

# Splitting full matrix algebras over number fields

Lajos Rónyai

joint work with Gábor Ivanyos, Ádám D. Lelkes, and Josef Schicho

AANT, RICAM, Linz, November 28, 2013

- Background on algorithms for algebras
- Orders
- Splitting matrix algebras over  $\mathbb{Q}$
- Extension to number fields
- Applications
- Some improvements
- Open problems

# The computational model

Exact (symbolic) computations of substructures

Input and results (algebras) will be given by bases

Ground fields:

Algebraic number fields:  $\mathbb{K} = \mathbb{Q}[x]/(f)$ ,  $f(x) \in \mathbb{Z}[x]$  irreducible

Finite fields:  $\mathbb{K} = \mathbb{F}_q$ .

Global function fields:  $\mathbb{K} = \mathbb{F}_q(x)$ , and finite extensions

**Size**= number of bits representing the object

We consider polynomial time algorithms (deterministic, randomized, ff)

# Structure constants representation

Let  $\mathcal{A}$  be an algebra over  $\mathbb{K}$  with basis  $a_1, \dots, a_m$ . Then multiplication can be specified by giving

$$a_i \cdot a_j = \gamma_{ij1}a_1 + \gamma_{ij2}a_2 + \dots + \gamma_{ijm}a_m.$$

The  $\gamma_{ijk} \in \mathbb{K}$  are the *structure constants*. Multiplication table of the basis.

Essentially the regular representation (possibly via Dorroh's extension): one may assume

$$\mathcal{A} \leq M_{m+1}(\mathbb{K}).$$

- arithmetic over  $\mathbb{K}$
- linear algebra (solving systems of linear equations) over  $\mathbb{K}$
- factoring univariate polynomials over  $\mathbb{K}$  (Berlekamp, LLL, van Hoeij)
- approximate computations with real algebraic numbers
- approximate lattice basis reduction (LLL, Buchmann)

# Computing the radical of $\mathcal{A} \leq M_n(\mathbb{K})$

An  $a \in \mathcal{A}$  is nilpotent, if  $a^d = 0$  for some  $d$ .  $\text{Rad}(\mathcal{A})$  is the largest ideal of  $\mathcal{A}$  consisting of nilpotent elements.

Polynomial time algorithms based on linear algebra

## Theorem (Dickson '23)

Assume  $\text{char } \mathbb{K} = 0$ . Then

$\mathcal{A}$  is nilpotent  $\Leftrightarrow \forall a \in \mathcal{A}, \text{Tr}(a) = 0$ .

$$\text{Rad}(\mathcal{A}) = \{a \in \mathcal{A} \mid \forall b \in \mathcal{A} \cup \{I\}, \text{Tr}(ba) = 0\}.$$

## Corollary

Assume  $\text{char } \mathbb{K} = 0$ ,  $B = (\text{a basis of } \mathcal{A}) \cup \{I\}$ . Then

$$\text{Rad}(\mathcal{A}) = \{a \in \mathcal{A} \mid \forall b \in B, \text{Tr}(ba) = 0\}.$$

# Computing the radical of $\mathcal{A} \leq M_n(\mathbb{K})$

Over  $\mathbb{K} = \mathbb{F}_p$  [Friedl, R '85]: Compute a sequence of ideals

$$\mathcal{A} = \mathcal{A}_0 \supseteq \mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \dots \supseteq \mathcal{A}_{\lceil \log_p n \rceil} = \text{Rad}(\mathcal{A})$$

## Extensions

- $\mathbb{K} = \mathbb{F}_q$  [Eberly '89]
- $\mathbb{K} = \mathbb{F}_q(x)$  [Ivanyos, R, Szántó '94]
- Arbitrary  $\mathbb{K}$  [Cohen, Ivanyos, Wales '96]  
 $\mathcal{A}_i \longrightarrow \mathcal{A}_{i+1}$  : system of semilinear equations over  $\mathbb{K}$   
Equations: from coefficients of the char. polynomial
- Radical (nil, solvable) algorithms for Lie algebras [R'90]

# Wedderburn decomposition

Assume  $\text{Rad}(\mathcal{A}) = (0)$ . Then  $\mathcal{A}$  is the direct sum of its minimal ideals:

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_k.$$

This is reflected in the central part:

$$Z(\mathcal{A}) = Z(\mathcal{A}_1) \oplus Z(\mathcal{A}_2) \oplus \cdots \oplus Z(\mathcal{A}_k).$$

Let  $0 \neq e_i \in Z(\mathcal{A}_i)$ . Then

$$\mathcal{A}_i = e_i \mathcal{A}.$$

Finding the  $Z(\mathcal{A}_i)$ : reduced in polynomial time to factoring univariate polynomials over  $\mathbb{K}$



# Algorithms for Wedderburn decomposition

- Over finite fields and number fields: [Friedl, R '85] — an iterative algorithm
- Over sufficiently large fields [Eberly '91] — one round, randomized  
Pick a random  $a \in Z(\mathcal{A})$ , let  $f$  be the min. pol. of  $a$ . Then

$$Z(\mathcal{A}) \cong \mathbb{K}[x]/(f(x))$$

factors of  $f \leftrightarrow$  Wedderburn components of  $\mathcal{A}$

- Over global function fields:  
[Ivanyos, R, Szántó '94] reduced to factoring polynomials over the prime field

## Theorem (Wedderburn)

A simple  $\mathbb{K}$ -algebra  $\mathcal{A}$  is isomorphic to  $M_k(\mathbb{D})$ , for a (skew)field  $\mathbb{D}$  with  $Z(\mathbb{D}) \supseteq \mathbb{K}$  and positive integer  $k$ .

**Explicit isomorphism problem:** given  $\mathcal{A}$ , find  $k$ ,  $\mathbb{D}$  and  $\cong$ .

- $\mathbb{K}$  is finite:
  - [R '90] randomized poly time
  - [Eberly, Giesbrecht '97] randomized  $\approx O(n^3)$
  - [Ivanyos, Karpinski, R, Saxena '11] deterministic polynomial time for  $\dim \mathcal{A}$  bounded
- $\mathbb{K} = \mathbb{R}$  or  $\mathbb{K} = \mathbb{C}$ :
  - [Eberly '91] randomized poly time
  - derandomized [R; de Graaf, Ivanyos '93, '98]

# Explicit isomorphism over number fields

- Difficult: ( $\succ$  factoring integers) [R '88], [Voight '10]
- $\dim e\mathcal{A}e \prec$  factorization [Ivanyos, R '93]
- **Problem:** is explicit isomorphism  $\prec$  factorization?
- **ff-algorithm:** allowed to call an oracle for factoring integers, and for factoring univariate polynomials over finite fields
  
- Yes for  $\mathbb{K} = \mathbb{Q}$ ,  $\dim \mathcal{A} = 4$  [Ivanyos, Szántó '94]
- Yes for  $\mathcal{A} = M_n(\mathbb{K})$ , with  $\mathbb{K}$  and  $n$  small [Ivanyos, R, Schicho '12]
- Improvement for  $\mathbb{K} = \mathbb{Q}$  and  $n$  small [Lelkes, R '13]

Non conventional applications: rational parametrization of varieties,  $n$ -descent for elliptic curves [Cremona, Fisher, O'Neil, Simon, Stoll, '08, '09, '11]

**Integral element:** root in  $\mathcal{A}$  of a monic polynomial with integer coefficients

**Order:** Large subring of  $\mathcal{A}$  consisting of integral elements

**Full lattice in  $\mathcal{A}$ :** finitely generated  $\mathbb{Z}$ -submodule  $M$  with  $\mathbb{Q}M = \mathcal{A}$

**Order:** a subring  $\Lambda \leq \mathcal{A}$  with  $1$  of  $\mathcal{A}$  in  $\Lambda$  such that  $\Lambda$  is a full lattice in  $\mathcal{A}$

**Maximal order:** maximal w.r.t. inclusion (not unique)

- The sublattice generated by the basis elements and 1, if the structure constants are integers
- $\mathbb{Z}G$  in the group algebra  $\mathbb{Q}G$  for a finite group  $G$
- **Algebraic integer matrices:**  $\mathbb{K}$  number field,  
 $R = \{\text{alg. integers in } \mathbb{K}\}$   
 $M_n(R)$  in  $M_n(\mathbb{K})$  is a maximal order
- Stabilizers of lattices:  $M$  a full lattice in  $\mathcal{A}$   
 $\mathcal{O}(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$

# Constructing maximal orders

Given a semisimple algebra  $\mathcal{A}$  over  $\mathbb{K}$ , find a maximal order  $\Lambda \leq \mathcal{A}$

[Ivanyos, R '93] – a polynomial time ff-algorithm

Starts with an initial order  $\Gamma$  and then enlarges it into a maximal order  $\Lambda \geq \Gamma$

Suppose that  $\mathcal{A} \cong M_n(\mathbb{D})$ . From  $\Lambda$  one can efficiently determine  $n$

Use of factoring: we need only the prime factors of  $d(\Gamma)$

# Golden rings



# Golden algebra, golden ring, golden code

Ground field:  $\mathbb{K} = \mathbb{Q}(i)$  – the Gaussian rationals

$$\mathcal{GA} = \mathbb{K}(x, u; x^2 = 5, u^2 = i, xu = -ux)$$

$$\mathcal{GO} = \mathbb{Z}[i][x, u] \leq \mathcal{GA} \quad \text{the golden ring}$$

It leads to a highly efficient *space-time* radio code (Yao, Wornell; Dayal, Varanasi; Belfiore, Rekaya, Viterbo)

$\mathcal{GO}$  is a lattice with very small discriminant consisting of nonsingular **integral** matrices



Hollanti, Lahtonen, Ranto, Vehkalahti: find orders similar to  $\mathcal{GO}$  in other cyclic algebras

IR-algorithm: given an order  $\Gamma \leq \mathcal{A}$  in a finite dimensional simple algebra  $\mathcal{A}$  over  $\mathbb{Q}$ ; it computes a maximal order  $\Lambda \geq \Gamma$

Polynomial time ff-algorithm

de Graaf: MAGMA -implementation

With that better codes can be obtained. For example in

$$\mathcal{GA}+ = \mathbb{K}(x, u; x^2 = 2 + i, u^2 = i, xu = -ux)$$

the order  $\Gamma = \mathbb{Z}[i][x, u]$  is not maximal. The max. order  $\Lambda \supset \Gamma$  obtained by the IR-algorithm gives a better code

Engineering application of non commutative algebraic number theory

## Theorem

*Let  $\mathbb{K}$  be an algebraic number field of degree  $d$  and discriminant  $\Delta$  over  $\mathbb{Q}$ . Let  $\mathcal{A}$  be an associative algebra over  $\mathbb{K}$  given by structure constants such that  $\mathcal{A} \cong M_n(\mathbb{K})$  for some positive integer  $n$ .*

*Suppose that  $d$ ,  $n$  and  $|\Delta|$  are bounded. Then an isomorphism  $\mathcal{A} \rightarrow M_n(\mathbb{K})$  can be constructed by a polynomial time ff-algorithm. The time bound of our algorithm depends polynomially on  $|\Delta|$  and exponentially on  $n$  and  $d$ .*

Proof will be outlined for the case  $\mathbb{K} = \mathbb{Q}$

The general case follows by extending the argument via the canonical embedding  $\mathbb{K} \rightarrow \mathbb{R}^d$

## Theorem

Let  $\Lambda$  be a maximal order in  $\mathcal{A} \leq M_n(\mathbb{R})$ ,  $\mathcal{A} \cong M_n(\mathbb{Q})$ . Then there exists an element  $C \in \Lambda$  which has rank 1 as a matrix, and whose Frobenius norm  $\|C\|$  is less than  $n$ .

The Frobenius norm of a matrix  $X \in M_n(\mathbb{R})$  is  $\|X\| = \sqrt{\text{Tr}(X^T X)}$

We have

$$\Lambda = PM_n(\mathbb{Z})P^{-1}$$

for some  $P \in GL_n(\mathbb{R})$

Dividing by  $|\det P|^{1/n}$  we may assume  $P \in M_n(\mathbb{R})$ ,  $\det P = \pm 1$

Let  $\rho$  be the left ideal of  $M_n(\mathbb{Z})$  of all matrices which are 0 except in the first column

$\rho$  is a lattice of covolume 1 in the space  $S \cong \mathbb{R}^n$  of all real matrices having all zeros outside the first column

$L = P\rho$  is a sublattice of  $S$ , with covolume 1

Apply **Minkowski's theorem** to  $L$  in  $S$  and to the ball of radius  $\sqrt{n}$  in  $S$  centered at the zero matrix

The volume of the ball is more than  $2^n$  – contains  $2^n$  internally disjoint copies of the  $n$ -dimensional unit cube

There exists nonzero  $B \in \rho$  such that  $PB$  has length  $< \sqrt{n}$

$B$  and hence  $PB$  is a rank 1 matrix

Next consider the transpose of this argument with  $P^{-1}$  in the place of  $P$

There exists a nonzero integer matrix  $B'$ , which is 0 everywhere except in the first row, such that  $B'P^{-1}$  has length  $< \sqrt{n}$

$C := PBB'P^{-1}$  meets the requirements

It is in  $\Lambda$  because  $BB' \in M_n(\mathbb{Z})$ , and

$$\|C\| = \|(PB)(B'P^{-1})\| \leq \|PB\| \cdot \|B'P^{-1}\| < (\sqrt{n})^2 = n$$

Finally

$$\text{rank } BB' = \text{rank } C = 1.$$

$$\gamma_n = \sup_L \frac{\lambda_1(L)^2}{(\det L)^{2/n}},$$

where  $L$  is over all full lattices in  $\mathbb{R}^n$ , and  $\lambda_1(L)$  is the length of the shortest nonzero vector of  $L$ .

$\sqrt{\gamma_n}$ : diameter of spheres at the densest lattice based packing.

$n$	1	2	3	4	5	6	7	8	24
$\gamma_n^n$	1	$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	$2^8$	$4^{24}$

For large  $n$

$$\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1.745}{2\pi e}.$$

In fact, we proved also  $\|C\| \leq \gamma_n$ , and even  $\|C\| \leq \gamma'_n$ , where  $\gamma'_n$  is the Bergé-Martinet constant.

# The Bergé-Martinet constant

$$\gamma_n = \sup_L \frac{\lambda_1(L)\lambda_1(L^*)}{(\det L)^{2/n}},$$

where  $L$  is over all full lattices in  $\mathbb{R}^n$ , and  $L^*$  is the dual lattice of  $L$

$$L^* = \{\mathbf{y} \in \mathbb{R}^n, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for every } \mathbf{x} \in L\}.$$

Clearly  $\gamma'_n \leq \gamma_n$ .



## Lemma (Fisher '07)

Let  $X \in M_n(\mathbb{C})$  be a matrix such that  $\det X$  is an integer, and  $\|X\| < \sqrt{n}$ . Then  $X$  is a singular matrix.

**Proof.** Let  $X = QR$  be the QR decomposition of  $X$ ,  $Q$  unitary,  $R$  upper triangular with diagonal entries  $r_1, r_2, \dots, r_n$ . We have

$$\begin{aligned} |\det X|^{2/n} &= (|r_1|^2 |r_2|^2 \cdots |r_n|^2)^{1/n} \leq \\ &\leq \frac{1}{n} (|r_1|^2 + |r_2|^2 + \cdots + |r_n|^2) \leq \frac{1}{n} \|R\|^2 = \frac{1}{n} \|X\|^2 < 1. \end{aligned}$$

Note that  $\|X\| = \sqrt{\operatorname{Tr}(X^*X)} = \sqrt{\operatorname{Tr}(R^*R)}$  as  $Q^*Q = I$ . We conclude that  $\det X = 0$ .  $\square$

## Lemma

Let  $X \in M_n(\mathbb{Q})$  be a matrix whose characteristic polynomial has integral coefficients, and  $\|X\| < 1$ . Then  $X$  is a nilpotent matrix.

**Proof.** [G. Kós] The eigenvalues of  $X$  are algebraic integers, hence the eigenvalues of  $X^t$  are algebraic integers as well, for any  $t \in \mathbb{N}^+$ . We infer that  $X^t$  has char. poly. with integral coefficients. The norm condition implies

$$X^t \rightarrow O \text{ as } t \rightarrow \infty,$$

hence  $X^t = O$  for  $t$  large.  $\square$

The bound is sharp:

$$X = \begin{pmatrix} 1 & & \\ & \frac{1}{n} & \\ & & \ddots \\ & & & \frac{1}{n} \end{pmatrix}_{i,j=1}^n.$$

$\Gamma$  is a full lattice in  $\mathbb{R}^m$  with basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  over  $\mathbb{Z}$  such that

$$|\mathbf{b}_1| \cdot |\mathbf{b}_2| \cdots |\mathbf{b}_m| \leq c_m \cdot \det(\Gamma)$$

The LLL algorithm achieves  $c_m = 2^{m(m-1)/4}$

The approximate version of LLL by [Buchmann '94] gives

$$c_m := (\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$$

$\gamma_m$  is Hermite's constant

Lemma (H. W. Lenstra '83)

$\Gamma$  is a full lattice in  $\mathbb{R}^m$  with basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  over  $\mathbb{Z}$  such that

$$|\mathbf{b}_1| \cdot |\mathbf{b}_2| \cdots |\mathbf{b}_m| \leq c_m \cdot \det(\Gamma)$$

holds for a real number  $c_m > 0$ . Suppose that

$$\mathbf{v} = \sum_{i=1}^m \alpha_i \mathbf{b}_i \in \Gamma, \quad \alpha_i \in \mathbb{Z}.$$

Then we have  $|\alpha_i| \leq c_m \frac{|\mathbf{v}|}{|\mathbf{b}_i|}$  for  $i = 1, \dots, m$ .

The proof is Cramer's rule and Hadamard's bound.

# The algorithm for $\mathbb{K} = \mathbb{Q}$

Input:  $\mathcal{A} \cong M_n(\mathbb{Q})$ , given by a basis (of  $m = n^2$  vectors) and structure constants over  $\mathbb{Q}$

Output:  $C \in \mathcal{A}$ ,  $\text{rank } C = 1$

Note that  $M = \mathcal{A}C$  is an  $n$  dimensional  $\mathcal{A}$  module, hence left multiplication on  $M$  gives an  $\mathcal{A} \rightarrow M_n(\mathbb{Q})$  isomorphism

# The algorithm for $\mathbb{K} = \mathbb{Q}$

- 1 Use the IR algorithm to construct a maximal order  $\Lambda$  in  $\mathcal{A}$ .
- 2 Compute an  $\mathcal{A} \hookrightarrow M_n(\mathbb{R})$ . Use the derandomization from [de Graaf, Ivanyos '00] of [Eberly '91]. This gives a  $\|\cdot\|$  on  $\mathcal{A}$ .
- 3 Compute a sufficiently precise rational approximation  $A$  of our basis  $B$  of  $\Lambda$  by the method of [Schönhage '82].
- 4 Compute a reduced basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  of the lattice  $\Lambda \subset \mathbb{R}^m$  by the LLL algorithm on  $A$ . We have the bigger  $c_m$ .
- 5 If a  $\mathbf{b}_i$  is singular, then there are two cases. If  $\text{rank } \mathbf{b}_i = 1$ , then we STOP with the output  $C := \mathbf{b}_i$ . Else, if  $1 < \text{rank } \mathbf{b}_i < n$ , then we compute the the right identity element  $e$  of  $\mathcal{A}\mathbf{b}_i$ , set  $\mathcal{A} := e\mathcal{A}e$  and go back to Step 1.
- 6 Here  $|\mathbf{b}_i| \geq \sqrt{n}$  for every  $i$ . Generate  $C = \sum_{i=1}^m \alpha_i \mathbf{b}_i$ , where  $\alpha_i \in \mathbb{Z}$ ,

$$|\alpha_i| \leq c_m \frac{n}{|\mathbf{b}_i|} \leq c_m \sqrt{n}$$

until a rank 1  $C$  is found. Output this  $C$ .

If we have sufficient (polynomial) precision at ③, then by [Buchmann '94] after ④ we have

$$|\mathbf{b}_1| |\mathbf{b}_2| \cdots |\mathbf{b}_m| \leq (\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}.$$

When at ⑤, we have  $\text{rank } e = k$ , then it is easy to see that

$$e\mathcal{A}e \cong M_k(\mathbb{Q}).$$

A rank 1 element of  $e\mathcal{A}e$  has rank 1 in  $\mathcal{A}$  as well.

The theorem and the lemma (latter applied for  $\mathbf{v} := C$  and  $|\mathbf{v}| \leq n$ ) show that an element  $C$  with rank one exists at ⑥.

① runs in polynomial time as an ff-algorithm.

② , ④ and ⑤ can be done in deterministic polynomial time.

At ③ the precision parameter is polynomial in the input size, hence Schönhage's approximation algorithm runs in polynomial time.

The number of jumps back to ① is bounded, hence each Step is carried out in a bounded number of times.

Finally, the number of elements  $C$  enumerated at ⑥ is at most  $(2c_m\sqrt{n} + 1)^m$ .



# The general case

$\mathbb{K}$  be a number field of degree  $d$  over  $\mathbb{Q}$ , the maximal order of  $\mathbb{K}$  is  $R$ , the discriminant of  $R$  is  $\Delta$ .

Let  $\mathcal{A}$  be a central simple algebra over  $\mathbb{K}$  such that  $\mathcal{A} \cong M_n(\mathbb{K})$ , and let  $\Lambda$  be a maximal order in  $\mathcal{A}$ .

$\Lambda$  is isomorphic to

$$\Lambda' := \begin{pmatrix} R & \cdots R & J^{-1} \\ \vdots & \ddots & \vdots \\ R & \cdots R & J^{-1} \\ J & \cdots J & R \end{pmatrix},$$

where  $J$  is a fractional ideal in  $\mathbb{K}$ .

Let  $\sigma_1, \dots, \sigma_r$  be the embeddings of  $\mathbb{K}$  into  $\mathbb{R}$  and  $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$  be the non-real embeddings of  $\mathbb{K}$  into  $\mathbb{C}$ ; we have  $d = r + 2s$ .

For  $1 \leq i \leq r + s$  consider an embedding  $\phi_i$  of  $\mathcal{A}$  into  $M_n(\mathbb{C})$ , which extends  $\sigma_i$  (for  $i \leq r$  we require  $\phi_i(\mathcal{A}) \leq M_n(\mathbb{R})$ ). Such embeddings are poly. time computable.

Set

$$b = \left( \left( \frac{2}{\pi} \right)^{2sn} \Delta^n \right)^{\frac{1}{nd}} = \left( \frac{2}{\pi} \right)^{\frac{2s}{d}} \Delta^{\frac{1}{d}}.$$

## Theorem

*There exists a rank one element  $x \in \Lambda$  such that the entries of the matrices  $\phi_i(x)$  for  $i = 1, \dots, s + r$  all have absolute value  $\leq b$ .*

The proof is similar to the case  $\mathbb{K} = \mathbb{Q}$ . Here we employ Minkowski's Thm to a lattice in  $\mathbb{R}^{nd}$ .

Some special cases:

1.  $\mathbb{K} = \mathbb{Q}$ ,  $R = \mathbb{Z}$ , then  $\Delta = 1$ ,  $s = 0$ , hence  $b = 1$ . We have  $x \in \Lambda$  which has rank 1 as a matrix from  $M_n(\mathbb{Q})$ , and with respect to  $\mathcal{A} \hookrightarrow M_n(\mathbb{R})$  has elements of absolute value at most 1.
2. If  $D > 0$  is a squarefree integer,  $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ , then  $\Delta = D$ , if  $D$  is congruent to 1 modulo 4, and  $\Delta = 4D$ , if  $D$  is congruent to 3 modulo 4.

Then  $s = 0$ ,  $d = 2$ , hence  $b \leq 2\sqrt{D}$ .

A general variant of Fischer's Lemma.

### Lemma

*Let  $y \in \Lambda$  be an element such that  $\|\phi_i(y)\| \leq \sqrt{n}$  holds for  $i = 1, \dots, r + s$ . Then  $y$  is a zero divisor in  $\mathcal{A}$ .*

The algorithm works with a reduced basis of the lattice  $\Gamma$  of vectors

$(\phi_1(y), \dots, \phi_r(y), \Re(\phi_{r+1}(y)), \Im(\phi_{r+1}(y)), \dots, \Re(\phi_{r+s}(y)), \Im(\phi_{r+s}(y)))$ ,

where  $y \in \Lambda$ . We have  $\Gamma \subset \mathbb{R}^{n^2 d}$ .

Set  $m := n^2 d$

At the final step we have a reduced basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  of  $\Gamma$  with  $|\mathbf{b}_i| \geq \sqrt{n}$  for every  $i$ .

We generate all integer linear combinations

$$\mathbf{w} = \sum_{i=1}^m \alpha_i \mathbf{b}_i,$$

with

$$|\alpha_i| \leq c_m \left(\frac{2}{\pi}\right)^{\frac{2s}{d}} \Delta^{\frac{1}{d}} \sqrt{n(r+s)}$$

until a  $\mathbf{w}$  is found such that  $\text{rank } x = 1$  holds for the corresponding  $x \in \Lambda$ .

## Corollary

$\mathbb{K}$  is a number field,  $\mathcal{A}$  is given by structure constants, and  $\mathcal{A} \cong M_n(\mathbb{K})$  for an  $n > 1$ . Then there exists a zero divisor  $x \in \mathcal{A}$  which admits polynomially bounded coordinates with respect to the input basis of  $\mathcal{A}$ . Such an  $x$  can be computed in pspace.

**Proof.** Let  $\mathbf{c}_1, \dots, \mathbf{c}_{n^2}$  be the basis of  $\Lambda$  given by the IR algorithm. Express the element  $x$  of the Theorem in this basis:

$$x = \alpha_1 \mathbf{c}_1 + \alpha_2 \mathbf{c}_2 + \dots + \alpha_{n^2} \mathbf{c}_{n^2}$$

with  $\alpha_i \in \mathbb{Z}$ . Using that  $\|x\| \leq bn$ , and that the vectors  $\mathbf{c}_i$  have polynomial size, Cramer's rule implies a polynomial bound on the size of the  $\alpha_i$ .  $\square$

There is an important connection between split cyclic algebras and relative norm equations.

## Corollary

*Let  $\mathbb{K}$  be a number field,  $\mathbb{L}$  be cyclic extension of  $\mathbb{K}$ , and  $a \in \mathbb{K}$ . If the a norm equation*

$$N_{\mathbb{L}/\mathbb{K}}(x) = a$$

*is solvable, then there is a solution whose standard representation has polynomial size (in terms of the size of the standard representation of  $a$  and a basis of  $\mathbb{L}$ ). Furthermore, for fixed  $\mathbb{K}$  and fixed degree  $|\mathbb{L} : \mathbb{K}|$ , a solution can be found by a polynomial time ff-algorithm.*

## Corollary

$\mathbb{K}$  is a number field of degree  $d$  and discriminant  $\Delta$  over  $\mathbb{Q}$ . Let  $\mathcal{A}, \mathcal{B}$  be isomorphic central simple algebras over  $\mathbb{K}$  of dimension  $n^2$ , given by structure constants. Suppose that  $d, n$  and  $|\Delta|$  are bounded. Then an isomorphism  $\mathcal{A} \rightarrow \mathcal{B}$  can be constructed by a polynomial time algorithm. The running time is polynomial in  $|\Delta|$  and exponential in  $n$  and  $d$ .

**Proof.** We have  $\mathcal{A} \cong \mathcal{B}$  if and only if

$$\mathcal{A} \otimes_{\mathbb{K}} \mathcal{B}^{op} \cong M_{n^2}(\mathbb{K}).$$

Let  $V$  be a simple  $\mathcal{A} \otimes_{\mathbb{K}} \mathcal{B}^{op}$  module. Then  $\dim_{\mathbb{K}} V = n^2$ . So  $V$ , as left  $\mathcal{A}$ -module, is isomorphic to the regular left  $\mathcal{A}$  module.

Similarly,  $V$  is a regular right  $\mathcal{B}^{op}$ -module.

Let  $v \in V$  be a generating element of  $V$  as an  $\mathcal{A}$ -module, and also as a  $\mathcal{B}^{op}$  module.



Then  $\phi : a \mapsto av$  is a left  $\mathcal{A}$ -module isomorphism from  $\mathcal{A}$  to  $V$ .  
Also,  $\psi : b \mapsto vb$  is a right  $\mathcal{B}^{op}$ -module isomorphism from  $\mathcal{B}^{op}$  to  $V$ .

Then  $\sigma = \psi^{-1}\phi$  is a  $\mathbb{K}$  algebra isomorphism from  $\mathcal{A}$  and  $\mathcal{B}$ .

It is clear that  $\sigma$  is  $\mathbb{K}$  linear.

For  $a \in \mathcal{A}$ ,  $\sigma a$  is the unique element  $b \in \mathcal{B}$  with

$$av = vb.$$

Therefore  $\sigma(a_1 a_2)$  is the unique  $b \in \mathcal{B}$  with  $a_1 a_2 v = vb$ . But  $a_1 a_2 v = a_1 v(\sigma a_2) = v(\sigma a_1)(\sigma a_2)$ , whence  $\sigma(a_1 a_2) = (\sigma a_1)(\sigma a_2)$ .

□

# Tensor products of lattices

Let  $L \subset \mathbb{R}^m$  and  $M \subset \mathbb{R}^n$  be lattices. We have

$$L \otimes_{\mathbb{Z}} M \hookrightarrow \mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^n.$$

This allows one to define the lattice  $L \otimes M$ .

$L \otimes M$  can be viewed as the set of  $m$  by  $n$  matrices over  $\mathbb{R}$  which are integral linear combinations of dyads  $\mathbf{x}\mathbf{y}^T$ , where  $\mathbf{x} \in L$  and  $\mathbf{y} \in M$ .

$\mathbb{R}^m \otimes \mathbb{R}^n$  is an Euclidean space with

$$\langle \mathbf{x}_1 \otimes \mathbf{y}_1, \mathbf{x}_2 \otimes \mathbf{y}_2 \rangle = \langle \mathbf{x}_1, \mathbf{x}_2 \rangle \langle \mathbf{y}_1, \mathbf{y}_2 \rangle.$$

The norm on  $\mathbb{R}^m \otimes \mathbb{R}^n$  is the Frobenius norm on  $M_{m,n}(\mathbb{R})$ .

We have

$$\Lambda \cong PM_n(\mathbb{Z})P^{-1} \cong Q\mathbb{Z}^n \otimes (Q\mathbb{Z}^n)^*.$$

# Improvement when $\mathbb{K} = \mathbb{Q}$ and $n \leq 43$

Results of Y. Kitaoka (1977) on tensor products of lattices imply that the shortest nonzero element  $C$  in the ring  $PM_n(\mathbb{Z})P^{-1}$  must have rank one, when  $P$  is an invertible real matrix, and  $n \leq 43$ .

Above fails badly for  $n \geq 292$ .

Kitaoka's result leads to a simpler and faster method over  $\mathbb{Q}$ , when  $n \leq 43$ .

# An improved algorithm for $\mathbb{K} = \mathbb{Q}$ , $n \leq 43$

- 1 Use the IR algorithm to construct a maximal order  $\Lambda$  in  $\mathcal{A}$ .
- 2 Compute an  $\mathcal{A} \hookrightarrow M_n(\mathbb{R})$ . Use the derandomization from [de Graaf, Ivanyos '00] or [Eberly '91]. This gives a  $\|\cdot\|$  on  $\mathcal{A}$ .
- 3 Compute a sufficiently precise rational approximation  $A$  of our basis  $B$  of  $\Lambda$  by the method of [Schönhage '82].
- 4 Compute a reduced basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  of the lattice  $\Lambda \subset \mathbb{R}^m$  by the LLL algorithm on  $A$ . We have the bigger  $c_m$ .
- 5 Generate  $C = \sum_{i=1}^m \alpha_i \mathbf{b}_i$ , where  $\alpha_i \in \mathbb{Z}$ ,

$$|\alpha_i| \leq c_m \frac{\min\{\gamma'_n, |\mathbf{b}_1|\}}{|\mathbf{b}_i|} \leq c_m$$

until a rank 1  $C$  is found. Output this  $C$ .

# A Kitaoka type bound

Assume that  $2 \leq n \leq 8$ , and set  $\Lambda = PM_n(\mathbb{Z})P^{-1}$ , where  $P$  is an invertible real matrix. Let  $m$  be the minimal norm of the nonzero elements of  $\Lambda$ .

## Theorem

Let  $D \in \Lambda$  with rank at least 2. Then  $\|D\| \geq \sqrt{\frac{3}{2}}m$ .

Allows to reduce further the search space at step ⑤.

The proof is a refinement of Kitaoka's argument.

## Theorem

Let  $L$  and  $M$  be lattices. For every tensor  $\mathbf{v} \in L \otimes M$  of rank  $r$  we have

$$\|\mathbf{v}\| \geq \sqrt{\frac{r}{\gamma_r^2}} \lambda_1(L \otimes M).$$

## Lemma

Let  $A, B \in M_n(\mathbb{R})$  be positive definite real symmetric matrices. Then  $\text{Tr}(AB) \geq n \sqrt[n]{\det A} \sqrt[n]{\det B}$ .

**Proof of the Theorem.** Write  $\mathbf{v}$  as

$$\mathbf{v} = \sum_{i=1}^r \mathbf{x}_i \otimes \mathbf{y}_i.$$

Let  $L_1$  be the lattice generated by  $\{\mathbf{x}_1, \dots, \mathbf{x}_r\}$ , and  $M_1$  be the lattice spanned by  $\{\mathbf{y}_1, \dots, \mathbf{y}_r\}$ . The rank of these sublattices is  $r$ .

$$\|\mathbf{v}\|^2 = \left\| \sum_{i=1}^r \mathbf{x}_i \otimes \mathbf{y}_i \right\|^2 = \sum_{i,j=1}^r \langle \mathbf{x}_i, \mathbf{x}_j \rangle \langle \mathbf{y}_i, \mathbf{y}_j \rangle = \text{Tr}([\langle \mathbf{x}_i, \mathbf{x}_j \rangle]_{i,j=1}^r \cdot [\langle \mathbf{y}_i, \mathbf{y}_j \rangle]_{i,j=1}^r).$$

By the Lemma

$$\|\mathbf{v}\|^2 \geq r (\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle] \cdot \det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle])^{1/r}.$$

Now assume for contradiction that  $\|\mathbf{v}\|^2 < (r/\gamma_r^2)\lambda_1(L \otimes M)^2$ .  
It follows that

$$\|\mathbf{v}\|^2 < \frac{r}{\gamma_r^2} (\lambda_1(L)\lambda_1(M))^2 \leq \frac{r}{\gamma_r^2} (\lambda_1(L_1)\lambda_1(M_1))^2.$$

Combining the two inequalities

$$r < \frac{r}{\gamma_r^2} \cdot \frac{\lambda_1(L_1)^2}{(\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle])^{1/r}} \cdot \frac{\lambda_1(M_1)^2}{(\det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle])^{1/r}} \leq \frac{r}{\gamma_r^2} \gamma_r^2 = r,$$

as  $[\langle \mathbf{x}_i, \mathbf{x}_j \rangle]_{i,j=1}^r$  and  $[\langle \mathbf{y}_i, \mathbf{y}_j \rangle]_{i,j=1}^r$  are Gram matrices for  $L_1$  and  $M_1$ , respectively. Contradiction.

The minimum of  $r/\gamma_r^2$  for  $2 \leq r \leq 8$  is  $\frac{3}{2}$ , attained at  $r = 2$ .



# Improvement for $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ , $n = 2$ , $d = 1$ or $3$

Assume that  $\mathcal{A} \cong M_2(\mathbb{K})$ ,  $\Lambda$  is a maximal order in  $\mathcal{A}$ . Let  $\phi$  be an embedding of  $\mathcal{A}$  into  $M_2(\mathbb{C})$ .

Kitaoka-type results of R. Coulangeon over  $\mathbb{Q}(\sqrt{-d})$  give:

## Proposition

*For  $d = 1$ , at least one of the smallest nonzero elements of  $\phi(\Lambda)$  wrt the Frobenius norm has rank one.*

## Proposition

*For  $d = 3$ , the smallest nonzero elements of  $\phi(\Lambda)$  have rank one.*

Application: parametrization of Del Pezzo surfaces of degree 8 (W. A. de Graaf, J. Pílníková, J. Schicho, 2009).

# Problems for future work

- In the case  $\mathcal{A} \cong M_n(\mathbb{K})$  allow  $n$  or/and  $\mathbb{K}$  vary (even with  $d$  fixed)
- Study the case  $M_n(\mathbb{D})$ , where  $\mathbb{D}$  is a skewfield over  $\mathbb{K}$
- Develop a practical algorithm
- Extend the improvement to small number fields, say imaginary quadratic fields with small discriminant

Papers:

G. Ivanyos, L. R., J. Schicho:

Splitting full matrix algebras over algebraic number fields, *Journal of Algebra*, 354(2012), 211-223.

<http://arxiv.org/abs/1106.6191>

G. Ivanyos, Á. D. Lelkes, L. R.:

Improved algorithms for splitting full matrix algebras, *JP Journal of Algebra, Number Theory and Applications*, 28(2013), 141-156.

<http://arxiv.org/abs/1211.1356>

Thank you for your attention!