Recognition of division algebras.

Gabriele Nebe, Allan Steel

Lehrstuhl D für Mathematik, University of Sydney

DAG day, Eindhoven, 18.3.2010

Motivation.

Construction of irreducible matrix representations.

- G finite group, K a field, $n \in \mathbb{N}$, $\Delta : G \to \mathrm{GL}_n(K)$ group homomorphism
- KG-module structure on $V = K^{1\times n}$.
- The representation Δ is called irreducible, if V is a simple KG-module, i.e. V and $\{0\}$ are the only KG-submodules of V.
- There are only finitely many simple KG-modules up to isomorphism.
- Goal: Find all irreducible matrix representations of G.

Construct irreducible representations of G.

1) Construct representations:

- Permutation representations
- More general induced representations from subgroups
- Tensor products
- Symmetric square
- Alternating square
- More general symmetrizations

2) Find irreducible representations as subquotients.

Meataxe techniques.

Construct irreducible representations of G.

- If $\operatorname{char} K = p > 0$ then these are realized over a finite subfield. For finite fields meataxe techniques are available to find composition factors and to prove irreducibility.
- If $\operatorname{char} K = 0$, then these are realized over a number field K, a finite extension of $\mathbb{Q}$.
- Over $\mathbb{Q}$ meataxe techniques are used to obtain subrepresentations that are likely to be irreducible.
- Use the endomorphism ring

$$E = \{x \in K^{n\times n} \mid x\Delta(g) = \Delta(g)x \text{ for all } g \in G\}$$

- Schur's Lemma: Δ irreducible $\Longleftrightarrow$ E skewfield.
- Goal: Test if E is a skew field.
- E is a finite dimensional semisimple $\mathbb{Q}$-algebra.

Computing the endomorphism algebra.

$$E = \{x \in \mathbb{Q}^{n\times n} \mid x\Delta(g) = \Delta(g)x \text{ for all } g \in G\}$$

- Obtain E by solving system of linear equations
- or by finding random elements:
- $G = \langle g_1 = 1, g_2, \ldots, g_s \rangle$,
- $\pi : \mathbb{Q}^{n\times n} \to \mathbb{Q}^{n\times n}, \pi(x) = \frac{1}{s}\sum_{i=1}^{s} \Delta(g_i)^{-1}x\Delta(g_i)$ is linear
- 1 is unique eigenvalue ≥ 1
- eigenspace E
- iterating π approximates the projection $\pi_G : x \mapsto \frac{1}{|G|}\sum_{g\in G} \Delta(g)^{-1}x\Delta(g)$ onto $E \leq \mathbb{Q}^{n\times n}$
- $E = \langle \pi^\infty(b_1), \ldots, \pi^\infty(b_{n^2}) \rangle$
- $E = \langle \pi^\infty(x_1), \ldots, \pi^\infty(x_a) \rangle_{\mathbb{Q}\ algebra}$

Strategy to determine structure of E.

Wedderburn

$E \cong \bigoplus_{i=1}^{t} D_i^{n_i \times n_i}$ with division algebras D_i.

Algorithm (overview)

- $E = \langle b_1, \ldots, b_d \rangle_{\mathbb{Q}}$ given in right regular representation:
- $b_i \in \mathbb{Q}^{d \times d}, b_k b_i = \sum_{j=1}^{d} (b_i)_{j,k} b_j$
- find central idempotents, achieve $E = D^{n \times n}$
- calculate the Schur index of E as lcm of local Schur indices
- Use regular trace bilinear form:
  $\mathrm{Tr} : E \times E \to K, (a, b) \mapsto \mathrm{tr}_{reg}(ab)$.
- σ real place of K, then Schur index m_σ of $E \otimes_\sigma \mathbb{R}$ from signature of $\sigma \circ \mathrm{Tr}$.
- $\wp$ finite place of K, then Schur index $m_\wp$ of completion $E_\wp$ from discriminant of any maximal order.

Find idempotents in $Z(E)$.

$$Z = Z(E) := \{z \in E \mid zb_i = b_i z \text{ for all } 1 \leq i \leq d\}$$

- $Z \cong \bigoplus_{i=1}^{t} K_i$ étale
- regular representation: $Z = \langle z_1, \ldots, z_s \rangle \leq \mathbb{Q}^{s \times s}$
- Elementary fact: the z_i have a simultaneous diagonalization
- Choose random $z \in Z$, compute its minimal polynomial f
- If $f = gh$ is not irreducible, then $\mathbb{Q}^s = \ker(g(z)) \oplus \ker(h(z))$ is a Z-invariant decomposition of the natural module
- Compute the action of the generators on both invariant submodules and iterate this procedure
- Z is a field, if all z_i have irreducible minimal polynomial

Assume that $E = D^{n\times n}$ is simple.

- $E = D^{n\times n}$
- $K = Z(D) = Z(E)$ number field of degree $k = [K : \mathbb{Q}]$
- $m^2 = \dim_K(D)$ and so $d = \dim_{\mathbb{Q}}(E) = n^2m^2k$
- know d and k
- Goal: compute Schur index m of E
- Fact: Let $\mathbb{P}$ denote the set of all places of K. Then D is uniquely determined by all its completions $(D_\wp)_{\wp\in\mathbb{P}}$.
- The Schur index m of E is the least common multiple of the Schur indices $m_\wp$ of all completions $E_\wp := E \otimes_K K_\wp$.
- Goal: Determine all local Schur indices $m_\wp$ of E.
- For $\wp : K \to \mathbb{C}$ complex place $E \otimes_K \mathbb{C} = \mathbb{C}^{mn\times mn}$.
- If $\wp : K \to \mathbb{R}$ is a real place then

$$E_\wp = E \otimes_K \mathbb{R} = \begin{cases} \mathbb{R}^{nm\times nm} & \text{or} \\ \mathbb{H}^{nm/2\times nm/2} & \end{cases}$$

where $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.

The real completion.

Use the trace bilinear form. $\mathrm{Tr} : E \times E \to K, (a,b) \mapsto \mathrm{tr}_{reg}(ab)$.

Lemma

- Signature $(\mathbb{H}, \mathrm{Tr}) = (1, -3)$.
- Signature $(\mathbb{R}^{2\times 2}, \mathrm{Tr}) = (3, -1)$.
- Signature $(\mathbb{R}^{n\times n}, \mathrm{Tr}) = (n(n+1)/2, -n(n-1)/2)$.
- Signature $(\mathbb{H}^{n/2\times n/2}, \mathrm{Tr}) = (n(n-1)/2, -n(n+1)/2)$.

Proof:

- The Gram matrix of Tr for the basis $(1, i, j, k)$ of $\mathbb{H}$ is diag$(4, -4, -4, -4)$.
- The Gram matrix of Tr for the basis $\left(\begin{matrix}1&0\\0&0\end{matrix}, \begin{matrix}0&0\\0&1\end{matrix}, \begin{matrix}0&1\\0&0\end{matrix}, \begin{matrix}0&0\\1&0\end{matrix} \right)$ is diag $\left(2, 2, \begin{matrix}0&2\\2&0\end{matrix} \right)$.

Maximal order is a local property.

- $K = Z(E)$ number field, R ring of integers, $E = D^{n\times n}$.
- An R-order Λ in E is a subring of E which is a finitely generated R-module and spans E over K.
- Λ is called maximal, if it is not contained in a proper overorder.
- $\Lambda^* := \{d \in E \mid \mathrm{tr}(da) \in R \text{ for all } a \in \Lambda\}$
- Λ order $\Rightarrow \Lambda \subset \Lambda^*$.

Theorem.

The algebra E has a maximal order.
The order Λ is maximal if and only if all its finite completions are maximal orders.

Proof. $\Lambda \subset E$ any R-order, then $\Lambda \subset \Lambda^*$ and Λ^*/Λ is a finite group. So Λ has only finitely many overorders and one of them is maximal.

Local division algebras.

Let R be a complete discrete valuation ring with finite residue field $F = R/\pi R$ and quotient field K. Let D be a division algebra with center K and index m, so $m^2 = \dim_K(D)$.

Theorem.

The valuation of K extends uniquely to a valuation v of D and the corresponding valuation ring

$$M := \{d \in D \mid v(d) \geq 0\}$$

is the unique maximal R-order in D.
Let $\pi_D \in M$ be a prime element. Then $[(M/\pi_D M) : F] = m$.
Put

$$M^* := \{d \in D \mid \mathrm{tr}(da) \in R \text{ for all } a \in M\}$$

where tr denotes the regular trace $\mathrm{tr} : D \to K$. Then

$$M^* = \pi_D^{1-m} M \text{ and } |M^*/M| = |M/\pi_D M|^{m-1} = |F|^{m(m-1)}.$$

R complete dvr, $M \leq D$ valuation ring, $\dim_K(D) = m^2$.

Matrix rings.

All maximal R-orders Λ in $D^{n\times n}$ are conjugate to $M^{n\times n}$. With respect to the trace bilinear form, we obtain

$$\Lambda^* = \pi_D^{1-m}\Lambda \text{ and hence } |\Lambda^*/\Lambda| = |F|^{n^2(m^2-m)}.$$

- Know $(nm)^2 = \dim_K(D^{n\times n})$ so $s = nm$, and $|F|$.
- Calculate Λ and Λ^* and therewith $t = (nm)^2 - n^2m$.
- Then $m = (s^2 - t)/s = s - t/s$.

The discriminant of a maximal order.

- $E = D^{n\times n}$ central simple algebra over number field $K = Z(E)$ of dimension $s^2 = (nm)^2$
- $m_\wp$ the $\wp$-local Schur index of D, so $E_\wp \cong D_\wp^{n_\wp \times n_\wp}$ with $n_\wp m_\wp = s$
- Λ be a maximal R-order in E
- $t_\wp$ the number of composition factors $\cong R/\wp$ of the finite R-module Λ^*/Λ.

Theorem.

- $t_\wp > 0 \Leftrightarrow m_\wp \neq 1$
- $m_\wp = (s^2 - t_\wp)/s = s - t_\wp/s$
- The global Schur index is

$$m = \operatorname{lcm}\{m_\wp \mid \wp \in \mathcal{S}\} \cup \{m_\sigma \mid \sigma \text{ real place of } K\}$$

Rational calculation.

Theorem (see Yamada, The Schur subgroup of the Brauer group).

Let $E = D^{n\times n}$ be the endomorphism ring of a rational representation of a finite group. Then D has uniformly distributed invariants. This means that $Z(D)$ is Galois over $\mathbb{Q}$ and $m_\wp$ does not depend on the prime ideal $\wp$ of $Z(D) = K$, but only on the prime number $p \in \wp \cap \mathbb{Q} = p\mathbb{Z}$

$$m_p := m_\wp \text{ for any } \wp \trianglelefteq R, \wp \cap \mathbb{Q} = p\mathbb{Z}.$$

Discriminant maximal order Λ over $\mathbb{Z}$.

- $E = D^{n\times n}$, $K = Z(D) = Z(E)$, $s^2 = (mn)^2 = \dim_K(E)$.
- Assume that D has uniformly distributed invariants.
- $m_p := m_\wp$ for any $\wp \trianglelefteq R, \wp \cap \mathbb{Q} = p\mathbb{Z}$.
- $\wp \trianglelefteq R \Rightarrow N_p := N_{K/Q}(\wp)$, $a_p := |\{\wp \mid \wp \cap \mathbb{Q} = p\mathbb{Z}\}|$.
- Let Λ be a maximal order in E.
- $\Lambda^\# := \{x \in E \mid \mathrm{tr}_{reg}(x\lambda) \in \mathbb{Z}$ for all $\lambda \in \Lambda\} = R^\#\Lambda^*$.
- $\delta := \mathrm{disc}(K/\mathbb{Q}) = |R^\#/R|$.

Main result

$$|\Lambda^\#/\Lambda| = \delta^{s^2} \prod_p N_p^{a_p s(s-t_p)}$$

where $t_p = s/m_p$.

Computation of maximal order: direct approach.

- Let $\Lambda = \langle \lambda_1, \ldots, \lambda_{s^2k} \rangle \subset E$ be any order.
- Then there is a maximal order M in E such that

$$\Lambda \subset M \subset M^* \subset \Lambda^*.$$

- Λ^*/Λ is a finite R-module.
- Algorithm:
- Loop over the minimal submodules $\Lambda \subset S \subset \Lambda^*$.
- Compute the multiplicative closure $M(S) = \langle S, S^2, S^3, \ldots \rangle$
- If $M(S) \not\subset \Lambda^*$ then S is not contained in an order.
- Otherwise $M(S)$ is an overorder of Λ.
- Replace Λ by $M(S)$ and continue.
- If no $M(S)$ is an order, then Λ is already maximal.

Zassenhaus' computation of maximal order.

Let Λ be an order in E.

- The arithmetic radical $AR(\Lambda)$ of Λ is the intersection of all maximal right ideals of Λ that contain $|\Lambda^*/\Lambda|$.
- Then $AR(\Lambda)$ is an ideal, hence $\Lambda \subset O_r(AR(\Lambda)) := O(\Lambda) := \{x \in E \mid AR(\Lambda)x \subseteq AR(\Lambda)\}$.
- $\Lambda = O(\Lambda)$ if and only if Λ is hereditary.
- Any overorder of a hereditary order is hereditary.
- If Λ is hereditary, but not maximal, say $\Lambda_\wp$ is not maximal ($\wp$ prime ideal of R), then $O_r(I)$ is a proper overorder of Λ for any maximal twosided ideal I of Λ that contains $\wp$.
- all rational primes $p \mid |\Lambda^*/\Lambda|$ are handled separately
- Prime after prime we compute a p-maximal order.
- Involves only linear equations modulo p.

Example, $E = \mathrm{Mat}_3(\mathbb{Q}[\zeta_7 + \zeta_7^{-1}])$.

- Input E from file (algebra generators)
- Call SchurIndexJac(E)
- Dimension of E is 12
- Centre of dimension 3 and discriminant 7^2
- Determinant of order: $7^{10}43^6$, Discriminant $7^2 43^6$
- Order is already hereditary
- For prime 7: 2 maximal ideals
- Idealiser of first ideal is proper overorder
- and 7-maximal, so finished with prime 7
- For prime 43: 6 maximal ideals
- Idealiser of first ideal is proper overorder
- and has 5 maximal ideals
- Idealiser of second ideal is proper overorder
- and has 4 maximal ideals
- Idealiser of third ideal is proper overorder
- and 43-maximal, so finished with prime 43
- Discriminant of maximal order is 1

Situation for $43R = \wp_1\wp_2\wp_3$.

- $\Lambda = \begin{pmatrix} R & R \\ 43R & R \end{pmatrix}$,
- 6 maximal ideals:
- $I_i = \begin{pmatrix} \wp_i & R \\ 43R & R \end{pmatrix}$, $J_i = \begin{pmatrix} R & R \\ 43R & \wp_i \end{pmatrix}$ $i = 1, 2, 3$
- Idealiser of I_1 is $\Lambda_1 = \begin{pmatrix} R & \wp_1^{-1} \\ 43R & R \end{pmatrix} \sim \begin{pmatrix} R & R \\ \wp_2\wp_3 & R \end{pmatrix}$.
- Λ_1 has 5 maximal ideals: $\wp_1\Lambda_1$ and
- $I_i' = \begin{pmatrix} \wp_i & R \\ \wp_2\wp_3 & R \end{pmatrix}$, $J_i' = \begin{pmatrix} R & R \\ \wp_2\wp_3 & \wp_i \end{pmatrix}$ for $i = 2, 3$.
- Idealiser of I_2' is conjugate to $\Lambda_2 = \begin{pmatrix} R & R \\ \wp_3 & R \end{pmatrix}$
- has maximal ideals $\wp_1\Lambda_2$, $\wp_2\Lambda_2$ and I_3'', J_3''.
- The idealiser of I_3'' is maximal.

Cyclotomic orders.

- p prime, $\langle a\rangle = (\mathbb{Z}/p\mathbb{Z})^*$, $n \in \mathbb{Z}$
- $z_p \in \mathbb{Z}^{(p-1)\times(p-1)}$ companion matrix of the p-th cyclotomic polynomial
- $\Lambda := \langle \mathrm{diag}(z_p, z_p^a, \ldots, z_p^{a^{p-2}}), \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & 1 \\ n & 0 & \ldots & 0 & 0 \end{pmatrix} \rangle \leq$
  $\mathbb{Z}^{(p-1)^2\times(p-1)^2}$
- $E = \mathbb{Q}\Lambda$ central simple $\mathbb{Q}$-algebra of dimension $(p-1)^2$

$p = 7$:

n	2	-2	6	-6	7	10	-10
si	$2^3 7^3$	$2^3 7^6 \infty$	$2^3 3^6 7^2$	$2^3 3^6 \infty$	1	$2^3 5^6 7^6$	$2^3 5^6 7^3 \infty$