IDEAL CLASSES AND MATRIX CONJUGATION OVER $\mathbf{Z}$

KEITH CONRAD

When R is a commutative ring, matrices A and B in $\mathrm{M}_n(R)$ are called conjugate when $UAU^{-1} = B$ for some $U \in \mathrm{GL}_n(R)$. The conjugacy problem in $\mathrm{M}_n(R)$ is: decide when two matrices in $\mathrm{M}_n(R)$ are conjugate. We want to look at the conjugacy problem in $\mathrm{M}_n(\mathbf{Z})$, where ideal theory and class groups make an interesting appearance.

The most basic invariant for conjugacy classes of matrices is the characteristic polynomial: conjugate matrices have the same characteristic polynomial. This is not a complete invariant in general: the matrices $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, both have characteristic polynomial $(T-1)^2$, but $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ are not conjugate (in any $\mathrm{M}_2(R)$) since the identity matrix is conjugate only to itself. While there are refinements of the characteristic polynomial which settle the conjugacy problem in $\mathrm{M}_n(F)$ for F a field (use the rational canonical form), we don't pursue that direction. Instead our starting point is a special case where the characteristic polynomial is a complete invariant.

Theorem 1. *Let F be a field and $f(T) \in F[T]$ be monic irreducible of degree n.*

(a) *A matrix A in $\mathrm{M}_n(F)$ has characteristic polynomial $f(T)$ if and only if $f(A) = O$.*
(b) *All matrices in $\mathrm{M}_n(F)$ with characteristic polynomial $f(T)$ are conjugate in $\mathrm{M}_n(F)$.*

The key point here is irreducibility of the characteristic polynomial. If that assumption is dropped, the theorem breaks down completely (the matrices in $\mathrm{M}_n(F)$ sharing a common reducible characteristic polynomial are not all conjugate to each other in $\mathrm{M}_n(F)$).

Proof. (a) If A has characteristic polynomial $f(T)$ then $f(A) = O$ by the Cayley-Hamilton theorem. Conversely, suppose $f(A) = O$. Let $\chi(T)$ be the characteristic polynomial of A. We want to show $\chi(T) = f(T)$. Since $f(T)$ is irreducible in $F[T]$, $f(T)$ is the minimal polynomial of A in $F[T]$, so $f(T)|\chi(T)$ in $F[T]$ because $\chi(A) = O$. Since $f(T)$ and $\chi(T)$ are monic of the same degree, the divisibility relation forces equality.

(b) Suppose $A \in \mathrm{M}_n(F)$ has characteristic polynomial $f(T)$. We make F^n into an $F[T]$-module by letting multiplication by T on F^n be the action of A: $g(T)v = g(A)v$ for $v \in F^n$. We are going to show F^n as an $F[T]$-module in this way is isomorphic to $F[T]/(f(T))$ as an $F[T]$-module. Therefore any two matrices in $\mathrm{M}_n(F)$ with characteristic polynomial $f(T)$ give F^n isomorphic $F[T]$-module structures (it always looks like $F[T]/(f(T))$ as an $F[T]$-module), so the two matrices are conjugate because matrices in $\mathrm{M}_n(F)$ give rise to isomorphic $F[T]$-module structures on F^n if and only if they are conjugate.

Since $f(A) = O$, so $f(T)v = 0$ for all $v \in F^n$, the $F[T]$-module structure on F^n can be replaced with an $F[T]/(f(T))$-module structure: $\overline{g(T)}v = g(A)v$. The ring $F[T]/(f(T))$ is a field since $f(T)$ is irreducible, so F^n is an $F[T]/(f(T))$-vector space. Fixing a nonzero $v_0 \in F^n$, the multiples $F[T] \cdot v_0 = (F[T]/(f(T))) \cdot v_0$ form a subspace of F^n with F-dimension $\dim_F(F[T]/(f(T))) = n$, so it fills up all of F^n: $F^n = (F[T]/(f(T))) \cdot v_0$. Since $v_0 \neq 0$ and $F[T]/(f(T))$ is a field, $F[T]/(f(T)) \cong F[T]/(f(T)) \cdot v_0$ as $F[T]$-modules, so $F^n \cong F[T]/(f(T))$ as $F[T]$-modules. $\square$

Another key point in Theorem 1 besides irreducibility of the characteristic polynomial is that we are working over a field. If we work over $\mathbf{Z}$, irreducible characteristic polynomials don't necessarily provide a complete conjugacy invariant anymore. That is, two matrices in $\mathrm{M}_n(\mathbf{Z})$ can have a common irreducible characteristic polynomial while not being conjugate in $\mathrm{M}_n(\mathbf{Z})$ (but they must be conjugate in $\mathrm{M}_n(\mathbf{Q})$).

Example 2. The integral matrices $A = \left(\begin{smallmatrix} 0 & 4 \\ 2 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 8 \\ 1 & 0 \end{smallmatrix}\right)$ both have characteristic polynomial $T^2 - 8$, which is irreducible in $\mathbf{Z}[T]$, but they are not conjugate in $\mathrm{M}_2(\mathbf{Z})$. We show this by contradiction. Assume $UAU^{-1} = B$ for some $U \in \mathrm{GL}_2(\mathbf{Z})$. Then $UA = BU$. Apply both sides to $\binom{1}{0}$: $U\binom{0}{2} = BU\binom{1}{0}$. Let $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, so $\binom{2b}{2d} = B\binom{a}{c} = \binom{8c}{a}$. Then $b = 4c$ and $a = 2d$, so $\pm 1 = ad - bc = 2d^2 - 4c^2$, a contradiction.

Since $T^2 - 8$ is irreducible in $\mathbf{Q}[T]$, Theorem 1 says A and B are conjugate in $\mathrm{M}_2(\mathbf{Q})$, and indeed $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/2 \end{smallmatrix}\right)A\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/2 \end{smallmatrix}\right)^{-1} = B$.

If two integral matrices have the same irreducible characteristic polynomial, what additional data is needed to decide if the matrices are conjugate over $\mathbf{Z}$? This task turns out to be equivalent to finding the ideal classes in an order in a number field.

Let's recall some terminology. In any order $\mathcal{O}$ in a number field K, a *fractional $\mathcal{O}$-ideal* is a nonzero finitely generated $\mathcal{O}$-module in K. We call two fractional $\mathcal{O}$-ideals I and J *equivalent* if $I = xJ$ for some $x \in K^\times$. The equivalence classes are called (fractional) *$\mathcal{O}$-ideal classes* and there are finitely many of them. When $\mathcal{O} = \mathcal{O}_K$, every fractional $\mathcal{O}$-ideal is invertible. When $\mathcal{O} \neq \mathcal{O}_K$ there are some noninvertible fractional $\mathcal{O}$-ideals. The label "ideal classes" here allows *all* fractional $\mathcal{O}$-ideals, invertible and noninvertible.

Theorem 3. *Let $f(T) \in \mathbf{Z}[T]$ be monic irreducible of degree n.*

(a) *A matrix A in $\mathrm{M}_n(\mathbf{Z})$ has characteristic polynomial $f(T)$ if and only if $f(A) = O$.*

(b) *Conjugacy classes of matrices in $\mathrm{M}_n(\mathbf{Z})$ with characteristic polynomial $f(T)$ are in bijection with the $\mathbf{Z}[\alpha]$-ideal classes in $\mathbf{Q}(\alpha)$, where α is a root of $f(T)$.*

In particular, there are finitely many conjugacy classes of matrices in $\mathrm{M}_n(\mathbf{Z})$ with characteristic polynomial $f(T)$, since $\mathbf{Z}[\alpha]$ has finitely many ideal classes.

Theorem 3 is due to Latimer and MacDuffee [1]. See also [2, pp. 49–55], [3], and [4].

Example 4. Taking $f(T) = T^2 + 1$, all $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 + I_2 = O$ are conjugate since $\mathbf{Z}[i]$ has class number 1. One such matrix is $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Example 5. Taking $f(T) = T^2 + 5$, all $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 + 5I_2 = O$ fall into two conjugacy classes since $\mathbf{Z}[\sqrt{-5}]$ has class number 2.

Example 6. Taking $f(T) = T^3 - 2$, all $A \in \mathrm{M}_3(\mathbf{Z})$ satisfying $A^3 = 2I_3$ are conjugate to each other in $\mathrm{M}_3(\mathbf{Z})$ since $\mathbf{Z}[\sqrt[3]{2}]$ has class number 1.

Now we prove Theorem 3.

Proof. (a) The proof in Theorem 1(a) carries over, since a monic irreducible in $\mathbf{Z}[T]$ is irreducible in $\mathbf{Q}[T]$.

(b) For any $\mathbf{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ in $\mathbf{Q}(\alpha)$, multiplication by α is a $\mathbf{Z}$-linear map $m_\alpha \colon \mathfrak{a} \to \mathfrak{a}$. Since $\mathfrak{a}$ as a $\mathbf{Z}$-module has a basis of size n, choosing a $\mathbf{Z}$-basis lets us represent m_α by a matrix $[m_\alpha] \in \mathrm{M}_n(\mathbf{Z})$. Changing the $\mathbf{Z}$-basis of $\mathfrak{a}$ changes the matrix representation of m_α to a conjugate matrix. So independent of a choice of basis we can associate to a fractional ideal $\mathfrak{a}$ the *conjugacy class* in $\mathrm{M}_n(\mathbf{Z})$ of a matrix representation for $m_\alpha \colon \mathfrak{a} \to \mathfrak{a}$. All matrices A in this conjugacy class satisfy $f(A) = O$ since $f(A) = f([m_\alpha]) = [m_{f(\alpha)}] = [m_0] = O$.

For an equivalent fractional $\mathbf{Z}[\alpha]$-ideal $\mathfrak{b} = x\mathfrak{a}$, where $x \in \mathbf{Q}(\alpha)^\times$, its conjugacy class of matrices (the matrices representing $m_\alpha \colon \mathfrak{b} \to \mathfrak{b}$ with respect to $\mathbf{Z}$-bases of $\mathfrak{b}$) is the same as that for $\mathfrak{a}$, since the matrix for m_α with respect to a $\mathbf{Z}$-basis $\{e_1, \ldots, e_n\}$ of $\mathfrak{a}$ is the same matrix as that for m_α with respect to the $\mathbf{Z}$-basis $\{xe_1, \ldots, xe_n\}$ of $\mathfrak{b}$. Thus we have a well-defined function

$$(1) \qquad \mathbf{Z}[\alpha]\text{-ideal classes in } \mathbf{Q}(\alpha) \rightsquigarrow \text{conjugacy classes of } A \in \mathrm{M}_n(\mathbf{Z}) \text{ such that } f(A) = O$$

by the rule: pick a fractional ideal in the ideal class, pick a $\mathbf{Z}$-basis of it, write a matrix representation for m_α in terms of this basis, and use the conjugacy class of that matrix. We will show this function from fractional ideal classes to conjugacy classes of matrices is a bijection.

To show surjectivity, for every $A \in \mathrm{M}_n(\mathbf{Z})$ satisfying $f(A) = O$ we will find a $\mathbf{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ in $\mathbf{Q}(\alpha)$ such that A is the matrix representation for $m_\alpha \colon \mathfrak{a} \to \mathfrak{a}$ with respect to some $\mathbf{Z}$-basis of $\mathfrak{a}$. Let $K = \mathbf{Q}(\alpha) = \mathbf{Q}[\alpha]$. Make $\mathbf{Q}^n$ into a K-vector space in the following way. For $c \in K$, write $c = g(\alpha)$ for $g(T) \in \mathbf{Q}[T]$. For $v \in \mathbf{Q}^n$, set

$$(2) \qquad cv = g(\alpha)v := g(A)v$$

This is well-defined: if $c = h(\alpha)$ for $h(T) \in \mathbf{Q}[T]$ then $g(\alpha) = h(\alpha)$, so $g(T) - h(T)$ is divisible by $f(T)$ (because f is the minimal polynomial of α in $\mathbf{Q}[T]$, as it is monic irreducible with root α) and therefore $g(A) = h(A)$ as matrices (since $f(A) = O$), so $g(A)v = h(A)v$ for all $v \in \mathbf{Q}^n$. If $v \in \mathbf{Z}^n$ then $\alpha v = Av$ is in $\mathbf{Z}^n$ since A has integral entries, so $\mathbf{Z}^n$ is a $\mathbf{Z}[\alpha]$-submodule of $\mathbf{Q}^n$ that is finitely generated since $\mathbf{Z}^n$ is already finitely generated as an abelian group. From the way we define $\mathbf{Q}^n$ as a K-vector space, the equation $\alpha v = Av$ tells us the matrix representation of m_α on $\mathbf{Z}^n$ with respect to the standard basis of $\mathbf{Z}^n$ is A.

Treating $\mathbf{Q}^n$ as both a $\mathbf{Q}$-vector space and as K-vector space (by (2)), we have

$$n = \dim_{\mathbf{Q}}(\mathbf{Q}^n) = [K : \mathbf{Q}] \dim_K(\mathbf{Q}^n) = n \dim_K(\mathbf{Q}^n),$$

so $\mathbf{Q}^n$ is 1-dimensional as a K-vector space. That means for any nonzero $v_0 \in \mathbf{Q}^n$, the K-linear map $\varphi_{v_0} \colon K \to \mathbf{Q}^n$ given by $\varphi_{v_0}(c) = cv_0$ is an isomorphism of 1-dimensional K-vector spaces. The inverse image $\varphi_{v_0}^{-1}(\mathbf{Z}^n)$ is a finitely generated $\mathbf{Z}[\alpha]$-submodule of K since $\mathbf{Z}^n$ has these properties inside $\mathbf{Q}^n$. So $\varphi_{v_0}^{-1}(\mathbf{Z}^n)$ is a fractional $\mathbf{Z}[\alpha]$-ideal in K. Call it $\mathfrak{a}$, so

$$\mathfrak{a} = \varphi_{v_0}^{-1}(\mathbf{Z}^n) = \{c \in K : cv_0 \in \mathbf{Z}^n\}.$$

Since A is the matrix representation of m_α on $\mathbf{Z}^n$ with respect to its standard basis $e_1, \ldots, e_n$, A is also the matrix representation of m_α on $\mathfrak{a}$ with respect to the $\mathbf{Z}$-basis $\varphi_{v_0}^{-1}(e_1), \ldots, \varphi_{v_0}^{-1}(e_n)$ of $\mathfrak{a}$. We have realized A as a matrix representation for m_α on a fractional $\mathbf{Z}[\alpha]$-ideal $\mathfrak{a}$, so (1) is onto.

To show (1) is injective, suppose $\mathfrak{a}$ and $\mathfrak{b}$ are two fractional $\mathbf{Z}[\alpha]$-ideals in K such that the matrices A and B for m_α with respect to some $\mathbf{Z}$-bases of $\mathfrak{a}$ and $\mathfrak{b}$ are conjugate in $\mathrm{M}_n(\mathbf{Z})$. We want to show $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class: $\mathfrak{b} = x\mathfrak{a}$ for some $x \in K^\times$.

Since A represents $m_\alpha \colon \mathfrak{a} \to \mathfrak{a}$ with respect to some $\mathbf{Z}$-basis $\mathcal{A}$ of $\mathfrak{a}$, there is a commutative diagram

$$\begin{tikzcd}
\mathfrak{a} \arrow[r, "{[\cdot]_{\mathcal{A}}}"] \arrow[d, "m_\alpha"'] & \mathbf{Z}^n \arrow[d, "A"] \\
\mathfrak{a} \arrow[r, "{[\cdot]_{\mathcal{A}}}"'] & \mathbf{Z}^n
\end{tikzcd}$$

where the horitzonal arrows are the coordinate isomorphisms that identify $\mathcal{A}$ with the standard basis of $\mathbf{Z}^n$. Similarly for the basis $\mathcal{B}$ of $\mathfrak{b}$ with respect to which $m_\alpha\colon \mathfrak{b} \to \mathfrak{b}$ has matrix representation B, we have a commutative diagram

$$\begin{tikzcd}
\mathfrak{b} \arrow[r, "{[\cdot]_{\mathcal{B}}}"] \arrow[d, "m_\alpha"'] & \mathbf{Z}^n \arrow[d, "B"] \\
\mathfrak{b} \arrow[r, "{[\cdot]_{\mathcal{B}}}"'] & \mathbf{Z}^n
\end{tikzcd}.$$

Since A and B are conjugate in $\mathrm{M}_n(\mathbf{Z})$, $B = UAU^{-1}$ for some $U \in \mathrm{GL}_n(\mathbf{Z})$, so

$$\begin{tikzcd}
\mathbf{Z}^n \arrow[r, "U"] \arrow[d, "A"'] & \mathbf{Z}^n \arrow[d, "B"] \\
\mathbf{Z}^n \arrow[r, "U"'] & \mathbf{Z}^n
\end{tikzcd}$$

commutes. Let's put these diagrams together:

$$\begin{tikzcd}
\mathfrak{a} \arrow[r, "{[\cdot]_{\mathcal{A}}}"] \arrow[d, "m_\alpha"'] & \mathbf{Z}^n \arrow[r, "U"] \arrow[d, "A"'] & \mathbf{Z}^n \arrow[r, "{[\cdot]_{\mathcal{B}}^{-1}}"] \arrow[d, "B"'] & \mathfrak{b} \arrow[d, "m_\alpha"] \\
\mathfrak{a} \arrow[r, "{[\cdot]_{\mathcal{A}}}"'] & \mathbf{Z}^n \arrow[r, "U"'] & \mathbf{Z}^n \arrow[r, "{[\cdot]_{\mathcal{B}}^{-1}}"'] & \mathfrak{b}
\end{tikzcd}$$

Each square in the diagram commutes, so the whole diagram commutes. The top and bottom maps are $\mathbf{Z}$-linear isomorphisms, so the common composite map $\mathfrak{a} \to \mathfrak{b}$ on the top and bottom is a $\mathbf{Z}$-linear isomorphism which commutes with m_α by commutativity of the diagram around the boundary. That implies the composite map $\mathfrak{a} \to \mathfrak{b}$ is $\mathbf{Z}[\alpha]$-linear, not just $\mathbf{Z}$-linear, so $\mathfrak{a}$ and $\mathfrak{b}$ are isomorphic as $\mathbf{Z}[\alpha]$-modules. Isomorphic fractional $\mathbf{Z}[\alpha]$-ideals are scalar multiples of each other, so $\mathfrak{b} = x\mathfrak{a}$ for some $x \in K^\times$. □

Remark 7. Here is a more conceptual version of the proof of part b.

The fractional $\mathbf{Z}[\alpha]$-ideals are the $\mathbf{Z}[\alpha]$-modules in $\mathbf{Q}(\alpha)$ which are free of rank n as $\mathbf{Z}$-modules. Moreover, any abstract $\mathbf{Z}[\alpha]$-module M whose underlying additive group is $\mathbf{Z}^n$ is isomorphic as a $\mathbf{Z}[\alpha]$-module to a fractional $\mathbf{Z}[\alpha]$-ideal. (Proof: Since $M \cong \mathbf{Z}^n$ as abelian groups, $\mathbf{Q} \otimes_{\mathbf{Z}} M \cong \mathbf{Q}^n$ as $\mathbf{Q}$-vector spaces. Since M is a $\mathbf{Z}[\alpha]$-module, $\mathbf{Q} \otimes_{\mathbf{Z}} M$ is a module over $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}[\alpha] \cong \mathbf{Q}(\alpha)$, and since $\dim_{\mathbf{Q}}(\mathbf{Q}(\alpha)) = n = \dim_{\mathbf{Q}}(\mathbf{Q} \otimes_{\mathbf{Z}} M)$, $\mathbf{Q} \otimes_{\mathbf{Z}} M$ has dimension 1 as a $\mathbf{Q}(\alpha)$-vector space. Using any vector space isomorphism of $\mathbf{Q} \otimes_{\mathbf{Z}} M$ with $\mathbf{Q}(\alpha)$ lets us identify the subset $1 \otimes M$ of $\mathbf{Q} \otimes_{\mathbf{Z}} M$ with a $\mathbf{Z}[\alpha]$-module in $\mathbf{Q}(\alpha)$ that's additively $\mathbf{Z}^n$, and this is a fractional $\mathbf{Z}[\alpha]$-ideal in $\mathbf{Q}(\alpha)$.) Fractional $\mathbf{Z}[\alpha]$-ideals are equivalent precisely when they are isomorphic as $\mathbf{Z}[\alpha]$-modules, so $\mathbf{Z}[\alpha]$-ideal classes in $\mathbf{Q}(\alpha)$ can be identified with isomorphism classes of $\mathbf{Z}[\alpha]$-modules which additively are $\mathbf{Z}^n$, or equivalently with isomorphism classes of $\mathbf{Z}[\alpha]$-module *structures* on $\mathbf{Z}^n$.

Next we show $\mathbf{Z}[\alpha]$-module structures on $\mathbf{Z}^n$ are in bijection with conjugacy classes of $A \in \mathrm{M}_n(\mathbf{Z})$ such that $f(A) = O$. A $\mathbf{Z}[\alpha]$-module structure on $\mathbf{Z}^n$ is the same as equipping $\mathbf{Z}^n$ with a linear map $A\colon \mathbf{Z}^n \to \mathbf{Z}^n$ such that $f(A) = O$. (The action of A on $\mathbf{Z}^n$ is interpreted as multiplication by α, which gives $\mathbf{Z}^n$ a $\mathbf{Z}[\alpha]$-module structure.) Two such A define isomorphic

$\mathbf{Z}[\alpha]$-module structures on $\mathbf{Z}^n$ precisely when they are conjugate in $\mathrm{M}_n(\mathbf{Z})$[1], so $\mathbf{Z}[\alpha]$-module structures on $\mathbf{Z}^n$, up to isomorphism, can be identified with conjugacy classes of solutions to $f(A) = O$ in $\mathrm{M}_n(\mathbf{Z})$.

To illustrate Theorem 3 in examples, for some monic irreducible $f(T) \in \mathbf{Z}[T]$ we write down a set of ideals in $\mathbf{Z}[\alpha]$, where $f(\alpha) = 0$, which represent the different $\mathbf{Z}[\alpha]$-ideal classes and compute the matrix for multiplication by α on each ideal with respect to a $\mathbf{Z}$-basis of that ideal. The resulting matrices are a complete set of representatives for the conjugacy classes of all $A \in \mathrm{M}_n(\mathbf{Z})$ satisfying $f(A) = O$, where $n = \deg f$. Our examples will have $\deg f = 2$.

Example 8. Let $f(T) = T^2 + 5$ and $\alpha = \sqrt{-5}$. We seek representatives for the conjugacy classes of $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 + 5I_2 = O$. The ring $\mathbf{Z}[\alpha] = \mathbf{Z}[\sqrt{-5}]$ has class number 2, with ideal classes represented by (1) and $(2, 1+\sqrt{-5})$. To find matrices in $\mathrm{M}_2(\mathbf{Z})$ associated to multiplication by α on the ideals (1) and $(2, 1+\sqrt{-5})$ we need $\mathbf{Z}$-bases of the ideals: $(1) = \mathbf{Z} + \sqrt{-5}\mathbf{Z}$ and $(2, 1+\sqrt{-5}) = 2\mathbf{Z} + (1+\sqrt{-5})\mathbf{Z}$. Multiplying the $\mathbf{Z}$-basis $\{1, \sqrt{-5}\}$ of (1) by $\sqrt{-5}$,

$$\begin{aligned} \sqrt{-5} \cdot 1 &= 0 \cdot 1 + 1 \cdot \sqrt{-5} \\ \sqrt{-5} \cdot \sqrt{-5} &= -5 \cdot 1 + 0 \cdot \sqrt{-5}, \end{aligned}$$

and multiplying the basis $\{2, 1+\sqrt{-5}\}$ of $(2, 1+\sqrt{-5})$ by $\sqrt{-5}$,

$$\begin{aligned} \sqrt{-5} \cdot 2 &= (-1) \cdot 2 + 2 \cdot (1+\sqrt{-5}) \\ \sqrt{-5} \cdot (1+\sqrt{-5}) &= (-3) \cdot 2 + 1 \cdot (1+\sqrt{-5}). \end{aligned}$$

Therefore multiplication by $\sqrt{-5}$ on these two ideals is represented by the matrices $\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. That means any $A \in \mathrm{M}_2(\mathbf{Z})$ which satisfies $A^2 + 5I_2 = O$ is conjugate to exactly one of these two matrices.

Another pair of ideals representing the two ideal classes is $(4+\sqrt{-5})$ and $(7, 2+3\sqrt{-5})$. Let's convert these into matrices. The first ideal has $\mathbf{Z}$-basis $\{4+\sqrt{-5}, -5+4\sqrt{-5}\}$, and

$$\begin{aligned} \sqrt{-5} \cdot (4+\sqrt{-5}) &= 0 \cdot (4+\sqrt{-5}) + 1 \cdot (-5+4\sqrt{-5}) \\ \sqrt{-5} \cdot (-5+4\sqrt{-5}) &= -5 \cdot 1 + 0 \cdot \sqrt{-5}, \end{aligned}$$

so multiplication by $\sqrt{-5}$ with respect to this basis is $\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$. Is it a coincidence we get the same matrix as we did for multiplication by $\sqrt{-5}$ on the ideal (1)? Not really. For any principal ideal $(a+b\sqrt{-5})$ the matrix for multiplication by $\sqrt{-5}$ with respect to the obvious first choice of $\mathbf{Z}$-basis – $\{a+b\sqrt{-5}, -5b+a\sqrt{-5}\}$ – is $\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$. Just compute it and see. So it's just a fluke of carrying out the computation on what happens to be the first basis that comes to mind. If you use a different basis of a principal ideal you would get a different matrix. Turning now to the second ideal $(7, 2+3\sqrt{-5})$, multiplying 7 and $2+3\sqrt{-5}$ by $\sqrt{-5}$ leads to the equations

$$\begin{aligned} \sqrt{-5} \cdot 7 &= -\frac{2}{3} \cdot 7 + 7 \cdot (2+3\sqrt{-5}) \\ \sqrt{-5} \cdot (2+3\sqrt{-5}) &= -\frac{7}{3} \cdot 7 + \frac{2}{3} \cdot (2+3\sqrt{-5}). \end{aligned}$$

[1] This is similar to a vector space V over a field F having isomorphic $F[T]$-module structures from two linear operators A and B on V if and only if A and B are conjugate in $\mathrm{End}_F(V)$.

How come we got rational coefficients and not integral coefficients? Because the computation needs a $\mathbf{Z}$-basis of $(7, 2+3\sqrt{-5})$ but $\{7, 2+3\sqrt{-5}\}$ is *not* a $\mathbf{Z}$-basis (*e.g.*, $7\sqrt{-5}$ is in the ideal but it is not in the $\mathbf{Z}$-span of 7 and $2+3\sqrt{-5}$.) A $\mathbf{Z}$-basis of $(7, 2+3\sqrt{-5})$ is $\{7, 3+\sqrt{-5}\}$ (check!) and relative to this basis

$$\begin{aligned} \sqrt{-5}\cdot 7 &= -3\cdot 7 + 7\cdot(3+\sqrt{-5}) \\ \sqrt{-5}\cdot(3+\sqrt{-5}) &= -2\cdot 7 + 3\cdot(3+\sqrt{-5}), \end{aligned}$$

so the corresponding matrix is $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right)$. Therefore $\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right)$ are a pair of conjugacy class representatives of $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 + 5I_2 = O$.

Example 9. Let $f(T) = T^2 - T + 6 = 0$, with root $\alpha = \frac{1+\sqrt{-23}}{2}$. The ring $\mathbf{Z}[\alpha]$ has class number 3, with ideal classes represented by (1), $(2,\alpha)$, and $(2,\alpha)^2 = (4, 6+\alpha)$. As $\mathbf{Z}$-modules, these ideals have respective $\mathbf{Z}$-bases $\{1,\alpha\}$, $\{2,\alpha\}$, and $\{4, 6+\alpha\}$.

The matrices for multiplication by α on these ideals, with respect to the indicated $\mathbf{Z}$-bases of them, are found as follows:

$$\begin{aligned} \alpha\cdot 1 &= 0\cdot 1 + 1\cdot\alpha \\ \alpha\cdot\alpha &= -6\cdot 1 + 1\cdot\alpha, \end{aligned}$$

$$\begin{aligned} \alpha\cdot 2 &= 0\cdot 1 + 2\cdot\alpha \\ \alpha\cdot\alpha &= -3\cdot 2 + 1\cdot\alpha, \end{aligned}$$

$$\begin{aligned} \alpha\cdot 4 &= (-6)\cdot 4 + 4\cdot(6+\alpha) \\ \alpha\cdot(6+\alpha) &= (-12)\cdot 4 + 7\cdot(6+\alpha), \end{aligned}$$

so the three conjugacy classes of $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 - A + 6I_2 = O$ are represented by $\left(\begin{smallmatrix} 0 & -6 \\ 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -3 \\ 2 & 1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} -6 & -12 \\ 4 & 7 \end{smallmatrix}\right)$.

Example 10. Let d be a nonsquare in $\mathbf{Z}$ and $m \geq 2$. Then $f(T) = T^2 - m^2 d$ is irreducible in $\mathbf{Z}[T]$ with root $\alpha = m\sqrt{d}$. Both $\mathfrak{a} := \mathbf{Z}[\sqrt{d}] = \mathbf{Z} + \mathbf{Z}\sqrt{d}$ and $\mathfrak{b} := \mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}m\sqrt{d}$ are fractional $\mathbf{Z}[\alpha]$-ideals in $\mathbf{Q}(\alpha)$ which do not lie in the same $\mathbf{Z}[\alpha]$-ideal class. (As fractional $\mathbf{Z}[\alpha]$-ideals, $\mathfrak{b}$ is principal and $\mathfrak{a}$ is nonprincipal.) We are *not* saying every $\mathbf{Z}[\alpha]$-fractional ideal is equivalent to $\mathfrak{a}$ or $\mathfrak{b}$, but only that $\mathfrak{a}$ and $\mathfrak{b}$ are inequivalent.

To find matrices satisfying $f(A) = O$ which correspond to $\mathfrak{a}$ and $\mathfrak{b}$, we compute the matrix for multiplication by $\alpha = m\sqrt{d}$ with respect to $\mathbf{Z}$-bases of each of them. Using the $\mathbf{Z}$-bases $\{1, \sqrt{d}\}$ for $\mathfrak{a}$ and $\{1, m\sqrt{d}\}$ for $\mathfrak{b}$,

$$\begin{aligned} m\sqrt{d}\cdot 1 &= 0\cdot 1 + m\cdot\sqrt{d} \\ m\sqrt{d}\cdot\sqrt{d} &= md\cdot 1 + 0\cdot\sqrt{d}, \end{aligned}$$

and

$$\begin{aligned} m\sqrt{d}\cdot 1 &= 0\cdot 1 + 1\cdot m\sqrt{d} \\ m\sqrt{d}\cdot m\sqrt{d} &= m^2 d\cdot 1 + 0\cdot m\sqrt{d}, \end{aligned}$$

so the matrices are $\left(\begin{smallmatrix} 0 & md \\ m & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & m^2 d \\ 1 & 0 \end{smallmatrix}\right)$. These both satisfy $A^2 = m^2 d I_2$ and they are nonconjugate in $\mathrm{M}_2(\mathbf{Z})$. Taking $d = 2$ and $m = 2$ recovers Example 2, where the nonconjugate matrices $\left(\begin{smallmatrix} 0 & 4 \\ 2 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 8 \\ 1 & 0 \end{smallmatrix}\right)$ can now be interpreted as multiplication by $\sqrt{8} = 2\sqrt{2}$ on $\mathbf{Z}[\sqrt{2}]$ with respect to the $\mathbf{Z}$-basis $\{1, \sqrt{2}\}$ and on $\mathbf{Z}[2\sqrt{2}]$ with respect to the $\mathbf{Z}$-basis $\{1, 2\sqrt{2}\}$.

The matrix $\left(\begin{smallmatrix}1&0\\0&1/2\end{smallmatrix}\right)$ in $\mathrm{M}_2(\mathbf{Q})$ that conjugates $\left(\begin{smallmatrix}0&4\\2&0\end{smallmatrix}\right)$ to $\left(\begin{smallmatrix}0&8\\1&0\end{smallmatrix}\right)$ can now be explained: it is the change of basis matrix from $\{1, 2\sqrt{2}\}$ to $\{1, \sqrt{2}\}$ as $\mathbf{Q}$-bases of $\mathbf{Q}(\sqrt{2})$.

Example 11. So far we have computed matrices from fractional ideals. Let's go the other way around. The matrix $A = \left(\begin{smallmatrix}2&3\\-3&-2\end{smallmatrix}\right)$ satisfies $A^2 + 5I_2 = O$. We will convert A into a $\mathbf{Z}[\sqrt{-5}]$-fractional ideal in $\mathbf{Q}(\sqrt{-5})$ using the proof of the surjectivity in Theorem 3(b). Make $\mathbf{Q}^2$ into a $\mathbf{Q}(\sqrt{-5})$-vector space by

$$(a+b\sqrt{-5})\begin{pmatrix}x\\y\end{pmatrix} := (a+bA)\begin{pmatrix}x\\y\end{pmatrix} = \left(a+b\begin{pmatrix}2&3\\-3&-2\end{pmatrix}\right)\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}a+2b&3b\\-3b&a-2b\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}.$$

Set $v_0 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, so there is an isomorphism $\mathbf{Q}(\sqrt{-5}) \to \mathbf{Q}^2$ as $\mathbf{Q}(\sqrt{-5})$-vector spaces by $c \mapsto cv_0$. The fractional ideal we want is the inverse image of $\mathbf{Z}^2$ under this isomorphism $\mathbf{Q}(\sqrt{-5}) \to \mathbf{Q}^2$. This is $\{c \in \mathbf{Q}(\sqrt{-5}) : cv_0 \in \mathbf{Z}^2\}$. Writing $c = a + b\sqrt{-5}$,

$$cv_0 = (a+bA)\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a+2b\\-3b\end{pmatrix} = \begin{pmatrix}1&2\\0&-3\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix},$$

so

$$cv_0 \in \mathbf{Z}^2 \iff \begin{pmatrix}a\\b\end{pmatrix} \in \begin{pmatrix}1&2\\0&-3\end{pmatrix}^{-1}\mathbf{Z}^2 = \begin{pmatrix}1&2/3\\0&-1/3\end{pmatrix}\mathbf{Z}^2 = \left\{\begin{pmatrix}x+(2/3)y\\-(1/3)y\end{pmatrix} : x, y \in \mathbf{Z}\right\}.$$

Therefore having $cv_0 \in \mathbf{Z}^2$ is the same as saying $c = x + (2/3)y - (1/3)y\sqrt{-5}$ for some integers x and y, so the $\mathbf{Z}[\sqrt{-5}]$-fractional ideal in $\mathbf{Q}(\sqrt{-5})$ corresponding to A is

$$\left\{x + \left(\frac{2}{3} - \frac{1}{3}\sqrt{-5}\right)y : x, y \in \mathbf{Z}\right\} = \mathbf{Z} + \left(\frac{2-\sqrt{-5}}{3}\right)\mathbf{Z}. \tag{3}$$

If we change $v_0 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ to another nonzero vector in $\mathbf{Q}^2$, we get an equivalent fractional ideal. The ideal class of these fractional ideals is independent of the choice of v_0. Scaling a fractional ideal doesn't change its ideal class, so we multiply the fractional ideal by 3 and get the ideal $3\mathbf{Z} + (2-\sqrt{-5})\mathbf{Z} = (3, 2-\sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$.

As a check that our work is correct, let's compute the matrix for multiplication by $\sqrt{-5}$ on the ideal $(3, 2-\sqrt{-5})$ using the $\mathbf{Z}$-basis $\{3, 2-\sqrt{-5}\}$:

$$\begin{aligned}\sqrt{-5}\cdot 3 &= 2\cdot 3 - 3(2-\sqrt{-5})\\ \sqrt{-5}\cdot(2-\sqrt{-5}) &= 3\cdot 3 - 2\cdot(2-\sqrt{-5}),\end{aligned}$$

so the matrix is $\left(\begin{smallmatrix}2&3\\-3&-2\end{smallmatrix}\right) = A$.

Wait, there's more! In Example 8 we said any $A \in \mathrm{M}_2(\mathbf{Z})$ satisfying $A^2 + 5I_2 = O$ is conjugate to either $\left(\begin{smallmatrix}0&-5\\1&0\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}-1&-3\\2&1\end{smallmatrix}\right)$. Which of these is $\left(\begin{smallmatrix}2&3\\-3&-2\end{smallmatrix}\right)$ conjugate to? We will answer this by turning it into a question about ideals. Table 11 summarizes the list of matrices and corresponding ideals and their $\mathbf{Z}$-bases with respect to which the matrix represents multiplication by $\sqrt{-5}$ on the ideal.

Matrix	Ideal	Basis
$\left(\begin{smallmatrix}0&-5\\1&0\end{smallmatrix}\right)$	(1)	$\{1, \sqrt{-5}\}$
$\left(\begin{smallmatrix}-1&-3\\2&1\end{smallmatrix}\right)$	$(2, 1+\sqrt{-5})$	$\{2, 1+\sqrt{-5}\}$
$\left(\begin{smallmatrix}2&3\\-3&-2\end{smallmatrix}\right)$	$(3, 2-\sqrt{-5})$	$\{3, 2-\sqrt{-5}\}$

The ideal $(3, 2-\sqrt{-5})$ is equivalent to (1) or $(2, 1+\sqrt{-5})$: it is principal or nonprincipal. We show $(3, 2-\sqrt{-5})$ is not principal by looking at the quotient ring

$$\mathbf{Z}[\sqrt{-5}]/(3, 2-\sqrt{-5}) \cong \mathbf{Z}[T]/(T^2+5, 3, 2-T) \cong \mathbf{Z}/3\mathbf{Z}.$$

If $(3, 2-\sqrt{-5}) = (\gamma)$ is principal then $\#\mathbf{Z}[\sqrt{-5}]/(\gamma) = 3$, so $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})/\mathbf{Q}}(\gamma) = 3$. But no element of $\mathbf{Z}[\sqrt{-5}]$ has norm 3. So $(3, 2-\sqrt{-5})$ is not principal, which makes it equivalent to $(2, 1+\sqrt{-5})$, so $\left(\begin{smallmatrix} 2 & 3 \\ -3 & -2 \end{smallmatrix}\right)$ is conjugate in $\mathrm{M}_2(\mathbf{Z})$ to $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$.

Now it is natural to ask for an explicit conjugating matrix between $\left(\begin{smallmatrix} 2 & 3 \\ -3 & -2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. To find one, we will find an explicit scaling factor between the ideals $(3, 2-\sqrt{-5})$ and $(2, 1+\sqrt{-5})$. There is an $x \in \mathbf{Q}(\sqrt{-5})$ such that $(3, 2-\sqrt{-5}) = x(2, 1+\sqrt{-5})$. To find x, multiply both sides by $(2, 1+\sqrt{-5})$. The right side becomes $x(2) = (2x)$ and the left side becomes

$$(3, 2-\sqrt{-5})(2, 1+\sqrt{-5}) = (6, 3+3\sqrt{-5}, 4-2\sqrt{-5}, 7+\sqrt{-5}).$$

We can eliminate the middle two generators since $3+3\sqrt{-5} = (-3)\cdot 6 + 3(7+\sqrt{-5})$ and $4-2\sqrt{-5} = 3\cdot 6 - 2(7+\sqrt{-5})$, so

$$\begin{aligned}
(3, 2-\sqrt{-5})(2, 1+\sqrt{-5}) &= (6, 7+\sqrt{-5}) \\
&= ((1+\sqrt{-5})(1-\sqrt{-5}), (1+\sqrt{-5})(2-\sqrt{-5})) \\
&= (1+\sqrt{-5})(1-\sqrt{-5}, 2-\sqrt{-5}) \\
&= (1+\sqrt{-5}).
\end{aligned}$$

Therefore $(1+\sqrt{-5}) = (2x)$, so we can use $x = \frac{1+\sqrt{-5}}{2}$:

$$(3, 2-\sqrt{-5}) = \frac{1+\sqrt{-5}}{2}(2, 1+\sqrt{-5}).$$

Since $(3, 2-\sqrt{-5})$ and $(2, 1+\sqrt{-5})$ are scalar multiples of each other, we can multiply the chosen $\mathbf{Z}$-basis of $(2, 1+\sqrt{-5})$ in Table 11 by $\frac{1+\sqrt{-5}}{2}$ to express the second matrix in the table as a representation of multiplication by $\sqrt{-5}$ on the ideal $(3, 2-\sqrt{-5})$:

$$\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix} = [m_{\sqrt{-5}}] \text{ on } (3, 2-\sqrt{-5}) \text{ with respect to } \{1+\sqrt{-5}, -2+\sqrt{-5}\}.$$

The matrices $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 3 \\ -3 & -2 \end{smallmatrix}\right)$ are now seen as representations of $m_{\sqrt{-5}}$ with respect to different $\mathbf{Z}$-bases of the *same* ideal $(3, 2-\sqrt{-5})$. (That is the special feature of equivalent fractional ideals: a basis of one can be scaled to a basis of the other, so a matrix representation on one is also valid on the other.) All we have to do now is compute the change of basis matrix for the two bases $\{1+\sqrt{-5}, -2+\sqrt{-5}\}$ and $\{3, 2-\sqrt{-5}\}$ of $(3, 2-\sqrt{-5})$. Writing the second basis in terms of the first,

$$3 = 1\cdot(1+\sqrt{-5}) + (-1)\cdot(-2+\sqrt{-5}), \quad 2-\sqrt{-5} = 0\cdot(1+\sqrt{-5}) + (-1)\cdot(-2+\sqrt{-5}).$$

The change of basis matrix is $\left(\begin{smallmatrix} 1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 0 \\ -1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ -1 & -1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 2 & 3 \\ -3 & -2 \end{smallmatrix}\right)$.

Example 12. Let's find an integral matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{Z})$ such that A and $A^\top$ are not conjugate to each other in $\mathrm{M}_2(\mathbf{Z})$. (In $\mathrm{M}_n(F)$ for any field F, a matrix and its transpose are conjugate.) The characteristic polynomials of A and $A^\top$ are the same, namely

$$\chi(T) = T^2 - (a+d)T + (ad-bc) \in \mathbf{Z}[T].$$

Suppose $\chi(T)$ is irreducible in $\mathbf{Z}[T]$, which is fairly typical anyway. Let α be a root of $\chi(T)$. We will produce ideals in $\mathbf{Z}[\alpha]$ corresponding to A and $A^\top$, and then carefully select a choice of A for which those two ideals are guaranteed to be inequivalent in an appropriate quadratic ring.

Let $K = \mathbf{Q}(\alpha)$, and make $\mathbf{Q}^2$ into a K-vector space by

$$(r+s\alpha)\begin{pmatrix} x \\ y \end{pmatrix} := (r+sA)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r+sa & sb \\ sc & r+sd \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

A fractional $\mathbf{Z}[\alpha]$-ideal corresponding to A in $\mathbf{Z}[\alpha]$ is

$$\mathfrak{a} = \left\{ m+n\alpha : m,n \in \mathbf{Z}, (m+n\alpha)\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbf{Z}^2 \right\} = \left\{ m+n\alpha : m,n \in \mathbf{Z}, \begin{pmatrix} m+na \\ nc \end{pmatrix} \in \mathbf{Z}^2 \right\}.$$

The condition

$$\begin{pmatrix} m+na \\ nc \end{pmatrix} \in \mathbf{Z}^2$$

is the same as

$$\begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} \in \mathbf{Z}^2,$$

so

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}^{-1}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-ay/c \\ y/c \end{pmatrix}$$

with integers x and y. Therefore

$$\mathfrak{a} = \left\{ x - \frac{ay}{c} + \frac{y}{c}\alpha : x,y \in \mathbf{Z} \right\} = \mathbf{Z} + \left(\frac{-a+\alpha}{c}\right)\mathbf{Z}.$$

If we run through this argument using $A^\top$ in place of A, the roles of b and c get flipped, so the corresponding fractional $\mathbf{Z}[\alpha]$-ideal is

$$\mathfrak{a}' = \mathbf{Z} + \left(\frac{-a+\alpha}{b}\right)\mathbf{Z}.$$

Scaling fractional ideals doesn't change the correspondence, so we replace $\mathfrak{a}$ with $c\mathfrak{a}$ and $\mathfrak{a}'$ with $b\mathfrak{a}'$. That is, redefine

$$\mathfrak{a} = (c, a-\alpha), \quad \mathfrak{a}' = (b, a-\alpha).$$

Putting everything together, we can formulate our task in terms of ideals rather than (non)conjugate matrices: find $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{Z})$ such that its characteristic polynomial $\chi(T)$ is irreducible and for a root α of $\chi(T)$ the ideals $(c, a-\alpha)$ and $(b, a-\alpha)$ in $\mathbf{Z}[\alpha]$ are inequivalent. Let's try to get this to work in a quadratic ring $\mathbf{Z}[\sqrt{D}]$. We want $\chi(T) = T^2 - D$ (thus $\alpha = \pm\sqrt{D}$), so A has to have trace 0 and determinant $-D$:

$$a+d = 0, \quad ad-bc = -D.$$

Thus

$$d = -a, \quad a^2+bc = D.$$

Scaling $\mathfrak{a}'$ by c,

$$c\mathfrak{a}' = (bc, ac-c\alpha) = (D-a^2, (a-\alpha)c) = ((\alpha-a)(\alpha+a), (a-\alpha)c) = (a-\alpha)(c, a+\alpha) = (a-\alpha)\overline{\mathfrak{a}},$$

where $\overline{\mathfrak{a}}$ is the conjugate ideal to $\mathfrak{a}$ in the sense of $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ acting on ideals. Thus $\mathfrak{a}'$ is in the same ideal class as $\overline{\mathfrak{a}}$. So we can dispense with $\mathfrak{a}'$ by using $\overline{\mathfrak{a}}$. We seek $\mathfrak{a} = (c, a-\alpha)$ such that $\mathfrak{a}$ is not equivalent to $\overline{\mathfrak{a}}$. If $\mathbf{Z}[\sqrt{D}]$ is the full ring of integers of $\mathbf{Q}(\sqrt{D})$, then $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal[2], so $[\overline{\mathfrak{a}}]$ is the inverse ideal class to $[\mathfrak{a}]$. Asking for $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ to be inequivalent ideals is therefore the same as asking for $\mathfrak{a}$ to have order greater than 2 in the ideal class group of $\mathbf{Q}(\sqrt{D})$.

Now it's time to consult tables of class numbers of quadratic fields. The first imaginary quadratic field with $h > 2$ is $\mathbf{Q}(\sqrt{-14})$, where $h = 4$. You can check that the ideal $(3, 1 - \sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$ has order 4 in the class group. (That is, the smallest power of this ideal which is principal is its 4th power.) Let's use this ideal. To have this be $(c, a - \alpha)$, take $c = 3$ and $a = 1$, and $D = -14 = a^2 + bc = 1 + 3b$, so $b = -5$. Our matrix is $\left(\begin{smallmatrix} 1 & -5 \\ 3 & -1 \end{smallmatrix}\right)$. (We took the bottom right entry to be -1 because we need A to have trace 0.) This integral matrix is not conjugate in $\mathrm{M}_2(\mathbf{Z})$ to its transpose $\left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right)$ because it corresponds to an ideal class in $\mathbf{Z}[\sqrt{-14}]$ having order greater than 2.

Of course, the statement that $\left(\begin{smallmatrix} 1 & -5 \\ 3 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right)$ are not conjugate in $\mathrm{M}_2(\mathbf{Z})$ is wholly elementary, not mentioning ideals at all, and the fact that they are not conjugate in $\mathrm{M}_2(\mathbf{Z})$ can be proved by contradiction in an elementary way. But if you follow that approach then you have absolutely no idea how the example was found or even how to find more examples. The way we went about finding the example shows a path through number theory by which many more examples can be found.

Over a field, a square matrix and its transpose are conjugate, so $\left(\begin{smallmatrix} 1 & -5 \\ 3 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right)$ are conjugate in $\mathrm{M}_2(\mathbf{Q})$. An explicit $U \in \mathrm{GL}_2(\mathbf{Q})$ satisfying $U\left(\begin{smallmatrix} 1 & -5 \\ 3 & -1 \end{smallmatrix}\right)U^{-1} = \left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right)$ is $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -5/3 \end{smallmatrix}\right)$. Darij Grinberg noticed an interesting aspect of this example when we reduce mod p. Since $\mathbf{Z}/p\mathbf{Z}$ is a field, $\left(\begin{smallmatrix} 1 & -5 \\ 3 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right)$ have to be conjugate in $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$ for every prime p. (In fact, $U \bmod p$ works as a conjugating matrix unless $p = 3$. In that case $\left(\begin{smallmatrix} 1 & -1 \\ -1 & 0 \end{smallmatrix}\right) \bmod 3$ can be used.) Therefore it is false that if two matrices in $\mathrm{M}_2(\mathbf{Z})$ are conjugate in $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$ for all primes p then they are conjugate in $\mathrm{M}_2(\mathbf{Z})$.

References

[1] C. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. **34** (1933), 313–316.

[2] M. Newman, "Integral Matrices," Academic Press, New York, 1972.

[3] O. Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math **1** (1949), 300–302.

[4] D. I. Wallace, *Conjugacy classes of hyperbolic matrices in* $\mathrm{SL}_n(\mathbf{Z})$ *and ideal classes in an order*, Trans. Amer. Math. Soc. **283** (1984), 177–184.

[2] $\mathfrak{a}\overline{\mathfrak{a}} = (c^2, 2ac, bc)$ and an ideal with generators in $\mathbf{Z}$ is principal.