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

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

Question 1:

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

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

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

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

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):

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

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.

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

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...

- Let R be a commutative ring 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 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 $\det(A - xI_n)$.

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! Every such a P must have determinant divisible by 3.

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)

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?

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

$$\left\{\mathbb{Z}[\pi]\text{-lattices in } V\right\}_{\big/ \simeq_{\mathbb{Z}[\pi]}}$$

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

$$\left\{\mathbb{Z}[\pi]\text{-lattices in } V\right\}_{/\simeq_{\mathbb{Z}[\pi]}}$$

$$\updownarrow$$

$$\left\{\text{matrices with min. poly. } m \text{ and char. poly. } h\right\}_{/\sim_{\mathbb{Z}}}$$

Proof (idea):
TODO

Question 3 How do you compute abelian varieties over $\mathbb{F}_q$ with ordinary characteristic polynomial of Frobenius $h = m_1^{s_1} \cdots m_n^{s_n}$ (up to $\mathbb{F}_q$-isomorphism)?

Question 3 How do you compute abelian varieties over $\mathbb{F}_q$ with ordinary characteristic polynomial of Frobenius $h = m_1^{s_1} \cdots m_n^{s_n}$ (up to $\mathbb{F}_q$-isomorphism)?

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

Question 3 How do you compute abelian varieties over $\mathbb{F}_q$ with ordinary characteristic polynomial of Frobenius $h = m_1^{s_1} \cdots m_n^{s_n}$ (up to $\mathbb{F}_q$-isomorphism)?
Answer: Do the same thing with $\mathbb{Z}[\pi, q/\pi]$ instead of $\mathbb{Z}[\pi]$:

Theorem (Deligne)

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

Question 3 How do you compute abelian varieties over $\mathbb{F}_q$ with ordinary characteristic polynomial of Frobenius $h = m_1^{s_1} \cdots m_n^{s_n}$ (up to $\mathbb{F}_q$-isomorphism)?
Answer: Do the same thing with $\mathbb{Z}[\pi, q/\pi]$ instead of $\mathbb{Z}[\pi]$:

Theorem (Deligne)

$$\left\{ \textit{abelian varieties with char. poly. } h \right\}_{\Big/ \simeq_{\mathbb{F}_q}}$$
$$\updownarrow$$
$$\left\{ \begin{array}{l} \mathbb{Z}\textit{-lattices in } V = \left(\frac{\mathbb{Q}[x]}{m_1}\right)^{s_1} \times \ldots \times \left(\frac{\mathbb{Q}[x]}{m_n}\right)^{s_n} \textit{ closed} \\ \textit{under multiplication by } \pi := x \bmod m \textit{ and } q/\pi \end{array} \right\}_{\Big/ \simeq_{\mathbb{Z}[\pi, q/\pi]}}$$

How do we make this two theorems effective?

Set-up:

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

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

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

The isomorphism class of M is uniquely determined by the isomorphism class of the fractional $\mathscr{O}$-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:
Compute 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 $M' = \psi^{-1}(M)$.
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, 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 is an algorithm `IsIsomorphic` that solves the following problem:

- 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

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

- For each fractional $\mathscr{O}$-ideal I, we have an $\mathscr{O}$-isomorphism $\Psi_I : \mathscr{Q}(I) \to \mathscr{Q}(\mathscr{O})$ inducing a bijection between the sub-R-modules.
- Important: there is an algorithm `IsIsomorphic` that solves the following problem: given $M, M' \in \mathscr{L}(R,V)$, is there an R-linear isomorphism $M \simeq M'$.
- See TODO ADD REF, which is implemented in Nemo/Hecke, or
- see TODO ADD REF, which is older and slower and implemented in Magma.

Algorithm

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

Example:

Let

$$m_1 = x^2 - x + 3, \quad m_2 = x^2 + x + 3,$$
$$m = m_1 m_2 = x^4 + 5x^2 + 9,$$
$$h = m_1^2 m_2 = x^6 - x^5 + 8x^4 - 5x^3 + 24x^2 - 9x - 27.$$

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 $\mathrm{GL}_6(\mathbb{Z})$-conj. classes of matrices with min. poly m and char. poly h are in bijection with $\mathscr{L}(E, V)$: 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 $\mathscr{L}(R, V)$: there is 2 of them.