}_i$. Clearly F_i is a finite extension field of K and $\mathcal{A}_i$ is central simple over F_i.

We write $m_i = \dim_K \mathcal{A}_i$, $l_i = \dim_K E_i$. Straightforward calculation gives that the degree of the irreducible G-modules associated with $\mathcal{A}_i$ (i.e., the dimension over K of the simple $\mathcal{A}_i$-modules) is $\sqrt{m_i l_i}$. It suffices therefore to determine the integers m_i and l_i. The ideals $\mathcal{A}_i$ and the numbers m_i are computed by the deterministic polynomial time method of Friedl & Rónyai (1985), Theorem 7.6.

We turn to the problem of computing the numbers l_i. We compute first a maximal $\mathbb{Z}$-order Λ in KG by using the algorithm of Corollary 5.5. Next we form the $\mathbb{Z}$-orders $\Lambda_i = \mathcal{A}_i \cap \Lambda$ in $\mathcal{A}_i$. This task is easily accomplished because we have $\Lambda_i = e_i \Lambda$, where e_i is the identity element of $\mathcal{A}_i$. Let D_i denote the ring of algebraic integers of F_i. The maximality of Λ implies that Λ_i is a maximal D_i-order in $\mathcal{A}_i$. We intend to use a variant of the method of Rónyai (1992), Theorems 1.1 and 5.1 adapted to our setting at hand to compute $\dim_{F_i} E_i$. This suffices because we already know $\dim_K F_i$ and we have $l_i = \dim_{F_i} E_i \dim_K F_i$. Using the notation of Rónyai (1992), we have $\sqrt{\dim_{F_i} E_i} = \mathrm{lcm}\{m_P\}$ where P ranges over the primes of F_i and m_P denotes the local index of Λ_i at P.

Concerning finite primes P, the key observation is that we have to calculate the local indices m_P of Λ_i only for prime ideals P of D_i which contain a rational prime p dividing $\mid G \mid$ by Reiner (1975), Theorem 41.7. Here again we can use the deterministic factoring method of Berlekamp.

If P is a real prime, then we can not use directly the method of Eberly (1991), as it was done in Rónyai (1992), because this method uses randomization for finding a splitting element in $\mathcal{A}_i$. Recently we have found a deterministic polynomial time algorithm for solving this subtask (Rónyai 1993). By using this procedure we obtain m_P in deterministic polynomial time. This proves the statement. □

Most of the results of this paper, in particular Proposition 4.1 and Theorem 4.5, are applicable to separable algebras over global fields (i.e., number fields and univariate function fields over finite fields). Extending the algorithms of this paper to global fields will be the subject of a subsequent paper.

Acknowledgements

Research partially supported by Hungarian National Foundation for Scientific Research (OTKA), Grant 2581, and EC Cooperative Action IC 1000, Algorithms for Future Technologies (ALTEC).

References

E. R. BERLEKAMP, Factoring polynomials over finite fields. *Bell System Technical Journal* **46** (1967), 1853-1859.

W. M. EBERLY, Decompositions of algebras over **R** and **C**. *Computational Complexity* **1** (1991), 207-230.

K. FRIEDL, L. RÓNYAI, Polynomial time solutions of some problems in computational algebra. *Proc. 17th ACM STOC,* Providence, Rhode Island, 1985, 153-162.

M. HARADA, Hereditary orders. *Trans. Amer. Math. Soc.* **107** (1963), 273-290.

H. JACOBINSKI, Two remarks about hereditary orders. *Proc. Amer. Math. Soc.* **28** (1971), 1-8.

M. E. POHST, Three principal tasks of computational algebraic number theory. *Number theory and applications, Proc. NATO Advanced Study Inst.*, Kluwer Academic Publishers, 1989, 123-133.

I. REINER, *Maximal orders.* Academic Press, 1975.

L. RÓNYAI, Computing the structure of finite algebras. *Journal of Symbolic Computation* **9** (1990), 355-373.

L. RÓNYAI, Algorithmic properties of maximal orders in simple algebras over **Q**. *Computational Complexity* **2** (1992), 225-243.

L. RÓNYAI, A deterministic method for computing splitting elements in simple algebras over **Q**. 1993, accepted for publication in *Journal of Algorithms.*

H. ZASSENHAUS, Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung. *Funktionalanalysis, Birkhäuser*, 1967, 90-103.

Manuscript received February 24, 1992

GÁBOR IVANYOS
Computer and Automation Institute
Hungarian Academy of Sciences
Budapest, Victor Hugo u. 18-22.
H-1132 Hungary
h1510iva@ella.hu

LAJOS RÓNYAI
Computer and Automation Institute
Hungarian Academy of Sciences
Budapest, Victor Hugo u. 18-22.
H-1132 Hungary
h631ron@ella.hu