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

- 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 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 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 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 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 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 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 even determinant.

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 2.1 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 2.1 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 2.1 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):

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)

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

How do we make this 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 $\mathscr{L}(R, V) = \{R\text{-lattice in } V\} / \simeq_R$.

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 $I = I_1 \oplus \dots \oplus I_n$.

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

Theorem: Let M be in $\mathscr{L}(R, V)$. Then there exist an 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:

IsIsomorphic

the algorithm

reduced the number of enumerations to 1