INTEGER MATRICES AND NUMBER FIELD IDEALS

JOE PACOLD

1. Conjugacy classes in $\mathrm{M}_n(\mathbb{Z})$

For both intrinsic interest and many applications, it is useful to have a criterion for when two matrices are conjugate. There is a single condition for matrices over a field K: $A, B \in \mathrm{M}_n(K)$ are conjugate by some $U \in \mathrm{GL}_n(K)$ if and only if they have the same rational canonical form [1]. The simplest case of this is:

Theorem 1.1. *Let $A, B \in \mathrm{M}_n(K)$ have irreducible characteristic polynomials $f_A, f_B \in K[x]$. Then A and B are conjugate if and only if $f_A(x) = f_B(x)$.*

Proof. Suppose $A = UBU^{-1}$ for some $U \in \mathrm{GL}_n(K)$. Then

$$f_A(x) = \det(xI_n - A) = \det(U(xI_n - B)U^{-1}) = \det(xI_n - B) = f_B(x).$$

On the other hand, suppose $f_A(x) = f_B(x) = f(x)$. Fix a nonzero $\vec{v} \in K^n$, and consider the set of vectors $S_A = \{\vec{v}, A\vec{v}, A^2\vec{v}, \ldots, A^{n-1}\vec{v}\}$. These must be linearly independent. If not, there is a nonzero polynomial $g \in K[x]$ with $\deg(g) < n$ and $g(A)\vec{v} = 0$. This implies that some eigenvalue of A, say $\lambda \in \overline{K}$, is a root of $g(x)$. This is a contradiction, since λ is also a root of $f(x)$ (which is irreducible over K and has degree n). Therefore S_A is a basis for K^n, and with respect to this basis, A is the companion matrix of $f(x)$

Similarly, $S_B = \{\vec{v}, B\vec{v}, B^2\vec{v}, \ldots, B^{n-1}\vec{v}\}$ is a basis for K^n, and the action of B on this basis is the also the companion matrix of $f(x)$. Let U be the matrix that changes basis from S_A to S_B; then $A = UBU^{-1}$. □

Here the fact that K is a field is important. If we try to apply this theorem to $\mathrm{M}_n(\mathbb{Z})$, in general U or U^{-1} will not have integer entries. For example,

$$A = \begin{pmatrix} 0 & -13 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} -1 & -7 \\ 2 & 1 \end{pmatrix}$$

both have characteristic polynomial $x^2 + 13$. This is irreducible over $\mathbb{Q}$, so A and B are conjugate over $\mathbb{Q}$, and both have rational canonical form

$$\begin{pmatrix} 0 & -13 \\ 1 & 0 \end{pmatrix} = A = UBU^{-1} \text{ where } U = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \notin \mathrm{GL}_2(\mathbb{Z}).$$

If we try to find a $U \in \mathrm{GL}_2(\mathbb{Z})$ such that $UBU^{-1} = A$, we get

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -13 \\ 1 & 0 \end{pmatrix} (\pm 1) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} -1 & -7 \\ 2 & 1 \end{pmatrix}$$

Looking at the lower left entry, we get $d^2 + 13c^2 = \pm 2$, which has no integer solutions. We therefore have at least two conjugacy classes of matrices with this characteristic polynomial, and the natural question is whether there are more. It turns out that these are the only two, and in general we can count the conjugacy classes by working in the number field $\mathbb{Q}(\lambda)$, where λ is a root of $f(x)$ [2].

Theorem 1.2. *(Latimer-MacDuffee) Let $f \in \mathbb{Z}[x]$ be monic and irreducible, with degree n, and let $f(\lambda) = 0$. Then there is a bijection between the conjugacy classes of matrices $A \in \mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial f and the ideal classes in the order $\mathbb{Z}[\lambda]$ of $\mathbb{Q}[\lambda]$.*

Proof. Following [3], we construct the bijection as follows. Given a matrix A, let $\vec{\omega}$ be an eigenvector with eigenvalue λ. We can freely scale $\vec{\omega}$, so let some nonzero ω_i be 1. Then $A\vec{\omega} = \lambda\vec{\omega}$ is a system of linear equations in the remaining ω_i, with coefficients in $\mathbb{Z}[\lambda]$. Therefore $\omega_i \in \mathbb{Q}(\lambda)$ for all i. Let I be the $\mathbb{Z}$-module spanned by the ω_i. Now since $A \in \mathrm{M}_n(\mathbb{Z})$,

$$\lambda\omega_i = \sum_{j=1}^{n} A_{ij}\omega_j \in I,$$

so I is a fractional ideal of $\mathbb{Z}[\lambda]$. Choosing to rescale $\vec{\omega}$ gives a fractional ideal in the same class as I. Furthermore, if $U \in \mathrm{GL}_n(\mathbb{Z})$, then

$$(UAU^{-1})(U\vec{\omega}) = \lambda(U\vec{\omega}),$$

and the entries of $U\vec{\omega}$ are simply another basis for I. Hence this procedure gives a well-defined map from matrix conjugacy classes to ideal classes.

To show that the map is surjective, let I be a fractional ideal of $\mathbb{Z}[\lambda]$. Since λ has degree n over $\mathbb{Z}$, I must have dimension n as a $\mathbb{Z}$-module. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for I, and let A be the matrix that represents multiplication by λ in this basis. Then A has integer entries, and $A\vec{\omega} = \lambda\vec{\omega}$, so the characteristic polynomial of A is $f(x)$.

To show that it is injective, suppose that $A, B \in \mathrm{M}_n(\mathbb{Z})$, $A\vec{\omega} = \lambda\vec{\omega}$, $B\vec{\psi} = \lambda\vec{\psi}$, and that $I = \langle\omega_1, \ldots, \omega_n\rangle_{\mathbb{Z}}$ is in the same ideal class as $J = \langle\psi_1, \ldots, \psi_n\rangle_{\mathbb{Z}}$, i.e. $\alpha I = \beta J$ for some nonzero $\alpha, \beta \in \mathbb{Z}[\lambda]$. Then let $U \in \mathrm{GL}_n(\mathbb{Z})$ be the matrix that changes basis from βJ to αI, so that $\alpha\vec{\omega} = U(\beta\vec{\psi})$. Now,

$$A(U\beta\vec{\psi}) = A(\alpha\vec{\omega}) = \lambda(\alpha\vec{\omega}) = \lambda(U\beta\vec{\psi}) = \beta U(B\vec{\psi})$$

$$\beta(AU)\vec{\psi} = \beta(UB)\vec{\psi} \;\Rightarrow\; (AU - UB)\vec{\psi} = \vec{0}$$

Noting that the entries of $\vec{\psi}$ are linearly independent over $\mathbb{Z}$, we conclude that
$AU - UB = 0$, so $A = UBU^{-1}$. □

Returning to the example above, let $f(x) = x^2 + 13$ and $\lambda = \sqrt{-13}$. Then $\mathbb{Z}[\lambda]$ is the ring of integers of the number field $\mathbb{Q}(\lambda)$. We can compute the class group, which has order 2; the ideal classes are represented by (1) and $(2, 1 + \lambda)$. Therefore there are two conjugacy classes in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial $x^2 + 13$, and we can write down representatives for them by multiplying λ by a basis for each ideal:

$$\begin{array}{rcl} \{1, \lambda\} \xrightarrow{\lambda} & \{\lambda, -13\} & \longrightarrow \begin{pmatrix} 0 & -13 \\ 1 & 0 \end{pmatrix} \\ \{2, 1 + \lambda\} \xrightarrow{\lambda} & \{-1(2) + 2(1 + \lambda), -7(2) + 1(1 + \lambda)\} & \longrightarrow \begin{pmatrix} -1 & -7 \\ 2 & 1 \end{pmatrix} \end{array}$$

This approach makes it easy to compute which conjugacy class a given matrix satisfying x^2+13 falls into. For example,

$$\begin{pmatrix} 3 & 11 \\ -2 & -3 \end{pmatrix} \text{ has eigenvector } \begin{pmatrix} -3-\lambda \\ 2 \end{pmatrix} \longrightarrow (2,-3-\lambda)=(2,1+\lambda)$$

And, in fact,

$$\begin{pmatrix} 3 & 11 \\ -2 & -3 \end{pmatrix} = U \begin{pmatrix} -1 & -7 \\ 2 & 1 \end{pmatrix} U^{-1} \text{ for } U = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

2. Implementation for $\lambda = \sqrt{d}$

The accompanying Sage code demonstrates this for integer matrices with characteristic polynomial x^2-d, with d nonsquare. Such matrices are traceless, with determinant $-d$, so they have the form

$$\begin{pmatrix} a & b \\ -(a^2+d)/b & -a \end{pmatrix}$$

The eigenvectors have nonzero entries, since

$$\begin{pmatrix} a & b \\ -(a^2+d)/b & -a \end{pmatrix} \begin{pmatrix} x \\ 0 \end{pmatrix} = \sqrt{d} \begin{pmatrix} x \\ 0 \end{pmatrix} \;\Rightarrow\; ax = \sqrt{d}x, a \in \mathbb{Z} \Rightarrow\Leftarrow$$

(and similarly $y \neq 0$). We can therefore scale arbitrarily to fix one entry. A convenient choice is

$$\begin{pmatrix} a & b \\ -(a^2+d)/b & -a \end{pmatrix} \begin{pmatrix} b \\ \sqrt{d}-a \end{pmatrix} = \begin{pmatrix} b\sqrt{d} \\ d-a\sqrt{d} \end{pmatrix},$$

so the matrix corresponds to the ideal $(b, \sqrt{d}-a) \subset \mathbb{Z}[\sqrt{d}]$.

In most cases this ideal has to be computed carefully, since in general $\mathbb{Z}[\lambda]$ is not the full ring of integers of $\mathbb{Q}(\lambda)$. In the case of quadratic fields, we know that the ring of integers is $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 2,3 \pmod 4$, and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ for $d \equiv 1 \pmod 4$. Note, however, that I is an ideal of $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if and only if $2I$ is an ideal of $\mathbb{Z}[\sqrt{d}]$, and that I and $2I$ are in the same ideal class. Therefore we can work in the full ring of integers in all cases, using existing tools to calculate with its ideals. We compute the fractional ideals corresponding to the two matrices, and check whether one divided by the other gives a principal ideal, i.e. whether they are in the same class. If they are, then we compute (largely by brute force) the matrix that changes basis between the original two.

3. References

[1] D.S. Dummit and R.M. Foote, “Abstract Algebra,” Wiley, 2004

[2] C. Latimer and C.C. Macduffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. **34**)1933), 33-316

[3] M. Newman, “Integral matrices,” Academic Press, 1972