Ideal Classes and Matrix Conjugation Over $\mathbb{Z}$

Michael Nelson

1 Introduction

In this presentation, we will describe a relationship between conjugacy classes of matrices with integer coefficients and $\mathcal{O}$-ideal classes of fractional $\mathcal{O}$-ideals where $\mathcal{O}$ is an order in a number field K. This presentation was inspired by Keith Conrad's expository notes [1].

Conjugacy Classes of Matrices in $\mathrm{M}_n(\mathbb{Z})$

Let A and B be matrices in $\mathrm{M}_n(\mathbb{Z})$. We say A is **conjugate** to B, denoted by $A \sim_{\mathrm{c}} B$, if there exists a $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAU^{-1} = B$. It is straightforward to check that $\sim_{\mathrm{c}}$ is an equivalence relation. We will denote by $[A]_{\mathrm{c}}$ to be the equivalence class which is represented by the matrix $A \in \mathrm{M}_n(\mathbb{Z})$. We call these equivalence classes **conjugacy classes**. We denote by $\mathrm{C}_n(\mathbb{Z})$ to be set of all conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$. Recall the characteristic polynomial of a matrix $A \in \mathrm{M}_n(\mathbb{Z})$ is defined by

$$\chi_A(T) = \det(T\mathrm{I}_n - A).$$

If $A \sim_{\mathrm{c}} B$, then there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAU^{-1} = B$, and hence

$$\begin{aligned}
\chi_B(T) &= \det(T\mathrm{I}_n - B) \\
&= \det(T\mathrm{I}_n - UAU^{-1}) \\
&= \det(U(T\mathrm{I}_n - A)U^{-1}) \\
&= \det(U)\det(T\mathrm{I}_n - A)\det(U^{-1}) \\
&= \det(T\mathrm{I}_n - A) \\
&= \chi_A(T).
\end{aligned}$$

Therefore it makes sense to assign a characteristic polynomial to a conjugacy class of matrices in $\mathrm{M}_n(\mathbb{Z})$. For any monic polynomial $f(T) \in \mathbb{Z}[T]$ of degree n, we will denote by $\mathrm{C}_n(\mathbb{Z}, f)$ to be the set of all conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial f.

Fractional $\mathcal{O}$-Ideals

Let $\mathcal{O}$ be an order in a number field K. That is, $\mathcal{O}$ is a subring of K that is finitely generated as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of K. A typical example of an order is $\mathbb{Z}[\alpha]$ in $\mathbb{Q}(\alpha)$ where α is an algebraic integer over $\mathbb{Q}$. A **fractional $\mathcal{O}$-ideal** is a nonzero finitely generated $\mathcal{O}$-module in K. Let I an J be two fractional $\mathcal{O}$-ideals. We say I and J are **equivalent**, denoted $I \sim J$, if $I = xJ$ for some $x \in K^\times$. It is straightforward to check that this is an equivalence relation. We will denote by $[I]$ to be the equivalence class which is represented by the $\mathcal{O}$-fractional ideal I. We call these equivalence classes **$\mathcal{O}$-ideal classes**. We denote by $\mathrm{Cl}(\mathcal{O})$ to be the set of all $\mathcal{O}$-ideal classes. In fact, it is easy to show that $\mathrm{Cl}(\mathcal{O})$ is none other than the set of isomorphism classes of $\mathcal{O}$-fractional ideals. That is, the relation $I \sim J$ is equivalent to saying I is isomorphic to J as $\mathcal{O}$-modules. Indeed, if $I \sim J$, then $I = xJ$ for some $x \in K^\times$. Then the multiplication by x map $\mathrm{m}_x \colon I \to J$, given by

$$\mathrm{m}_x(y) = xy$$

for all $y \in I$ is an $\mathcal{O}$-module isomorphism from I to J. Conversely, if $\varphi \colon I \to J$ is an $\mathcal{O}$-module isomorphism, then we claim that $\varphi(y)/y = \varphi(z)/z$ for all nonzero $y, z \in I$. To see this, first choose a nonzero $\gamma \in \mathcal{O}$ such that $\gamma y, \gamma z \in \mathcal{O}$ (such a choice is possible since I is a fractional $\mathcal{O}$-ideal). Then observe that

$$\begin{aligned}
\gamma\left(\frac{\varphi(y)}{y} - \frac{\varphi(z)}{z}\right) &= \gamma\left(\frac{z\varphi(y) - y\varphi(z)}{yz}\right) \\
&= \frac{\gamma z\varphi(y) - \gamma y\varphi(z)}{yz} \\
&= \frac{\varphi(\gamma z y) - \varphi(\gamma y z)}{yz} \\
&= 0.
\end{aligned}$$

This implies $\varphi(y)/y = \varphi(z)/z$ since $\mathcal{O}$ is an integral domain. Now write $x = \varphi(y)/y$ for some nonzero $y \in I$. Then for any nonzero $z \in I$, we have

$$\begin{aligned}
\varphi(z) &= \frac{\varphi(z)}{z}z \\
&= \frac{\varphi(y)}{y}z \\
&= xz \\
&= \mathrm{m}_x(z),
\end{aligned}$$

and since clearly $\varphi(0) = \mathrm{m}_x(0)$, we see that $\varphi = \mathrm{m}_x$. Thus $I \sim J$.

Main Theorem

Theorem 1.1. *Let $f(T) \in \mathbb{Z}[T]$ be a monic irreducible polynomial of degree n and let α be a root of $f(T)$. Then we have a bijection*

$$\mathrm{C}_n(\mathbb{Z}, f) \cong \mathrm{Cl}(\mathbb{Z}[\alpha]).$$

Proof. We define $\Psi \colon \mathrm{Cl}(\mathbb{Z}[\alpha]) \to \mathrm{C}_n(\mathbb{Z}, f)$ as follows: let $\mathfrak{a}$ be a $\mathbb{Z}[\alpha]$-fractional ideal. From the structure of finitely-generated torsion-free modules over $\mathbb{Z}$, we know that $\mathfrak{a}$ is a finitely-generated free $\mathbb{Z}$-module of rank n. Choose an ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, say $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$. Let $\mathrm{m}_\alpha \colon \mathfrak{a} \to \mathfrak{a}$ be the multiplication by α map, given by

$$\mathrm{m}_\alpha(x) = \alpha x$$

for all $x \in \mathfrak{a}$ and let $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} \in \mathrm{M}_n(\mathbb{Z})$ denote the matrix representation of m_α with respect to the basis $\mathbf{a}$. That is, the (i, j)'th entry in $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$ is given by $a_{ji} \in \mathbb{Z}$ where

$$\mathrm{m}_\alpha(\alpha_i) = \sum_{j=1}^{n} a_{ji}\alpha_j.$$

If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is another ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, then the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ is given by $[1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}} \in \mathrm{GL}_n(\mathbb{Z})$, and we have

$$\begin{aligned}
[1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}\left([1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}\right)^{-1} &= [1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}[1_{\mathfrak{a}}]_{\mathbf{a}}^{\mathbf{a}'} \\
&= [1_{\mathfrak{a}} \circ \mathrm{m}_\alpha \circ 1_{\mathfrak{a}}]_{\mathbf{a}}^{\mathbf{a}}. \\
&= [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}
\end{aligned}$$

Thus changing the basis from $\mathbf{a}$ to $\mathbf{a}'$ corresponds to conjugating the matrix $[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}$ to $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$.

We are now ready to define Ψ. We set

$$\Psi([\mathfrak{a}]) = [[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}]_{\mathrm{c}}. \tag{1}$$

We must check that (1) is in fact well-defined. Our construction of Ψ involved two choices. One choice that we made was in the choice of a basis for $\mathfrak{a}$ as free $\mathbb{Z}$-module (where we chose $\mathbf{a}$). By what was mentioned above, changing this basis to another basis would result in a matrix which is conjugate to $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$ and hence would result in the same conjugacy class $[[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}]_{\mathrm{c}}$. The other choice that we made was in the choice of a representative of the $\mathbb{Z}[\alpha]$-ideal class $[\mathfrak{a}]$ (where we chose $\mathfrak{a}$) So let $\mathfrak{b}$ be another another coset representative of the coset $[\mathfrak{a}]$, so $\mathfrak{b} \sim \mathfrak{a}$. Choose $x \in \mathbb{Q}(\alpha)^\times$ such that $\mathfrak{b} = x\mathfrak{a}$. Then observe that $x\mathbf{a}$ is a basis for $\mathfrak{b}$ as a free $\mathbb{Z}$-module! Indeed, it clearly spans $\mathfrak{b}$ as a $\mathbb{Z}$-module since $\mathfrak{b} = x\mathfrak{a}$. Also, it is $\mathbb{Z}$-linearly independent since it is $\mathbb{Q}$-linearly independent (since multiplication by x is a $\mathbb{Q}$-isomorphism). Furthermore, it is easy to check that since $\mathrm{m}_x\mathrm{m}_\alpha = \mathrm{m}_\alpha\mathrm{m}_x$, we have

$$\begin{aligned}
[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} &= [\mathrm{m}_\alpha]_{x\mathbf{a}}^{x\mathbf{a}} \\
&= [\mathrm{m}_\alpha]_{\mathbf{b}}^{\mathbf{b}}.
\end{aligned}$$

Thus (1) is well-defined.

Now we show that Ψ is injective. Let $[\mathfrak{a}]$ and $[\mathfrak{a}']$ be two fractional $\mathcal{O}$-ideals and let $\mathbf{a}$ and $\mathbf{a}'$ be ordered bases for $\mathfrak{a}$ and $\mathfrak{a}'$ as free $\mathbb{Z}$-modules respectively. Suppose $\Psi([\mathfrak{a}]) = \Psi([\mathfrak{a}'])$, that is suppose

$$U[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}U^{-1} = [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}$$

for some $U \in \mathrm{GL}_n(\mathbb{Z})$. Let $[\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. That is $[\cdot]_{\mathbf{a}}$ is the unique $\mathbb{Z}$-linear map which sends α_i to e_i for all $1 \le i \le n$, where $\mathbf{e} = (e_1, \dots, e_n)$ is the standard ordered column basis for $\mathbb{Z}^n$ as a free $\mathbb{Z}$-module. Similarly, let $[\cdot]_{\mathbf{a}'} \colon \mathfrak{a}' \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. Then observe that $[\cdot]_{\mathbf{a}'}^{-1}U[\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathfrak{a}'$ gives us an isomorphism of $\mathfrak{a}$ and $\mathfrak{a}'$ as $\mathbb{Z}$-modules. In fact, this is a $\mathbb{Z}[\alpha]$-isomorphism since it commutes with m_α. Indeed, we have

$$\begin{aligned}
[\cdot]_{\mathbf{a}'}^{-1}U[\cdot]_{\mathbf{a}}\mathrm{m}_\alpha &= [\cdot]_{\mathbf{a}'}^{-1}U[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}[\cdot]_{\mathbf{a}} \\
&= [\cdot]_{\mathbf{a}'}^{-1}[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}U[\cdot]_{\mathbf{a}} \\
&= \mathrm{m}_\alpha[\cdot]_{\mathbf{a}'}^{-1}U[\cdot]_{\mathbf{a}}.
\end{aligned}$$

Isomorphic fractional $\mathbb{Z}[\alpha]$-ideals are scalar multiples of each other, so $\mathfrak{a}' = x\mathfrak{a}$ for some $x \in \mathbb{Q}(\alpha)^\times$. In particular, $[\mathfrak{a}] = [\mathfrak{a}']$. Thus Ψ is injective.

Now let us show that Ψ is surjective. Let $A = (a_{ij})$ be in $\mathrm{M}_n(\mathbb{Z})$ such that $\chi_A(T) = f(T)$. We will find a $\mathbb{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ and a ordered basis $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ of $\mathfrak{a}$ as a free $\mathbb{Z}$-module such that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. First, we make $\mathbb{Q}^n$ into a $\mathbb{Q}(\alpha)$-vector space as follows: Let $x \in \mathbb{Q}(\alpha)$ and let $v \in \mathbb{Q}^n$. Choose $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$ (such a choice is possible since $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$). We define scalar multiplication of $\mathbb{Q}(\alpha)$ on $\mathbb{Q}^n$ by

$$x \cdot v = g(A)v. \tag{2}$$

We need to check that (2) is well-defined. In our construction of (2), we made a choice, namely $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$, so suppose $h(T) \in \mathbb{Q}[T]$ such that $h(\alpha) = x$. Then $(g - h)(\alpha) = 0$ and this implies $f \mid (g - h)$ (since f is the minimal polynomial of α over $\mathbb{Q}$ since it is monic and irreducible with root α) and therefore $g(A) = h(A)$ as matrices, so $g(A)v = h(A)v$ for all $v \in \mathbb{Q}^n$. Thus (2) is well-defined. It is straightforward to check that (2) gives $\mathbb{Q}^n$ a $\mathbb{Q}(\alpha)$-vector space structure. By restricting scalars, (2) also gives

$\mathbb{Q}^n$ a $\mathbb{Z}[\alpha]$-module structure. In fact, if $v \in \mathbb{Z}^n$, then $\alpha \cdot v = Av$ is in $\mathbb{Z}^n$ since A has integral entries, so $\mathbb{Z}^n$ is a $\mathbb{Z}[\alpha]$-submodule of $\mathbb{Q}^n$. Treating $\mathbb{Q}^n$ as both a $\mathbb{Q}$-vector space and as a $\mathbb{Q}(\alpha)$-vector space, we have

$$\begin{aligned} n &= \dim_{\mathbb{Q}}(\mathbb{Q}^n) \\ &= [\mathbb{Q}(\alpha):\mathbb{Q}] \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \\ &= n \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n), \end{aligned}$$

so $\mathbb{Q}^n$ is 1-dimensional as a $\mathbb{Q}(\alpha)$-vector space. In particular, this means that for any nonzero $v_0 \in \mathbb{Q}^n$, the $\mathbb{Q}(\alpha)$-linear map $\varphi_{v_0} \colon \mathbb{Q}(\alpha) \to \mathbb{Q}^n$ given by

$$\varphi_{v_0}(x) = x \cdot v_0$$

for all $x \in \mathbb{Q}(\alpha)$ is an isomorphism of 1-dimensional $\mathbb{Q}(\alpha)$-vector spaces. Thus, letting $\mathbf{e} = (e_1, \dots, e_n)$ denote the standard ordered column basis for $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space, there exists unique $\alpha_i \in \mathbb{Q}(\alpha)$ such that $\varphi_{v_0}(\alpha_i) = e_i$ for all $1 \le i \le n$. In particular, $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ is an ordered basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space. Let

$$\mathfrak{a} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i.$$

Observe that $\mathfrak{a}$ is a $\mathbb{Z}[\alpha]$-fractional ideal. Indeed, it suffices to show that $\alpha\alpha_i \in \mathfrak{a}$ for all $1 \le i \le n$, and this follows from the fact that

$$\begin{aligned} \varphi_{v_0}\left(\alpha\alpha_i - \sum_{j=1}^n a_{ji}\alpha_i\right) &= \alpha \cdot \varphi_{v_0}(\alpha_i) - \sum_{j=1}^n a_{ji}\varphi_{v_0}(\alpha_i) \\ &= \alpha \cdot e_i - \sum_{j=1}^n a_{ji} e_i \\ &= Ae_i - Ae_i \\ &= 0, \end{aligned}$$

which implies

$$\alpha\alpha_i = \sum_{j=1}^n a_{ji}\alpha_i \tag{3}$$

since φ_{v_0} is injective. In fact, (3) also shows that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. So we have realized A as a matrix representation for m_α on a fractional $\mathbb{Z}[\alpha]$-ideal $\mathfrak{a}$. Thus Ψ is onto. $\square$

Example

Example 1.1. Let $f(T) = T^2 + 5$. We will count $\#\mathrm{C}_2(\mathbb{Z}, f)$ and we will find a coset representative for each conjugacy class in $\mathrm{C}_2(\mathbb{Z}, f)$. Note that f is a monic irreducible polynomial over $\mathbb{Z}$ and $\sqrt{-5}$ is a root of f. The ring $\mathbb{Z}[\sqrt{-5}]$ has class number 2, and so by Theorem (2.1), we see that $\#\mathrm{C}_2(\mathbb{Z}, f) = 2$. The ideal classes in $\mathbb{Z}[\sqrt{-5}]$ can be represented by $\mathbb{Z}[\sqrt{-5}] = \langle 1 \rangle$ and $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-5} \rangle$. An ordered basis for $\mathbb{Z}[\sqrt{-5}]$ is given by $\mathbf{a}_1 = (1, \sqrt{-5})$ and an ordered basis for $\mathfrak{p}_2$ is given by $\mathbf{a}_2 = (2, 1 + \sqrt{-5})$. We calculate

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

Therefore $[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_1}^{\mathbf{a}_1} = \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$. Similarly, we calculate

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

Therefore $[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_2}^{\mathbf{a}_2} = \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. Thus if $A \in \mathrm{M}_2(\mathbb{Z})$ has characteristic polynomial $f(T)$, then $A \sim_{\mathrm{c}} \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$ or $A \sim_{\mathrm{c}} \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. Now let $\mathfrak{p}_7 = \langle 7, 3 + \sqrt{-5} \rangle$. Then $\mathfrak{p}_7 \sim \mathfrak{p}_2$ since

$$\mathfrak{p}_7 = \left(\frac{3 - \sqrt{-5}}{2}\right) \mathfrak{p}_2$$

An ordered basis for $\mathfrak{p}_7$ is given by $\mathbf{a}_7 = (7, 3 - \sqrt{-5})$. By a straightforward calculation, we have $[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_7}^{\mathbf{a}_7} = \left(\begin{smallmatrix} 3 & 2 \\ -7 & -3 \end{smallmatrix}\right)$. Thus $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right) \sim_{\mathrm{c}} \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. To find the matrix which conjugates $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$ we first change the ordered $\mathbb{Z}$-basis $\mathbf{a}_2$ of $\mathfrak{p}_2$ to the ordered $\mathbb{Z}$-basis $\mathbf{a}_2' = (2, 3 + \sqrt{-5})$. The change of basis matrix from $\mathbf{a}_2$ to $\mathbf{a}_2'$ is given by $[1_{\mathfrak{p}_2}]_{\mathbf{a}_2'}^{\mathbf{a}_2} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Similarly, we change the ordered $\mathbb{Z}$-basis $\mathbf{a}_7$ of $\mathfrak{p}_7$ to the ordered $\mathbb{Z}$-basis $\mathbf{a}_7' = (3 - \sqrt{-5}, 7)$. The change of basis matrix from $\mathbf{a}_7$ to $\mathbf{a}_7'$ is given by $[1_{\mathfrak{p}_7}]_{\mathbf{a}_7'}^{\mathbf{a}_7} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Next we observe that

$$\begin{aligned} \left(\frac{3 - \sqrt{-5}}{2}\right) \mathbf{a}_2' &= \left(\frac{3 - \sqrt{-5}}{2}\right) \left(2, 3 + \sqrt{-5}\right) \\ &= (3 - \sqrt{-5}, 7) \\ &= \mathbf{a}_7'. \end{aligned}$$

Therefore we have

$$\begin{aligned}
\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix} &= [\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_2}^{\mathbf{a}_2} \\
&= [1_{\mathfrak{p}_2}]_{\mathbf{a}_2'}^{\mathbf{a}_2}[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_2'}^{\mathbf{a}_2'}[1_{\mathfrak{p}_2}]_{\mathbf{a}_2}^{\mathbf{a}_2'} \\
&= [1_{\mathfrak{p}_2}]_{\mathbf{a}_2'}^{\mathbf{a}_2}[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_7'}^{\mathbf{a}_7'}[1_{\mathfrak{p}_2}]_{\mathbf{a}_2}^{\mathbf{a}_2'} \\
&= [1_{\mathfrak{p}_2}]_{\mathbf{a}_2'}^{\mathbf{a}_2}[1_{\mathfrak{p}_7}]_{\mathbf{a}_7}^{\mathbf{a}_7'}[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_7}^{\mathbf{a}_7}[1_{\mathfrak{p}_7}]_{\mathbf{a}_7'}^{\mathbf{a}_7}[1_{\mathfrak{p}_2}]_{\mathbf{a}_2}^{\mathbf{a}_2'} \\
&= \left([1_{\mathfrak{p}_2}]_{\mathbf{a}_2'}^{\mathbf{a}_2}[1_{\mathfrak{p}_7}]_{\mathbf{a}_7}^{\mathbf{a}_7'}\right)[\mathrm{m}_{\sqrt{-5}}]_{\mathbf{a}_7}^{\mathbf{a}_7}\left([1_{\mathfrak{p}_7}]_{\mathbf{a}_2'}^{\mathbf{a}_2}[1_{\mathfrak{p}_2}]_{\mathbf{a}_7}^{\mathbf{a}_7'}\right)^{-1}. \\
&= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)\begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)^{-1} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1}.
\end{aligned}$$

The table below summarizes our calculations

Fractional Ideal	$[\mathrm{m}_{\sqrt{-5}}]$	Ordered $\mathbb{Z}$-Basis	$\sim$
$\langle 1\rangle = \mathbb{Z}[\sqrt{-5}]$	$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$	$\mathbf{a}_1 = (1, \sqrt{-5})$	$\langle 1\rangle = \langle 1\rangle$
$\mathfrak{p}_2 = \langle 2, 1+\sqrt{-5}\rangle$	$\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}$	$\mathbf{a}_2 = (2, 1+\sqrt{-5})$	$\mathfrak{p}_2 = \left(\frac{2}{3-\sqrt{-5}}\right)\mathfrak{p}_7$
$\mathfrak{p}_7 = \langle 7, 3-\sqrt{-5}\rangle$	$\begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix}$	$\mathbf{a}_7 = (7, 3+\sqrt{-5})$	$\mathfrak{p}_7 = \left(\frac{3-\sqrt{-5}}{2}\right)\mathfrak{p}_2$

2 Generalizations

We now would like to generalize our results in Theorem (2.1). Let us consider the following example. Let $f(T) = T^2+2$. Then f is monic irreducible polynomial over $\mathbb{Q}$ and $\sqrt{-2}$ is a root of f. We compute a table similar to the one in Example (1.1):

Fractional Ideal	$[\mathrm{m}_{\sqrt{-2}}]$	Ordered $\mathbb{Z}$-Basis
$\mathbb{Z}[\sqrt{-2}]$	$\begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$	$\mathbf{a} = \{1, \sqrt{-2}\}$
$\mathbb{Z}[\sqrt{-2}]$	$\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$	$\overline{\mathbf{a}} = (1, -\sqrt{-2})$

Now $\mathbb{Z}[\sqrt{-2}]$ has class number 1, so Theorem (2.1) tells us that the matrices $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ are conjugate. However, more specifically, when we say conjugate, we mean they $\mathrm{GL}_2(\mathbb{Z})$-conjugate. In fact, the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ conjugates $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$. Indeed, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

However note that $\det\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -1$, and so $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \notin \mathrm{SL}_2(\mathbb{Z})$. It's natural wonder if $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ are $\mathrm{SL}_2(\mathbb{Z})$-conjugate. It turns out that they are not even conjugate by an element of $\mathrm{SL}_2(\mathbb{Q})$. However, they are $\mathrm{SL}_2(\mathbb{Z}[\mathrm{i}])$-conjugate. The matrix $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}[i])$ conjugates $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$. Indeed, we have

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

$\mathrm{SL}_n(\mathbb{Z})$-Conjugacy Classes of Matrices in $\mathrm{M}_n(\mathbb{Z})$

To improve Theorem (2.1), we introduce the following notation. We denote by $\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ to be the set of all $\mathrm{SL}_n(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$. Similarly, if $f(T) \in \mathbb{Z}[T]$ is a nonzero monic polynomial, then we denote by $\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ to be the set of all $\mathrm{SL}_n(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial f.

Orientations

Let V be a nonzero $\mathbb{R}$-vector space with n and let $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ be an ordered basis of V. This gives rise to a nonzero vector

$$\wedge(\mathbf{a}) = \alpha_1 \wedge \cdots \wedge \alpha_n \in \Lambda^n(V)$$

in the line $\Lambda^n(V)$. If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is a second ordered basis, then $\wedge(\mathbf{a}')$ is another nonzero vector in the same line $\Lambda^n(V)$, so $\wedge(\mathbf{a}') = c \wedge (\mathbf{a})$ for a unique $c \in \mathbb{R}^\times$. Concretely, if $T_{\mathbf{a},\mathbf{a}'} \colon V \to V$ is the unique linear automorphism satisfying $\alpha_i' = T(\alpha_i)$ for all i (it is the "change of basis matrix" from $\mathbf{a}'$-coordinates to $\mathbf{a}$-coordinates), then $c = \det T_{\mathbf{a},\mathbf{a}'}$ and $1/c = \det T_{\mathbf{a}',\mathbf{a}}^{-1}$. Hence $c > 0$ if and only if $\wedge(\mathbf{a})$ and $\wedge(\mathbf{a}')$ lie in the same connected component of $\Lambda^n(V)\backslash\{0\}$.

Definition 2.1. An **orientation** μ on V is a choice of connected component of $\Lambda^n(V)\backslash\{0\}$, called the **positive component** with respect to μ. An **oriented vector space** is a nonzero vector space V equipped with a choice of orientation μ.

Definition 2.2. Let V be a $\mathbb{Q}$-vector space and let $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ and $\mathbf{a}' = (\alpha_1', \dots, \alpha_n)$ be two ordered bases of V. We say $\mathbf{a}$ and $\mathbf{a}'$ are **similarly oriented**, denoted $\mathbf{a} \sim_+ \mathbf{a}'$, if the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ has positive determinant, that is if

$$\det[1_V]^{\mathbf{a}}_{\mathbf{a}'} > 0.$$

It is straightforward to check that $\sim_+$ is an equivalence relation. Indeed, reflexivity and symmetry of $\sim_+$ are clear. For transitivity, suppose $\mathbf{a} \sim_+ \mathbf{a}'$ and $\mathbf{a}' \sim_+ \mathbf{a}''$. Then

$$\begin{aligned}\det[1_V]^{\mathbf{a}}_{\mathbf{a}''} &= \det\left([1_V]^{\mathbf{a}}_{\mathbf{a}'}[1_V]^{\mathbf{a}'}_{\mathbf{a}''}\right)\\ &= \det[1_V]^{\mathbf{a}}_{\mathbf{a}'}\det[1_V]^{\mathbf{a}'}_{\mathbf{a}''}\\ &> 0\end{aligned}$$

implies $\mathbf{a} \sim_+ \mathbf{a}''$. We shall denote by $[\mathbf{a}]_o$ to by the $\sim_+$-equivalence class which is represented by the ordered basis $\mathbf{a}$. Clearly, there are just two $\sim_o$-equivalence classes. An oriented $\mathbb{Q}$-vector space (V, μ_+) is a $\mathbb{Q}$-vector space V equipped with the choice of a $\sim_o$-equivalence class, which we shall call the **positive orientation**. We shall also denote this equivalence class by μ_+. In this case, the other $\sim_o$-equivalence class will be denoted by μ_-. Note that if $[\mathbf{a}]_o = \mu_+$, then $[-\mathbf{a}]_o = \mu_-$. If an ordered basis represents μ_+, then we say it is **positively oriented**. If an ordered basis represents μ_-, then we say it is **negatively oriented**. If (V, μ_+) and (W, ν_+) are two oriented n-dimensional $\mathbb{Q}$-vector spaces and $T\colon V \to W$ is a linear isomorphism, then we say T is **orientation-preserving** if $\det[T]^{\mathbf{b}}_{\mathbf{a}} > 0$, where $\mathbf{a}$ represents μ_+ and $\mathbf{b}$ represents ν_+.

Generalized Theorem

Theorem 2.1. *Let $f(T) \in \mathbb{Z}[T]$ be a monic irreducible polynomial of degree n and let α be a root of $f(T)$. Then we have a bijection*

$$\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f) \cong \mathrm{Cl}_+(\mathbb{Z}[\alpha]).$$

Proof. We define $\Psi\colon \mathrm{Cl}_+(\mathbb{Z}[\alpha]) \to \mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ as follows: let $\mathfrak{a}$ be a $\mathbb{Z}[\alpha]$-fractional ideal. From the structure of finitely-generated torsion-free modules over $\mathbb{Z}$, we know that $\mathfrak{a}$ is a finitely-generated free $\mathbb{Z}$-module of rank n. Choose a positive ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, say $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$. Let $\mathrm{m}_\alpha\colon \mathfrak{a} \to \mathfrak{a}$ be the multiplication by α map and let $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}} \in \mathrm{M}_n(\mathbb{Z})$ denote the matrix representation of m_α with respect to $\mathbf{a}$. If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is another positive ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, then the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ is given by $[1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'} \in \mathrm{SL}_n(\mathbb{Z})$ since both $\mathbf{a}$ and $\mathbf{a}'$ are positive, and hence $\det[1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'} > 0$ which implies $\det[1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'} = 1$. Furthermore, we have

$$\begin{aligned}[1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'}[\mathrm{m}_\alpha]^{\mathbf{a}'}_{\mathbf{a}'}\left([1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'}\right)^{-1} &= [1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}'}[\mathrm{m}_\alpha]^{\mathbf{a}'}_{\mathbf{a}'}[1_\mathfrak{a}]^{\mathbf{a}'}_{\mathbf{a}}\\ &= [1_\mathfrak{a} \circ \mathrm{m}_\alpha \circ 1_\mathfrak{a}]^{\mathbf{a}}_{\mathbf{a}}.\\ &= [\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}.\end{aligned}$$

Thus changing the positive basis from $\mathbf{a}$ to $\mathbf{a}'$ corresponds to a $\mathrm{SL}_n(\mathbb{Z})$-conjugate matrix of $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}$.

We are now ready to define Ψ. We set

$$\Psi([\mathfrak{a}]) = [[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}]_{\mathrm{c}}. \tag{4}$$

We must check that (1) is in fact well-defined. Our construction of Ψ involved two choices. One choice that we made was in the choice of a positive orderd basis for $\mathfrak{a}$ as free $\mathbb{Z}$-module (where we chose $\mathbf{a}$). By what was mentioned above, changing this basis to another basis would result in a matrix which is $\mathrm{SL}_n(\mathbb{Z})$-conjugate to $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}$ and hence would result in the same conjugacy class $[[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}]_{\mathrm{c}}$. The other choice that we made was in the choice of a representative of the $\mathbb{Z}[\alpha]$-ideal class $[\mathfrak{a}]$ (where we chose $\mathfrak{a}$) So let $\mathfrak{b}$ be another another coset representative of the coset $[\mathfrak{a}]$, so $\mathfrak{b} \sim \mathfrak{a}$. Choose $x \in \mathbb{Q}(\alpha)^\times$ such $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x) > 0$ and $\mathfrak{b} = x\mathfrak{a}$. Then observe that $x\mathbf{a}$ is a positively oriented ordered basis for $\mathfrak{b}$ as a free $\mathbb{Z}$-module! Indeed, it clearly spans $\mathfrak{b}$ as a $\mathbb{Z}$-module since $\mathfrak{b} = x\mathfrak{a}$. Also, it is $\mathbb{Z}$-linearly independent since it is $\mathbb{Q}$-linearly independent (since multiplication by x is a $\mathbb{Q}$-isomorphism). It is also positively oriented precisely because $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x) > 0$. Furthermore, it is easy to check that since $\mathrm{m}_x\mathrm{m}_\alpha = \mathrm{m}_\alpha\mathrm{m}_x$, we have

$$\begin{aligned}[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}} &= [\mathrm{m}_\alpha]^{x\mathbf{a}}_{x\mathbf{a}}\\ &= [\mathrm{m}_\alpha]^{\mathbf{b}}_{\mathbf{b}}.\end{aligned}$$

Thus (1) is well-defined.

Now we show that Ψ is injective. Let $[\mathfrak{a}]$ and $[\mathfrak{a}']$ be two fractional $\mathcal{O}$-ideals and let $\mathbf{a}$ and $\mathbf{a}'$ be ordered bases for $\mathfrak{a}$ and $\mathfrak{a}'$ as free $\mathbb{Z}$-modules respectively. Suppose $\Psi([\mathfrak{a}]) = \Psi([\mathfrak{a}'])$, that is suppose

$$U[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}U^{-1} = [\mathrm{m}_\alpha]^{\mathbf{a}'}_{\mathbf{a}'}$$

for some $U \in \mathrm{SL}_n(\mathbb{Z})$. Let $[\cdot]_{\mathbf{a}}\colon \mathfrak{a} \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. That is $[\cdot]_{\mathbf{a}}$ is the unique $\mathbb{Z}$-linear map which sends α_i to e_i for all $1 \leq i \leq n$, where $\mathbf{e} = (e_1, \dots, e_n)$ is the standard ordered column basis for $\mathbb{Z}^n$ as a free $\mathbb{Z}$-module. Similarly, let $[\cdot]_{\mathbf{a}'}\colon \mathfrak{a}' \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. Then observe that $[\cdot]^{-1}_{\mathbf{a}'}U[\cdot]_{\mathbf{a}}\colon \mathfrak{a} \to \mathfrak{a}'$ gives us an isomorphism of $\mathfrak{a}$ and $\mathfrak{a}'$ as $\mathbb{Z}$-modules. In fact, this is a $\mathbb{Z}[\alpha]$-isomorphism since it commutes with m_α. Indeed, we have

$$\sigma[\cdot]^{-1}_{\mathbf{a}'}U[\cdot]_{\mathbf{a}}\sigma^{-1} = [\cdot]^{-1}_{\sigma\mathbf{a}'}[\sigma]^{\sigma\mathbf{a}'}_{\mathbf{a}'}U[\sigma^{-1}]^{\mathbf{a}}_{\sigma\mathbf{a}}[\cdot]_{\sigma\mathbf{a}}$$

$$
\begin{aligned}
[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \mathrm{m}_\alpha &= [\cdot]_{\mathbf{a}'}^{-1} U [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} [\cdot]_{\mathbf{a}} \\
&= [\cdot]_{\mathbf{a}'}^{-1} [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'} U [\cdot]_{\mathbf{a}} \\
&= \mathrm{m}_\alpha [\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}}.
\end{aligned}
$$

Isomorphic fractional $\mathbb{Z}[\alpha]$-ideals are scalar multiples of each other, so $\mathfrak{a}' = x\mathfrak{a}$ for some $x \in \mathbb{Q}(\alpha)^\times$. In particular, $[\mathfrak{a}] = [\mathfrak{a}']$. Thus Ψ is injective.

Now let us show that Ψ is surjective. Let $A = (a_{ij})$ be in $\mathrm{M}_n(\mathbb{Z})$ such that $\chi_A(T) = f(T)$. We will find a $\mathbb{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ and a ordered basis $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ of $\mathfrak{a}$ as a free $\mathbb{Z}$-module such that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. First, we make $\mathbb{Q}^n$ into a $\mathbb{Q}(\alpha)$-vector space as follows: Let $x \in \mathbb{Q}(\alpha)$ and let $v \in \mathbb{Q}^n$. Choose $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$ (such a choice is possible since $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$). We define scalar multiplication of $\mathbb{Q}(\alpha)$ on $\mathbb{Q}^n$ by

$$
x \cdot v = g(A)v. \tag{5}
$$

We need to check that (2) is well-defined. In our construction of (2), we made a choice, namely $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$, so suppose $h(T) \in \mathbb{Q}[T]$ such that $h(\alpha) = x$. Then $(g - h)(\alpha) = 0$ and this implies $f \mid (g - h)$ (since f is the minimal polynomial of α over $\mathbb{Q}$ since it is monic and irreducible with root α) and therefore $g(A) = h(A)$ as matrices, so $g(A)v = h(A)v$ for all $v \in \mathbb{Q}^n$. Thus (2) is well-defined. It is straightforward to check that (2) gives $\mathbb{Q}^n$ a $\mathbb{Q}(\alpha)$-vector space structure. By restricting scalars, (2) also gives $\mathbb{Q}^n$ a $\mathbb{Z}[\alpha]$-module structure. In fact, if $v \in \mathbb{Z}^n$, then $\alpha \cdot v = Av$ is in $\mathbb{Z}^n$ since A has integral entries, so $\mathbb{Z}^n$ is a $\mathbb{Z}[\alpha]$-submodule of $\mathbb{Q}^n$. Treating $\mathbb{Q}^n$ as both a $\mathbb{Q}$-vector space and as a $\mathbb{Q}(\alpha)$-vector space, we have

$$
\begin{aligned}
n &= \dim_{\mathbb{Q}}(\mathbb{Q}^n) \\
&= [\mathbb{Q}(\alpha) : \mathbb{Q}] \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \\
&= n \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n),
\end{aligned}
$$

so $\mathbb{Q}^n$ is 1-dimensional as a $\mathbb{Q}(\alpha)$-vector space. In particular, this means that for any nonzero $v_0 \in \mathbb{Q}^n$, the $\mathbb{Q}(\alpha)$-linear map $\varphi_{v_0} \colon \mathbb{Q}(\alpha) \to \mathbb{Q}^n$ given by

$$
\varphi_{v_0}(x) = x \cdot v_0
$$

for all $x \in \mathbb{Q}(\alpha)$ is an isomorphism of 1-dimensional $\mathbb{Q}(\alpha)$-vector spaces. Thus, letting $\mathbf{e} = (e_1, \ldots, e_n)$ denote the standard ordered column basis for $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space, there exists unique $\alpha_i \in \mathbb{Q}(\alpha)$ such that $\varphi_{v_0}(\alpha_i) = e_i$ for all $1 \leq i \leq n$. In particular, $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ is an ordered basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space. Let

$$
\mathfrak{a} = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i.
$$

Observe that $\mathfrak{a}$ is a $\mathbb{Z}[\alpha]$-fractional ideal. Indeed, it suffices to show that $\alpha\alpha_i \in \mathfrak{a}$ for all $1 \leq i \leq n$, and this follows from the fact that

$$
\begin{aligned}
\varphi_{v_0}\left(\alpha\alpha_i - \sum_{j=1}^{n} a_{ji}\alpha_i\right) &= \alpha \cdot \varphi_{v_0}(\alpha_i) - \sum_{j=1}^{n} a_{ji}\varphi_{v_0}(\alpha_i) \\
&= \alpha \cdot e_i - \sum_{j=1}^{n} a_{ji}e_i \\
&= Ae_i - Ae_i \\
&= 0,
\end{aligned}
$$

which implies

$$
\alpha\alpha_i = \sum_{j=1}^{n} a_{ji}\alpha_i \tag{6}
$$

since φ_{v_0} is injective. In fact, (3) also shows that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. So we have realized A as a matrix representation for m_α on a fractional $\mathbb{Z}[\alpha]$-ideal $\mathfrak{a}$. Thus Ψ is onto. $\square$

3 Conclusion

References

[1] Keith Conrad, Expository Notes on Ideal Class and Matrix Conjugation