$\mathbb{Z}$-conjugacy classes of matrices and fractional ideals

and how to compute them

Stefano Marseglia

Utrecht University

ANTS Summer School - Europe - 27/06/2020

Introduction

Today's plan:

- Matrix conjugation
- Ideal Classes
- Latimer-MacDuffee Theorem
- Algorithms
- Generalizations

Motivation : the conjugacy problem

- Let $\mathscr{R}$ be a commutative ring (with 1).
- Let A and B be matrices in $\mathrm{Mat}_{n\times n}(\mathscr{R})$.
- We say that A and B are conjugate (over $\mathscr{R}$) if

$$\exists U \in \mathrm{GL}_n(\mathscr{R}) \text{ such that } A = UBU^{-1}.$$

- Question: by "looking" at A and B can we determine if they are conjugate?
- Question: are there invariants of A that determine its conjugacy class?

Invariants

Recall that:

- the characteristic polynomial of A is

$$\mathrm{char}_A(x) = \det(xI_n - A) \in \mathscr{R}[x].$$

- $\mathrm{char}_A(x)$ of A is an invariant of the conjugacy class of A...
  ...but in general not a complete invariant:
- The following matrices are not conjugate (over any ring $\mathscr{R}$)

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

  Same $\mathrm{char}_A(x) = \mathrm{char}_B(x) = (x-1)^2$ but different minimal polynomials: $m_A(x) = (x-1)^2$ while $m_B(x) = (x-1)$.

Over a field

- Over a field m_A and char_A tells us almost everything we need to know about the conjugacy class of A.
- More precisely:

Theorem (Rational Normal Form)

If $\mathscr{R}$ is a field, then there are polynomials

$$m_A(x) = g_1(x)|g_2(x)|\ldots|g_r(x) = \text{char}_A(x)$$

that completely determine the conjugacy class of A. Such polynomials can be computed using the Smith normal form of A.

- In particular: if $\text{char}_A(x)$ is irreducible the problem is solved (over a field)!

Our setting:

From now on we will consider the case $\mathscr{R} = \mathbb{Z}$.
Let $h(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial.

- Given $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ with $h(x) = \mathrm{char}_A(x) = \mathrm{char}_B(x)$
- Can we determine if A and B are conjugate?
- Can we list representatives of the conjugacy classes of matrices A with $\mathrm{char}_A(x) = h(x)$? Finite set?
- Answers: Yes and Yes!

...but first some Notation and Background material.

Orders

- $h(x) \in \mathbb{Z}[x]$ monic and irreducible
- $K = \mathbb{Q}[x]/(h)$ number field
- $\alpha = x \bmod h$ primitive element of K
- an order R in K is a subring such that $R \simeq_{\mathbb{Z}} \mathbb{Z}^{\deg(h)}$
- Eg. $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(h)$
- Eg. $\mathcal{O}_K$ the maximal order (a.k.a. ring of integers of K)
- an over-order of R is a ring S such that $R \subseteq S \subseteq \mathcal{O}_K$.

Fractional ideals

- a fractional R-ideal I is a sub-R-module of K such that $I \simeq_{\mathbb{Z}} \mathbb{Z}^{\deg(h)}$
- Eg. any non-zero ideal of R
- Eg. $\frac{1}{4}R$
- Eg. any over-order of R is a frac.R-ideals
- if I, J are frac.R-ideals then IJ, $I + J$, $I \cap J$ and

$$(I : J) = \{x \in K : xJ \subseteq I\}$$

  are also frac.R-ideals

ICM and Latimer-MacDufee theorem (1933)

- isomorphism: we say $I \simeq_R J$ if there exists $z \in K$ s.t. $zI = J$
- we denote by $[I]$ the isomorphism class of I
- define

$$\mathrm{ICM}(R) = \frac{\{\text{frac.}\, R\text{-ideals}\}}{\simeq_R} \qquad \text{ideal class monoid}$$

- Note: the monoid structure is induced by ideal multiplication.

Theorem (Latimer-MacDufee theorem (1933))

Let $h(x) \in \mathbb{Z}[x]$ monic and irreducible. There exists a bijection

$$\mathrm{ICM}(\mathbb{Z}[\alpha]) \longleftrightarrow \frac{\{A \in \mathrm{Mat}(\mathbb{Z}) : \mathrm{char}_A(x) = h(x)\}}{\sim_{\mathbb{Z}}}$$

Sketch of the proof :

- $I = x_1\mathbb{Z} \oplus \ldots \oplus x_N\mathbb{Z} \mapsto m_{\alpha,I,X}$ matrix representing multiplication-by-α w.r.t. the $\mathbb{Z}$-basis $X = \{x_1, \ldots, x_N\}$
- Note: $\mathrm{char}_{m_{\alpha,I,X}}(x) = h(x)$
- changing the $\mathbb{Z}$-basis X, replaces $m_{\alpha,I,X}$ with a $\mathbb{Z}$-conjugate matrix
- replacing I by zI $(z \in K^\times)$ and X by zX doesn't change the matrix:

$$m_{\alpha,I,X} = m_{\alpha,zI,zX}$$

- In the other direction: consider A with $\mathrm{char}_A(x) = h(x)$. Put $N = \deg(h)$.
- induce a $\mathbb{Z}[\alpha]$-module structure on $\mathbb{Z}^N$ by $\alpha.v := A.v$
- given any $\varphi_0 : K \simeq_{\mathbb{Q}} \mathbb{Q}^N$, put $I = \varphi_0^{-1}(\mathbb{Z}^N)$ and note that $A = m_{\alpha,I,X}$ where X is the pre-image via φ_0 of the standard basis of $\mathbb{Z}^N$.
- These two construction induce the bijection in the statement.

Example

- Take $h = x^3 + 10x^2 - 8$
- Put $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(h)$
- Consider the order

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z}$$

- $\mathbb{Z}[\alpha]$ has 2 proper over-orders: $\mathbb{Z}[\alpha] \subsetneq S \subsetneq \mathcal{O}$

$$S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}, \qquad \mathcal{O} = \mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2}{4}\mathbb{Z}$$

- Using the algorithm that I will present, we get:

$$\mathrm{ICM}(\mathbb{Z}[\alpha]) = \{[\mathbb{Z}[\alpha]], [S], [\mathcal{O}], [S^t]\},$$

where

$$S^t = \mathbb{Z} \oplus \left(\frac{2+\alpha}{4}\right)\mathbb{Z} \oplus \left(\frac{188 - 312\alpha + \alpha^2}{3784}\right)\mathbb{Z}$$

Example (cont)

Matrices:

$$[\mathbb{Z}[\alpha]] \longleftrightarrow \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & 0 \\ 0 & 1 & -10 \end{pmatrix}$$

$$[S^t] \longleftrightarrow \begin{pmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 1 & -10 \end{pmatrix}$$

$$[S] \longleftrightarrow \begin{pmatrix} 0 & 0 & 4 \\ 1 & 0 & 0 \\ 0 & 2 & -10 \end{pmatrix}$$

$$[\mathscr{O}] \longleftrightarrow \begin{pmatrix} 0 & 0 & 2 \\ 2 & 0 & 0 \\ 0 & 2 & -10 \end{pmatrix}$$

Questions one the first part?

In the rest of the talk, I will describe:

how to compute ICM(R) (for any order R in K)

how to test $I \simeq_R J$

invertible ideals: Pic

- As before: let R be an order in a number field K.
- A frac. R-ideal I is called invertible if

$$I(R:I) = R$$

- Define

$$\mathrm{Pic}(R) := \frac{\{\text{invertible frac.} R\text{-ideals}\}}{\simeq_R}$$

- It can be computed efficiently if we know the class group $\mathrm{Pic}(\mathcal{O}_K) = \mathrm{Cl}(K)$ and the unit group $\mathcal{O}_K^\times$ using:

$$1 \to R^\times \to \mathcal{O}_K^\times \to \frac{(\mathcal{O}/\mathfrak{f})^\times}{(R/\mathfrak{f})^\times} \to \mathrm{Pic}(R) \to \mathrm{Pic}(\mathcal{O}_K) \to 1$$

where $\mathfrak{f} = (R : \mathcal{O}_K)$ is the conductor of R. see Klüners/Pauli '05.

ICM and Pic

Lemma

$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R)$ *with equality iff* $R = \mathscr{O}_K$

Proof: Inclusion is clear. Every frac.$\mathscr{O}_K$-ideal is invertible (in $\mathscr{O}_K$).

- For a frac.R-ideal I the multiplicator ring of I is the over-order of R given by $(I:I)$ (the biggest over-order of R for which I is a module).

Lemma

$$\mathrm{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathscr{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S)$$

Proof: Let I be a frac.R-ideal.
Let S be an order $R \subseteq S \subseteq (I:I)$. Then I is a frac.S-ideal.
If I is invertible in S then $S = I(S:I) = I(I:I)(S:I) = S(I:I) = (I:I)$.

ICM in general

- "Usually" we have an equality : $\mathrm{ICM}(R) = \bigsqcup \mathrm{Pic}(S)$ (iff R is Bass)
- In this case: compute the over-orders of R and their Pic's.
  (for the over-orders see Hofmann-Sircana 2019)
- BUT sometimes there are MORE isomorphism classes
- previous example: $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 + 10x^2 - 8)$

$$\mathrm{ICM}(\mathbb{Z}[\alpha]) = \left\{ \underbrace{[\mathbb{Z}[\alpha]]}_{\mathrm{Pic}(\mathbb{Z}[\alpha])}, \underbrace{[S]}_{\mathrm{Pic}(S)}, \underbrace{[\mathcal{O}]}_{\mathrm{Pic}(\mathcal{O})}, [S^t] \right\}$$

where $S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}$ and $S^t = \mathbb{Z} \oplus \left(\frac{2+\alpha}{4}\right)\mathbb{Z} \oplus \left(\frac{188-312\alpha+\alpha^2}{3784}\right)\mathbb{Z}$.

- S^t is a non-invertible ideal with $(S^t : S^t) = S$
  (S is not Gorenstein)

How to handle the "unsual cases"?

- We want an algorithm that always works!
- Solution: first problem locally: (Dade, Taussky, Zassenhaus '62)
  Say that I and J are weakly equivalent if:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R) \quad \text{local nature!}$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

$$\Updownarrow$$

$$(I : I) = (J : J) = S \text{ and } \exists\ L \text{ invert. in } S \text{ s.t. } I = LJ$$

- Let $\mathscr{W}(R)$ be the monoid of weak eq. classes

Recover $\mathrm{ICM}(R)$ from $\mathscr{W}(R)$

Partition w.r.t. the multiplicator rings:

$$\mathscr{W}(R) = \bigsqcup_{R\subseteq S\subseteq \mathcal{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R\subseteq S\subseteq \mathcal{O}_K} \mathrm{ICM}_S(R)$$

$\mathscr{W}_S(R)$ and $\mathrm{ICM}_S(R)$ mean "only classes with multiplicator ring $= S$"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\mathrm{ICM}_S(R)$ and the quotient is

$$\mathscr{W}_S(R) = {}^{\mathrm{ICM}_S(R)}\!\big/_{\mathrm{Pic}(S)}$$

Repeat for every $R\subseteq S\subseteq \mathcal{O}_K$: $\rightsquigarrow \mathrm{ICM}(R)$.

How to compute $\mathscr{W}_S(R)$

- Define the trace-dual of S as $S^t = \{x \in K : \mathrm{Tr}(xS) \subseteq \mathbb{Z}\}$
- Let T be the (smallest) over-order of S s.t. $S^t T$ is invertible in T.
- Let I with $(I:I) = S$. Since $I \cdot I^t = S^t$, it follows that IT si invertible in T and hence (up to weak equivalence) we can assume that $IT = T$.
- We get that

$$\mathfrak{f} \subset I \subset T,$$

where $\mathfrak{f} = (S:T)$ is the "relative" conductor of S in T.

Proposition

We can find all representatives of $\mathscr{W}_S(R)$ in:

$$\{\textit{frac.S-ideals} : \mathfrak{f} \subset I \subset T\} \longleftrightarrow \left\{\textit{sub-S-modules of } {}^{T}\!/_{\mathfrak{f}}\right\}$$

finite!!! (and often not too big)

Recap

- A quick recap:

$$\mathscr{W}_S(R) \xrightarrow{\text{act with } \mathrm{Pic}(S)} \mathrm{ICM}_S(R) \xrightarrow{\text{repeat for every } S} \mathrm{ICM}(R) \qquad \text{Hurra!}$$

- Observe: $\mathscr{W}_S(R)$ and $\mathrm{Pic}(S)$ are finite for every S. So $\mathrm{ICM}(R)$ is finite
- So we can compute ICM's and hence representatives of the conjugacy classes of $\mathbb{Z}$-matrices with irreducible char. polynomial.

Isomorphism testing

- We also have all the ingredients to solve the isomorphism problem for ideals and hence the conjugacy test for matrices.

Proposition

Let I and J frac.ideals. Put $S = (I : I)$. Then

$$I \simeq J \iff \begin{cases} I \text{ weakly eq. } J \\ (I : J) \text{ is a principal } S\text{-ideal} \end{cases}$$

Proof: we know that if I is weakly eq. to J then there exists an invertible S-ideal L such that $I = LJ$. One can prove that $L = (I : J)$. Hence $I = zJ$ iff $(I : J) = zS$ for some z.

Example 1

Weak equivalence classes of $\mathbb{Z}[\alpha]$ in $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(h)$ where $h = x^3 + 31x^2 + 43x + 77$.

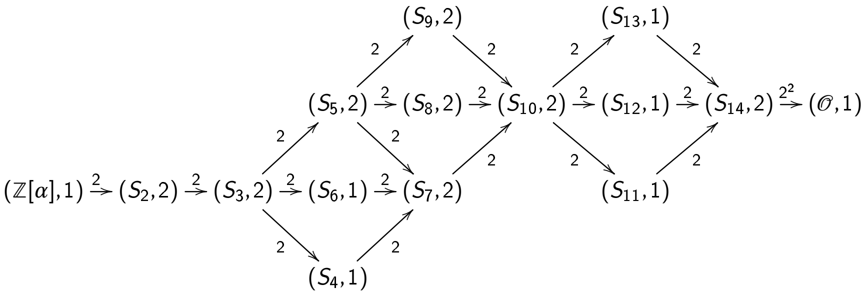
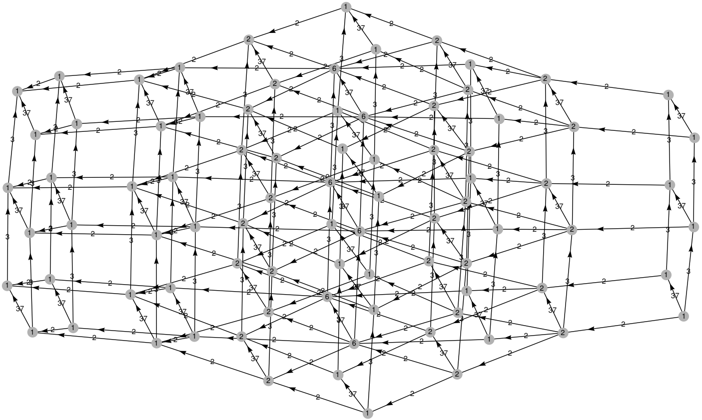


Figure: Each vertex is labeled as $(S_i, \#\mathscr{W}_{S_i}(\mathbb{Z}[\alpha]))$. The edges are marked by the index of the corresponding inclusion.

Example 2

Everything I told you generalizes *verbatim to the case when h is square-free*



Weak equivalence classes of the monogenic order of $\mathbb{Q}[x]/(h)$ *where*

$$h = (x^2 + 4x + 7)(x^3 - 9x^2 - 3x - 1).$$

Example 3

Consider in $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 + 10x^2 - 8)$ the frac.$\mathbb{Z}[\alpha]$-ideals:

$$I = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus (\alpha^2+2)\mathbb{Z} \qquad J = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus \left(\frac{\alpha^2+2\alpha}{8}\right)\mathbb{Z}$$

We have $I \simeq J \simeq \mathbb{Z}[\alpha]$. More precisely: $(\alpha^2+\alpha)J = I$.
Matrices:

$$m_I := \begin{pmatrix} 1 & 0 & -1 \\ 3 & -1 & -1 \\ 0 & 1 & -10 \end{pmatrix}, \quad m_J := \begin{pmatrix} 1 & -1 & 1 \\ 3 & -3 & 2 \\ 0 & 8 & -8 \end{pmatrix}, \quad V := \begin{pmatrix} 2 & -1 & 1 \\ 3 & -1 & 1 \\ 3 & -10 & 9 \end{pmatrix}.$$

Notice: V is represents $\mathbb{Z}$-basis of J times $(\alpha^2+\alpha)$ w.r.t the $\mathbb{Z}$-basis of I.
We have

$$V \cdot m_J \cdot V^{-1} = m_J$$

Generalization and related work

- the bijection between conj. classes of matrices and isomorphism classes of modules in product of number fields holds in much greater generality: see D. Husert PhD thesis 2016.
- there is a working algorithm to test conjugacy of matrices (no assumptions!) see Hofmann, Eick, O'Brien, 2019.
  (but no representatives for the conj. classes)
- the algorithms presented (both conj. test and representatives) generalize to the case when $\mathrm{char}_A(x) = m(x)^N$ with $m(x)$ square-free and the order $\mathbb{Z}[x]/(m)$ is Bass. see Marseglia 2020.
- Also ICM's are "everywhere" :-p
  there is an equivalence of categories

$$\left\{ \begin{array}{l} \text{ordinary abelian varieties over } \mathbb{F}_q \\ \text{with squarefree } q\text{-Weil poly. } h(x) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{frac. ideals of } \mathbb{Z}[F, q/F] \\ \text{in } \mathbb{Q}[F] = \mathbb{Q}[x]/(h(x)) \end{array} \right\}$$

Thanks for your attention