Modules over orders, conjugacy classes of integral matrices and abelian varieties over finite fields

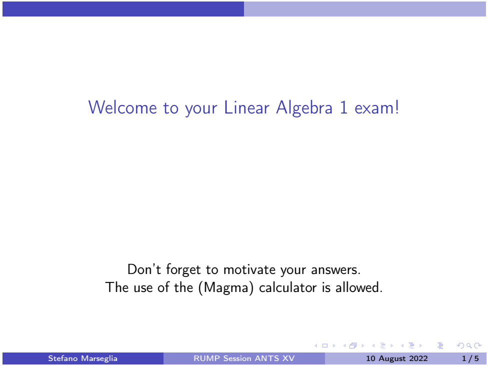
Stefano Marseglia

University of French Polynesia

July 18 2024 - ANTS XVI - MIT

Thank you

Back in Bristol. . . during the RUMP session



- Let R be an integral domain with unity.
- $A, B \in \mathrm{Mat}_{n\times n}(R)$ are R-**conjugate** ($A \sim_R B$) if $AP = PB$ for some $P \in \mathrm{GL}_n(R)$.
- The **minimal** polynomial $m(x)$ of $A \in \mathrm{Mat}_{n\times n}(R)$ is the monic polynomial of smallest degree such that $m(A) = O$ (the zero $n \times n$ matrix).
- The **characteristic** polynomial of $A \in \mathrm{Mat}_{n\times n}(R)$ is $\det(xI_n - A)$.

Question 1: Are the following two matrices $\mathbb{Q}$-conjugate? Are they $\mathbb{Z}$-conjugate?

$$A = \begin{pmatrix} 0 & -1 \\ 5 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$$

Answer(s):

Over $\mathbb{Q}$: yes! Same characteristic polynomial $x^2 + 5$, which is irreducible.

But...

Over $\mathbb{Z}$: no! Why?

Fix monic polynomials $m = m_1 \cdots m_n$ and $h = m_1^{s_1} \cdots m_n^{s_n}$ in $\mathbb{Z}[x]$ with

- each m_i irreducible and
- $m_i \neq m_j$ if $i \neq j$. (i.e. m is squarefree)

Question 2 Can we describe the representatives of the $\mathbb{Z}$-conjugacy classes of matrices with:

- minimal polynomial m, and
- characteristic polynomial h?

Answer:

Theorem ((generalized) Latimer-MacDuffee)

The order $\mathbb{Z}[\pi] = \frac{\mathbb{Z}[x]}{(m)}$ *acts on* $V = \left(\frac{\mathbb{Q}[x]}{m_1}\right)^{s_1} \times \ldots \times \left(\frac{\mathbb{Q}[x]}{m_n}\right)^{s_n}$.
We have a bijection

$$\left\{\mathbb{Z}[\pi]\text{-lattices in } V\right\}_{/\simeq_{\mathbb{Z}[\pi]}}$$
$$\updownarrow$$
$$\left\{\text{matrices with min. poly. } m \text{ and char. poly. } h\right\}_{/\sim_{\mathbb{Z}}}$$

Example

If $h = x^2 + 5$ then $K = V = \mathbb{Q}(\sqrt{-5})$.
The conjugacy classes of matrices with char. poly h are in bijection with $\text{Pic}(\mathscr{O}_K)$, which has 2 elements.

Proof (idea):

- Let M be a $\mathbb{Z}[\pi]$-lattice in V and fix a $\mathbb{Z}$-basis $\mathscr{B}$.
- Let A be the matrix representing the multiplication-by-π wrt $\mathscr{B}$.
- The induced map is well-defined and injective.
- For the 'surjectivity' part: take the $\mathbb{Z}$-span of 'algebraic eigenvectors'.

What about abelian varieties?

Question 3 Fix a Weil polynomial $h = m_1^{s_1} \cdots m_n^{s_n}$ which is ordinary over $\mathbb{F}_q$, or over $\mathbb{F}_p$ and without real roots. How do you compute abelian varieties over $\mathbb{F}_q$ with char. poly of Frobenius h? (up to $\mathbb{F}_q$-isomorphism)?

Answer: Do the same thing with $\mathbb{Z}[\pi, q/\pi]$ instead of $\mathbb{Z}[\pi]$:

Theorem (Deligne/Centelghe-Stix)

$$\left\{\textit{abelian varieties with char. poly. } h\right\}_{/\simeq_{\mathbb{F}_q}}$$

$$\updownarrow$$

$$\left\{\mathbb{Z}[\pi, q/\pi]\textit{-lattices in } V = \left(\frac{\mathbb{Q}[x]}{m_1}\right)^{s_1} \times \ldots \times \left(\frac{\mathbb{Q}[x]}{m_n}\right)^{s_n}\right\}_{/\simeq_{\mathbb{Z}[\pi, q/\pi]}}$$

How do we make these two theorems effective?

1. Find a 'finite box' that contains representatives of all isomorphism classes.
2. (Use other people's work to) pick out a minimal set of representatives.

Set-up:

- $K_1,\ldots,K_n$ number fields, with ring of integers $\mathcal{O}_i \subset K_i$.
- $K = K_1 \times \ldots \times K_n$.
- $\mathcal{O} = \mathcal{O}_1 \times \ldots \times \mathcal{O}_n$, the maximal order of K.
- $s_1,\ldots,s_n$ integers >0, $V = K_1^{s_1} \times \ldots \times K_n^{s_n}$, with the component-wise diagonal action of K.
- for an order R in K, set $\mathcal{L}(R,V) = \{R\text{-lattice in } V\}$.
- By the Jordan-Zassenhaus Theorem, $\mathcal{L}(R,V)/\simeq_R$ is finite.

Proposition (Steinitz)

Let M be in $\mathcal{L}(\mathcal{O},V)$. Then there are fractional $\mathcal{O}_i$-ideals I_i and an $\mathcal{O}$-linear isomorphism

$$M \simeq \bigoplus_{i=1}^{n} \left(\mathcal{O}_i^{\oplus(s_i-1)} \oplus I_i \right).$$

The isomorphism class of M is uniquely determined by the isomorphism class of the fractional $\mathcal{O}$-ideal $I = I_1 \oplus \cdots \oplus I_n$.

- Let $\mathfrak{f} = (R : \mathcal{O}) = \{x \in K : x\mathcal{O} \subseteq R\}$ be the conductor of R in $\mathcal{O}$.
- Write $\mathfrak{f} = \bigoplus_{i=1}^{n} \mathfrak{f}_i$, $\mathfrak{f}_i$ a fractional $\mathcal{O}_i$-ideal in K_i.

Theorem

Let M be in $\mathscr{L}(R, V)$. Then there exist M' in $\mathscr{L}(R, V)$, and fractional $\mathcal{O}_i$-ideals I_i such that

- $M' \simeq M$ as an R-module.
- $M'\mathcal{O} = \bigoplus_{i=1}^{n} \left(\mathcal{O}_i^{\oplus(s_i-1)} \oplus I_i\right)$.
- $\bigoplus_{i=1}^{n} \left(\mathfrak{f}_i^{\oplus(s_i-1)} \oplus \mathfrak{f}_i I_i\right) \subseteq M' \subseteq \bigoplus_{i=1}^{n} \left(\mathcal{O}_i^{\oplus(s_i-1)} \oplus I_i\right)$.

Proof:

By Steinintz: there are I_i's and an $\mathcal{O}$-isomorphism such that

$$\psi : M\mathcal{O} \to \bigoplus_{i=1}^{n} \left(\mathcal{O}_i^{\oplus(s_i-1)} \oplus I_i\right).$$

Set $M' = \psi(M)$. QED

- The previous theorem tells us that $M \in \mathscr{L}(R,V)$ admits an isomorphic copy M' among the lifts to V of the finitely many sub-R-modules of

$$\mathcal{Q}(I) = \frac{\mathscr{O}_1^{\oplus(s_1-1)} \oplus I_1 \oplus \cdots \oplus \mathscr{O}_n^{\oplus(s_n-1)} \oplus I_n}{\mathfrak{f}_1^{\oplus(s_1-1)} \oplus \mathfrak{f}_1 I_1 \oplus \cdots \oplus \mathfrak{f}_n^{\oplus(s_n-1)} \oplus \mathfrak{f}_n I_n}.$$

- For each fractional $\mathscr{O}$-ideal $I = \oplus_i I_i$, we have an $\mathscr{O}$-isomorphism $\Psi_I : \mathcal{Q}(I) \to \mathcal{Q}(\mathscr{O})$ inducing a bijection between the sub-R-modules.
- **Important**: there are algorithms `IsIsomorphic` that answer the following question: given $M, M' \in \mathscr{L}(R,V)$, is there an R-linear isomorphism $M \simeq M'$?
  See:
  - *Bley, Hofmann, Johnston. Computation of lattice isomor- phisms and the integral matrix similarity problem*, (2022), in Nemo/Hecke, or
  - *Eick, Hofmann, O'Brien. The conjugacy problem in* $\mathrm{GL}(n,\mathbb{Z})$, (2019), in Magma.

Algorithm

1. Enumerate all sub-R-modules of $\mathscr{Q}(\mathscr{O})$.
2. Compute the set $\mathscr{M}_{\mathscr{O}}$ of their lifts to V (via the natural quotient map).
3. Use `IsIsomorphic`, to sieve-out from $\mathscr{M}_{\mathscr{O}}$ a set $\mathscr{L}_{\mathscr{O}}$ of representative of the R-isomorphism classes.
4. For each class $[I] \in \mathrm{Pic}(\mathscr{O})$ compute $\Psi_I : \mathscr{Q}(I) \to \mathscr{Q}(\mathscr{O})$.
5. Define $\mathscr{L}_I$ as the 'pull-back' of $\mathscr{L}_{\mathscr{O}}$ vie Ψ_I.
6. Return $\sqcup_I \mathscr{L}_I$.

Example

Let
$$m_1 = x^2 - x + 3, \qquad m_2 = x^2 + x + 3,$$
$$m = m_1 m_2, \qquad h = m_1^2 m_2.$$

Set: $K_i = \mathbb{Q}[x]/m_i$, $K = K_1 \times K_2 = \mathbb{Q}[\pi]$, $V = K_1^2 \times K_2$, $E = \mathbb{Z}[\pi]$, $R = \mathbb{Z}[\pi, 3/\pi]$. Then:

- the $\mathbb{Z}$-conj. classes of 6×6-matrices with min. poly m and char. poly h are in bijection with $\mathscr{L}(E,V)/\simeq_E$: there is 4 of them.
- the $\mathbb{F}_3$-isomorphism classes of abelian varieties in the $\mathbb{F}_3$-isogeny class determined by the 3-Weil polynomial h are in bijection with $\mathscr{L}(R,V)/\simeq_R$: there is 2 of them.

Thank you!