Recognition of Division Algebras

Gabriele Nebe and Allan Steel

To John Cannon and Derek Holt on the occasions of their significant birthdays, in recognition of distinguished contributions to mathematics

Abstract. An algorithm to construct a maximal order Λ in a finite-dimensional semisimple rational algebra A is presented. The discriminants of the simple components of Λ allow one to read off the Wedderburn structure of A. If A has uniformly distributed invariants, which is the case for centralizer algebras of representations of finite groups, then it suffices to do the calculation over the rational integers.

1 Introduction.

One main task in representation theory of finite groups G is the explicit construction of irreducible matrix representations $\Delta : G \to \mathrm{GL}_n(F)$. There are several methods available for finding some representation of G that contains Δ as a subquotient, such as taking tensor products of known representations or inducing representations from a subgroup. The resulting representation is usually reducible. The paper [3] describes methods to construct irreducible subrepresentations $\Gamma : G \to \mathrm{GL}_n(F)$ when $F = \mathbb{Q}$. For a finite field F, such a representation Γ is irreducible if and only if the endomorphism ring

$$E := \mathrm{End}(\Gamma) = \{x \in F^{n\times n} \mid x\Gamma(g) = \Gamma(g)x \text{ for all } g \in G\}$$

is a field. This condition is equivalent to the case that E is commutative and all minimal polynomials of the generators are irreducible. For a number field F, however, the situation is more complicated because of the existence of noncommutative division algebras. This note presents an algorithm to decide whether E is a division algebra (in which case Γ is irreducible) and to calculate its Schur index. Magma code is available via the homepage of the first author.

2 Semisimple algebras.

We first deal with the problem of finding the building blocks of a finite-dimensional semisimple $\mathbb{Q}$-algebra A. By Wedderburn's theorem, such an algebra is of the form

$$\text{(Wed)} \qquad A = \bigoplus_{i=1}^{\ell} D_i^{n_i\times n_i}$$

for skewfields D_i with center $K_i := Z(D_i)$. Then the center of A is $Z(A) = \oplus_{i=1}^{\ell} K_i$.

Usually such an algebra A arises as the endomorphism algebra of some rational representation of a finite group, but it might also turn up in a different representation, but almost never in the explicit decomposition given in (Wed). From any representation of A it is usually not difficult to calculate the right regular representation, $\mathrm{rrr} : A \to \mathrm{End}_{\mathbb{Q}}(A)$. So we assume that the algebra is given in its right regular representation.

To reduce the problem to simple algebras we need to find the central primitive idempotents of A, and this is easy. For this we start with the regular representation of the center $Z(A) = \mathbb{Q}[z_1, \ldots, z_m]$, where the z_i are $\mathbb{Q}$-algebra generators of $Z(A)$. Since the z_i are pairwise commuting matrices, they can be diagonalized simultaneously and finding the decomposition $Z(A) = \oplus_{i=1}^{\ell} K_i$ is essentially equivalent to factoring the minimal polynomials f_i of the matrices z_i. Note that these are always squarefree rational polynomials, since $Z(A)$ is separable over $\mathbb{Q}$, and therefore they can be read off from the characteristic polynomials which are sometimes easier to compute.

Algorithm to split the center.
Input: Algebra generators $z_1, \ldots, z_m$ of a commutative semisimple $\mathbb{Q}$-algebra Z in the action on some module V.
Output: The decomposition $Z = \oplus_{i=1}^{\ell} K_i$.
Algorithm: (Sketch) Choose some element $z \in Z$ with minimal polynomial, say, f and calculate a non-trivial factorization $f = gh$ and the matrices $g(z)$, $h(z)$. Then $V = \ker(g(z)) \oplus \ker(h(z)) =: V_g \oplus V_h$ is a Z-invariant decomposition of the module V. Continue with V_g in place of V and $Z_g := \mathbb{Q}[h(z)z_1, \ldots, h(z)z_m]$, and similarly with V_h and $Z_h := \mathbb{Q}[g(z)z_1, \ldots, g(z)z_m]$.
If the minimal polynomials of all generators of Z are irreducible over the rationals, then the module V is simple and the action of Z on V is isomorphic to one of the fields K_i.

3 Simple algebras.

We may now assume that $A = D^{n \times n}$ is a simple $\mathbb{Q}$-algebra with center K. Then $d := \dim_{\mathbb{Q}}(A) = n^2 m^2 k$ where $k = \dim_{\mathbb{Q}}(K)$ and $m^2 = \dim_K(D)$. We know k and d and hence $s := nm = \sqrt{d/k} = \sqrt{\dim_K(A)}$. Let R be the ring of integers in K.

3.1 The discriminant of A.

Definition 3.1. *(a) Let* $\mathrm{trred} : A \to \mathbb{Q}, a \mapsto \frac{1}{s}\mathrm{trace}(\mathrm{rrr}(a))$ *denote the reduced trace of* A*. Let* M *be an* R*-order in* A*. Then*

$$M^{\#} := \{a \in A \mid \mathrm{trred}(aM) \subset \mathbb{Z}\}$$

is a $\mathbb{Z}$*-lattice in* A *which contains* M *of finite index* $[M^{\#} : M] =: \mathrm{disc}(M)$*, called the* discriminant of M*. Any two* maximal *orders have the same discriminant which is called* $\mathrm{disc}(A)$*, the* discriminant of A*.*
(b) Let $\mathrm{rrr}_K : A \to K^{s^2 \times s^2}$ *denote the regular representation of the* K*-algebra* A *and let* $\mathrm{trred}_K : A \to K, a \mapsto \frac{1}{s}\mathrm{trace}(\mathrm{rrr}_K(a))$ *denote the reduced trace of* A *as a* K*-algebra.*

Then for any R-order M in A the different

$$M^* := \{a \in A \mid \mathrm{trred}_K(aM) \subset R\}$$

is an R-lattice contained in $M^\#$. The finite R-module $M^*/M \cong \prod R/I_j$ is called the discriminant module *of M and* $\mathrm{discid}(M) := \prod I_j$ *the* discriminant ideal *of M. Since the property of being a maximal order is a local one, the discriminant ideal of a maximal order M does not depend on the choice of M and is denoted by* $\mathrm{discid}(A)$*, the discriminant ideal of A.*

By the local-global principle the algebra A is up to isomorphism uniquely determined by all its completions $A_\wp := K_\wp \otimes_K A$ where $\wp$ runs through the prime ideals of R together with its infinite completions $\mathbb{R} \otimes_K A = \begin{cases} \mathbb{R}^{s\times s} & \text{or} \\ \mathbb{H}^{s/2\times s/2} & \end{cases}$ resp. $\mathbb{C} \otimes_K A = \mathbb{C}^{s\times s}$ for all real resp. complex embeddings of K. Here $\mathbb{H}$ denotes the noncommutative real division algebra

$$\mathbb{H} = \langle 1, i, j, k \mid i^2 = j^2 = k^2 = -1, ij = -ji = k\rangle.$$

Also, an R-order M is a maximal R-order in A, if and only if for all prime ideals $\wp$ of R the completion $M_\wp = R_\wp \otimes_R M$ is a maximal $R_\wp$-order (see [2, Corollary (11.2)]) and the discriminant of M is the product over all discriminants of $M_\wp$,

$$\mathrm{disc}(M) = \prod_\wp \mathrm{disc}(M_\wp), \quad \mathrm{discid}(M) = \prod_\wp \mathrm{discid}(M_\wp).$$

Note that $\mathrm{discid}(M_\wp)$ is the $\wp$-primary component of $\mathrm{discid}(M)$.

Definition 3.2. *The algebra $A_\wp$ is isomorphic to $D_\wp^{t_\wp\times t_\wp}$ where $D_\wp$ is a $K_\wp$-division algebra of dimension $s_\wp^2$ and $t_\wp := s/s_\wp$. The natural number $s_\wp$ is called the* $\wp$-local Schur index *of A.*

Theorem 3.3. *(see [2, Theorem 14.9])* $\mathrm{discid}(D_\wp) = \wp^{s_\wp(s_\wp-1)}$

Since $t_\wp^2 s_\wp(s_\wp - 1) = s(s - t_\wp)$ this yields the following corollary.

Corollary 3.4. $\mathrm{discid}(A) = \prod_\wp \wp^{s(s-t_\wp)}$*, so the local Schur index $s_\wp$ can be obtained from the discriminant ideal of any maximal order in A (and the dimension $s^2 = \dim_K(A)$.)*

Now the global Schur index $m = \dim_K(D)^{1/2}$ is the least common multiple of all local Schur indices (including the real ones) and we will give an algorithm to determine a maximal order in A in the next subsection which yields the local Schur index $s_\wp$ for all finite primes $\wp$ by Corollary 3.4. So it remains to calculate the real Schur-index for all real embeddings $\iota : K \to \mathbb{R}$ (which is 2, if $\mathbb{R} \otimes_\iota A \cong \mathbb{H}^{s/2\times s/2}$ and 1, if this algebra is a matrix ring over the reals). The real Schur index can be read off from the signature of the trace bilinear form

$$T_\iota : A \times A \to \mathbb{R}, (a, b) \mapsto \iota(\mathrm{trred}_K(ab)).$$

Theorem 3.5. *For $n \in \mathbb{N}$ we let $n_+ := n(n+1)/2 \in \mathbb{N}$ and $n_- := n(n-1)/2$.*
(a) The signature of the trace bilinear form on $\mathbb{H}$ is $(1, -3) = (2_-, -2_+)$.
(b) The signature of the trace bilinear form on the matrix ring $\mathbb{R}^{n\times n}$ is $(n_+, -n_-)$.
(c) The signature of T_ι above is $(s_-, -s_+)$ if $\mathbb{R}\otimes_\iota A \cong \mathbb{H}^{t\times t}$ (where $t = s/2$) and $(s_+, -s_-)$ if $\mathbb{R} \otimes_\iota A \cong \mathbb{R}^{s\times s}$.

Proof. (a) is explicit calculation. Note that $(1, i, j, k)$ is an orthogonal basis for the trace form consisting of vectors of norm $(2, -2, -2, -2)$.
(b) The matrix units e_{ij} form a basis for the matrix ring. For $i \neq j$ the pair (e_{ij}, e_{ji}) generates a hyperbolic plane, and for $i = j$, e_{ii} has norm 1. So in total the signature is $(n + n(n-1)/2, -n(n-1)/2)$ as stated.
(c) Follows from (a) and (b) since $\mathbb{H}^{t\times t}$ is the tensor product $\mathbb{H} \otimes \mathbb{R}^{t\times t}$. □

3.2 Constructing a maximal order M in A.

Let Λ be any R-order in A. There is a canonical process, called the radical idealizer process (see [1]), that constructs a canonical overorder of Λ that is hereditary, where we may work locally at one prime ideal at a time. So let $I := \text{discid}(\Lambda)$ be the discriminant ideal and choose some prime ideal $\wp \trianglelefteq R$ that divides I.

Then the $\wp$-Jacobson radical $J_\wp(\Lambda)$ is the intersection of all maximal right ideals of Λ that contain $\wp\Lambda$. It is a two-sided ideal of Λ, in fact the smallest ideal I of Λ, such that Λ/I is a semisimple $R/\wp$-algebra.

Definition 3.6. *Let L be a full R-lattice in A. The* right order *of L is*

$$O_r(L) := \{a \in \mathcal{A} \mid La \subseteq L\}.$$

The following characterization of hereditary orders is shown in [2, Theorem 39.11]

Theorem 3.7. *Let Λ be an R-order in A. Then $\Lambda = O_r(J_\wp(\Lambda))$ if and only if the completion $\Lambda_\wp$ is hereditary.*

Remark 3.8. *(cf. [1]) Letting $\Lambda_0 := \Lambda$ and $\Lambda_{n+1} := O_r(J_\wp(\Lambda_n))$ for $n = 0, 1, 2, \ldots$ defines a canonical process, the so-called* radical idealizer process *that constructs from an R-order Λ in A successively larger R-orders $\Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_N = \Lambda_{N+1}$, the so-called* $\wp$-radical idealizer chain *of Λ and $\Lambda_N =: \mathcal{H}_\wp(\Lambda)$ the* $\wp$-head order.

Note that the calculation of $J_\wp(\Lambda)$ as well as of its idealizer only involves solving linear equations over the finite residue class field $R/\wp$, since $\Lambda_i \subset \wp^{-1}\Lambda_{i-1}$ for all $1 \leq i \leq N$.

Corollary 3.9. *Let $\{\wp_1, \ldots, \wp_f\}$ be the set of prime ideals that divide* discid(Λ). *Then*

$$\mathcal{H}(\Lambda) := \mathcal{H}_{\wp_f}(\mathcal{H}_{\wp_{f-1}}(\ldots \mathcal{H}_{\wp_2}(\mathcal{H}_{\wp_1}(\Lambda))\ldots))$$

is a hereditary overorder of Λ, called the head order *of Λ.*

Note that the head order of Λ does not depend on the ordering of the prime ideals $\wp_i$, since for different prime ideals $\wp \neq \wp'$ the operators $\mathcal{H}_\wp$ and $\mathcal{H}_{\wp'}$ commute.

[2, Theorem (39.14)] gives a complete description of the hereditary orders over complete discrete valuation rings $R_\wp$ in central simple algebras $A_\wp = D_\wp^{m\times m}$: Let Δ denote the unique maximal $R_\wp$-order in $D_\wp$ and P the maximal ideal in Δ. Then any hereditary $R_\wp$-order in $A_\wp$ is conjugate to

$$\mathcal{H}(n_1,\ldots,n_k) := \{(X_{ij})_{i,j=1}^k \in \Delta^{m\times m} \mid X_{ij} \in \Delta^{n_i\times n_j} \text{ for all } i,j \text{ and } X_{ij} \in P^{n_i\times n_j} \text{ if } i<j\}$$

for some $(n_1,\ldots,n_k) \in \mathbb{N}^k$, $n_1+\ldots+n_k = m$.

We now use the fact that $\mathcal{H}(\Lambda)$ is hereditary to construct a maximal overorder of $\mathcal{H}(\Lambda)$. Elementary calculations show that the right idealizer of any maximal 2-sided ideal of a non-maximal hereditary order $\mathcal{H}$ is a proper (hereditary) overorder of $\mathcal{H}$ as explicitly stated in the following lemma.

Lemma 3.10. *The maximal two-sided ideals of the hereditary order $\mathcal{H}(n_1,\ldots,n_k)$ defined above are the ideals*

$$I_\ell := \{X = (X_{ij})_{i,j=1}^k \in \mathcal{H}(n_1,\ldots,n_k) \mid X_{\ell,\ell} \in P^{n_\ell\times n_\ell}\}$$

for $\ell = 1,\ldots,k$. The right idealizer of I_ℓ is the proper overorder

$$O_r(I_\ell) = \mathcal{H}(n_1,\ldots,n_{\ell-1},n_\ell+n_{\ell+1},n_{\ell+2},\ldots,n_k)$$

$(1\le \ell < k)$ and $O_r(I_k) =$

$$\{(X_{ij})_{i,j=1}^k \mid X_{ij} \in \Delta^{n_i\times n_j} \textit{ for } (i,j)\neq(k,1), X_{k1} \in (P^{-1})^{n_k\times n_1} \textit{ and } X_{ij} \in P^{n_i\times n_j} \textit{ if } i<j\}$$

$\sim \mathcal{H}(n_2,\ldots,n_{k-1},n_k+n_1)$.

Successively replacing the order $\mathcal{H}(n_1,\ldots,n_k)$ by the right idealizer of any of its maximal 2-sided ideals hence constructs a maximal overorder in exactly $k-1$ steps. Since we will perform all calculations over the rationals, we give the final algorithm in the end.

3.3 Rational computations.

The implemented algorithm only uses calculations over the rational integers and not over the ring of integers R. The only ingredients we need from R are its discriminant $\delta = \mathrm{disc}(R)$ and the possibility to decompose rational primes into a product of prime ideals in R.

Lemma 3.11. *For any R-order Λ in A the discriminant*

$$\mathrm{disc}(\Lambda) = N_{K/\mathbb{Q}}(\mathrm{discid}(\Lambda))\delta^{s^2}$$

where $N_{K/\mathbb{Q}}$ denotes the norm of K over $\mathbb{Q}$.

Proof. $\Lambda^\# := \{a \in A \mid \mathrm{trred}(a\Lambda) \subset \mathbb{Z}\} = \{a\in A \mid \mathrm{trred}_K(a\Lambda) \subset R^\#\} = R^\#\Lambda^*$. Now the order of $\Lambda^\#/\Lambda$ is

$$|\Lambda^\#/\Lambda| = |R^\#\Lambda^*/\Lambda^*||\Lambda^*/\Lambda| = \delta^{s^2} N_{K/\mathbb{Q}}(\mathrm{discid}(\Lambda))$$

since $\delta = |R^\#/R|$. □

From the discriminant of a maximal order we can read off all local Schur indices $s_\wp$ and hence with Theorem 3.5 the global Schur index m of the algebra A, if A has uniformly distributed invariants, which means that K is a Galois extension of $\mathbb{Q}$ and the local Schur index $s_\wp$ does not depend on the prime ideal $\wp$ of R but only on the rational prime p contained in $\wp$ which allows one to define $s_p := s_\wp$. Epimorphic images of group algebras have uniformly distributed invariants (see [4]) and so do their centralizing algebras.

Corollary 3.4 then yields the following theorem.

Theorem 3.12. *Assume that A has uniformly distributed invariants and let $s_p := s_\wp$ be the $\wp$-local Schur index for any prime ideal $\wp$ of R that contains the rational prime p and $n_p := N_{K/\mathbb{Q}}(\wp)$, $d_p := |\{\wp \mid \text{ prime ideal with } p \in \wp\}|$. Then*

$$\mathrm{disc}(A) = \delta^{s^2} \prod_p n_p^{d_p s(s-t_p)} \text{ where } t_p = \frac{s}{s_p}.$$

In particular, the local Schur index s_p can be obtained from the discriminant $\mathrm{disc}(A)$ of any maximal order in A. To construct a maximal order in A the method from Section 3.2 is used, where all computations are done over the rationals. To obtain the head order $\mathcal{H}(\Lambda)$ we replace the discriminant ideal by the quotient $D := \mathrm{disc}(\Lambda)/(\delta^{s^2}) \in \mathbb{Z}$ and the prime ideals $\wp$ dividing $\mathrm{discid}(\Lambda)$ by the prime numbers p that divide D.

Algorithm to calculate a maximal overorder.

Input: An order $\Lambda = \langle B^{(1)}, \dots, B^{(d)} \rangle_{\mathbb{Z}}$ in a finite dimensional semisimple $\mathbb{Q}$-algebra A in its right regular representation
(so $d = \dim_{\mathbb{Q}}(A)$ and $B^{(i)} \in \mathbb{Z}^{d\times d}$ with $B^{(j)}B^{(i)} = \sum_{k=1}^{d} B^{(i)}_{j,k} B^{(k)}$).

Output: A maximal overorder Γ of Λ in its right regular representation.

Algorithm:

(1) Calculate a canonical hereditary overorder.

For all primes p that divide $D = \mathrm{disc}(\Lambda)/(\delta^{s^2}) \in \mathbb{Z}$ do

(lreg) Calculate $C^{(1)}, \dots, C^{(d)} \in \mathbb{Z}^{d\times d}$ with $C^{(i)}_{j,k} = B^{(j)}_{i,k}$ for $1 \le i, j, k \le d$.

(msub) Calculate the maximal submodules of the natural module for the $\mathbb{F}_p$-algebra

$$E = \langle \overline{C}^{(i)}, \overline{B}^{(i)} \mid 1 \le i \le d \rangle_{\mathbb{F}_p} \le \mathbb{F}_p^{d\times d}.$$

Their intersection $\overline{J}$ is the Jacobson radical of $\Lambda/p\Lambda$.

(rid) Calculate the basismatrix T of the Jacobson radical $J = J_p(\Lambda)$ as the full preimage of $\overline{J}$. Then a $\mathbb{Z}$-basis of the right idealizer

$$O_r(J) = \langle \frac{1}{p} T B^{(i)} T^{-1} \mid 1 \le i \le d \rangle_{\mathbb{Z}} \cap \mathbb{Z}^{d\times d}$$

can be determined by solving a system of linear equations over $\mathbb{F}_p$.

(loop) If $O_r(J) \neq \Lambda$ then replace Λ by $O_r(J)$ and $(B^{(1)}, \dots, B^{(d)})$ by the right regular representation of $O_r(J)$ and repeat with (lreg).
Else end the loop for the prime p and treat the next prime.

Recalculate the discriminant $D := \mathrm{disc}(\Lambda)/(\delta^{s^2}) \in \mathbb{Z}$.
(2) Calculate a maximal overorder of the hereditary order Λ
using the same procedure as in (1) with the Jacobson radical $J_p(\Lambda)$ replaced by any maximal two-sided ideal S of Λ that contains $p\Lambda$. Output Λ.

4 Examples.

Examples of orders in simple algebras may be easily constructed as cyclotomic orders. For a prime p, let $z_p \in \mathbb{Z}^{(p-1)\times(p-1)}$ denote the companion matrix of the p-th cyclotomic polynomial and let $a \in \{1, \dots, p-1\}$ be minimal such that $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. Then for $n \in \mathbb{Z}$ the cyclotomic $\mathbb{Z}$-order

$$\mathcal{O}_{p,n} := \langle Z_p := \mathrm{diag}(z_p, z_p^a, \dots, z_p^{a^{p-2}}), \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 1 \\ n & 0 & \dots & 0 & 0 \end{pmatrix} \rangle \leq \mathbb{Z}^{(p-1)^2\times(p-1)^2}$$

is a $\mathbb{Z}$-order in a central simple $\mathbb{Q}$-algebra of dimension $(p-1)^2$ over $\mathbb{Q}$. We tested our program using extensions of the form $R \otimes \mathcal{O}_{p,n}$ for an order R in a number field.

p	5	5	5	5	7	7	7
n	2	2	2	2	15	15	15
R	$\mathbb{Z}$	$\mathbb{Z}[\sqrt{-2}]$	$\mathbb{Z}[\sqrt{5}]$	$\mathbb{Z}[\sqrt{3}]$	$\mathbb{Z}$	$\mathbb{Z}[\sqrt{3}]$	$\mathbb{Z}[\sqrt{-5}]$
(1)	$2^1 5^2$	$2^8 5^1$	$2^5 5^8$	$2^3 3^6 5^1$	$3^1 5^1 7^1$	$3^4 5^1 7^1$	$3^1 5^4 7^1$
(2)	$2^1 5^1$	$2^1 5^2$	$2^2 5^1$	$2^1 5^2$	$3^1 5^1 7^6$	$3^1 5^2 7^6$	$3^1 5^1 7^{11}$
SI	$2^4 5^4 \infty^2$	$2^2 5^2$	$2^2 5^2 \infty^2$	$2^2 5^2 \infty^2$	$3^6 5^6 \infty^2$	$3^3 5^3 \infty^2$	$3^6 5^3$

The rows marked by (1) and (2) give the number of times we went through the respective loops in the algorithm as the exponent of the relevant prime. The last line marked by (SI) contains the local Schur indices as exponents of the relevant primes.

References

[1] H. Benz, H. Zassenhaus, Über verschränkte Produktordnungen. J. Number Theory **20** (1985), 282-298.

[2] I. Reiner, *Maximal orders.* Academic Press 1975.

[3] A. Steel, Constructing Irreducible Rational Representations of Finite Groups (in preparation).

[4] T. Yamada, *The Schur subgroup of the Brauer groups.* Springer LNM 397 (1974)