Math 361

March 22, 2023

Quiz

1. What is a Dedekind domain?
2. Why do we care?

Today

- Smith normal form

Motivation

Important concept. The norm of a nonzero ideal:
$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$.

Motivation

Important concept. The norm of a nonzero ideal:
$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathfrak{O}_K & \longrightarrow & \mathfrak{O}_K/\mathfrak{a} & \longrightarrow & 0 \\
 & & g \big\downarrow \wr & & f \big\downarrow \wr & & \big\downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n/\operatorname{im}(M) & \longrightarrow & 0,
\end{array}$$

Motivation

Important concept. The norm of a nonzero ideal:
$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathfrak{O}_K & \longrightarrow & \mathfrak{O}_K/\mathfrak{a} & \longrightarrow & 0 \\
 & & {\scriptstyle g}\downarrow\wr & & {\scriptstyle f}\downarrow\wr & & \vdots & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n/\operatorname{im}(M) & \longrightarrow & 0,
\end{array}
$$

The *Smith normal form* of the matrix M determines the structure of $\mathfrak{O}_K/\mathfrak{a}$.

Cokernel of an integer matrix

Let M be an $m \times n$ integer matrix.

Cokernel of an integer matrix

Let M be an $m \times n$ integer matrix.

Definition. The *cokernel* of M is

$$\operatorname{cok}(M) = \mathbb{Z}^m / \operatorname{im}(M).$$

Cokernel of an integer matrix

Let M be an $m \times n$ integer matrix.

Definition. The *cokernel* of M is

$$\operatorname{cok}(M) = \mathbb{Z}^m / \operatorname{im}(M).$$

- We have an exact sequence

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \to \operatorname{cok}(M) \to 0.$$

Cokernel of an integer matrix

Let M be an $m \times n$ integer matrix.

Definition. The *cokernel* of M is

$$\mathsf{cok}(M) = \mathbb{Z}^m / \operatorname{im}(M).$$

- We have an exact sequence

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \to \mathsf{cok}(M) \to 0.$$

- $\operatorname{im}(M) = \mathrm{colspace}_{\mathbb{Z}}(M)$.

Cokernel of an integer matrix

Examples.

- $M = [5]$,

Cokernel of an integer matrix

Examples.

- $M = [5]$, $\mathrm{cok}(M) = \mathbb{Z}/5\mathbb{Z}$.

Cokernel of an integer matrix

Examples.

- $M = [5]$, $\mathrm{cok}(M) = \mathbb{Z}/5\mathbb{Z}$.
- $M = \mathrm{diag}(2, 3)$, a 2×2 diagonal matrix.

Cokernel of an integer matrix

Examples.

- $M = [5]$, $\mathrm{cok}(M) = \mathbb{Z}/5\mathbb{Z}$.
- $M = \mathrm{diag}(2, 3)$, a 2×2 diagonal matrix. Then

$$\mathrm{cok}(M) = \mathbb{Z}^2 / \operatorname{Span}\left\{ \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right\} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

$$(a, b) \mapsto (a \bmod 2, b \bmod 3).$$

Cokernel of an integer matrix

Examples.

- $M = [5]$, $\text{cok}(M) = \mathbb{Z}/5\mathbb{Z}$.
- $M = \text{diag}(2, 3)$, a 2×2 diagonal matrix. Then

$$\text{cok}(M) = \mathbb{Z}^2 / \operatorname{Span}\left\{ \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right\} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

$$(a, b) \mapsto (a \bmod 2, b \bmod 3).$$

- Let $M = \text{diag}(0, 0, 1, 2, 3)$. Then

$$\text{cok}(M) \simeq \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}0\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

$$(a, b, c, d, e) \mapsto (a, b, d, e).$$

Integer row and column operations

Definition. The *integer row (resp., column) operations* on an integer matrix consist of the following:

1. swapping two rows (resp., columns);
2. negating a row (resp., column);
3. adding one row (resp., column) to a different row (resp., column).

Diagonalization

Claim. By performing integer row and column operations, the matrix M can be transformed into a diagonal matrix D,
i.e., $D_{ij} = 0$ for $i \neq j$.

Diagonalization

Claim. By performing integer row and column operations, the matrix M can be transformed into a diagonal matrix D, i.e., $D_{ij} = 0$ for $i \neq j$.

Start with the the identity matrix I_m and perform all of the same row operations on I_m as used in the reduction of M to D to create a matrix P.

Diagonalization

Claim. By performing integer row and column operations, the matrix M can be transformed into a diagonal matrix D, i.e., $D_{ij} = 0$ for $i \neq j$.

Start with the the identity matrix I_m and perform all of the same row operations on I_m as used in the reduction of M to D to create a matrix P.

Similarly, start with I_n and perform the same column operations on it as used in the reduction of M to D to create a matrix Q.

Diagonalization

Claim. By performing integer row and column operations, the matrix M can be transformed into a diagonal matrix D, i.e., $D_{ij} = 0$ for $i \neq j$.

Start with the the identity matrix I_m and perform all of the same row operations on I_m as used in the reduction of M to D to create a matrix P.

Similarly, start with I_n and perform the same column operations on it as used in the reduction of M to D to create a matrix Q.

Then both P and Q have inverses that are integer matrices (equivalently, $\det(P) = \pm 1$ and $\det(Q) = \pm 1$),

Diagonalization

Claim. By performing integer row and column operations, the matrix M can be transformed into a diagonal matrix D, i.e., $D_{ij} = 0$ for $i \neq j$.

Start with the the identity matrix I_m and perform all of the same row operations on I_m as used in the reduction of M to D to create a matrix P.

Similarly, start with I_n and perform the same column operations on it as used in the reduction of M to D to create a matrix Q.

Then both P and Q have inverses that are integer matrices (equivalently, $\det(P) = \pm 1$ and $\det(Q) = \pm 1$), and

$$PMQ = D.$$

Diagonalization

$$PMQ = D$$

Diagonalization

$$PMQ = D$$

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\downarrow\wr & & {\scriptstyle P}\downarrow\wr & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(D) & \longrightarrow & 0,
\end{array}
$$

Diagonalization

$$PMQ = D$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\downarrow\wr & & {\scriptstyle P}\downarrow\wr & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(D) & \longrightarrow & 0,
\end{array}$$

Changing basis in domain and codomain.

Diagonalization

$$PMQ = D$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\downarrow\wr & & {\scriptstyle P}\downarrow\wr & & \vdots & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(D) & \longrightarrow & 0,
\end{array}$$

Changing basis in domain and codomain.

Important point: Since D is diagonal, it is easy to see how $\operatorname{cok}(D)$ is a product of cyclic groups.

Diagonalization

$$PMQ = D$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\downarrow\wr & & {\scriptstyle P}\downarrow\wr & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(D) & \longrightarrow & 0,
\end{array}$$

Changing basis in domain and codomain.

Important point: Since D is diagonal, it is easy to see how $\operatorname{cok}(D)$ is a product of cyclic groups.

Discuss algorithm.

Example

Apply the algorithm to

$$M = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix}.$$

Example

$$\begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \xrightarrow{c_1 \to c_1 + c_2} \begin{pmatrix} 1 & -1 & -1 & 0 \\ 3 & 4 & -1 & -2 \\ -2 & -1 & 3 & -1 \\ -2 & -2 & -1 & 3 \end{pmatrix}$$

$$\xrightarrow[c_3 \to c_3 + c_1]{c_2 \to c_2 + c_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 7 & 2 & -2 \\ -2 & -3 & 1 & -1 \\ -2 & -4 & -3 & 3 \end{pmatrix}$$

$$\xrightarrow[r_3 \to r_3 + 2r_1, r_4 \to r_4 + 2r_1]{r_2 \to r_2 - 3r_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -2 \\ 0 & -6 & 1 & -1 \\ 0 & 5 & -3 & 3 \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -2 \\ 0 & -6 & 1 & -1 \\ 0 & 5 & -3 & 3 \end{pmatrix}$$

$$\xrightarrow[c_4 \to c_4 + 2c_2]{c_3 \to c_3 - 2c_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -6 & 13 & -13 \\ 0 & 5 & -13 & 13 \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -2 \\ 0 & -6 & 1 & -1 \\ 0 & 5 & -3 & 3 \end{pmatrix}$$

$$\xrightarrow[c_4 \to c_4 + 2c_2]{c_3 \to c_3 - 2c_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -6 & 13 & -13 \\ 0 & 5 & -13 & 13 \end{pmatrix}$$

$$\xrightarrow[r_4 \to r_4 - 5r_2]{r_3 \to r_3 + 6r_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & -13 \\ 0 & 0 & -13 & 13 \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & -13 \\ 0 & 0 & -13 & 13 \end{pmatrix} \xrightarrow{c_4 \to c_4 + c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & -13 & 0 \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & -13 \\ 0 & 0 & -13 & 13 \end{pmatrix} \xrightarrow{c_4 \to c_4 + c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & -13 & 0 \end{pmatrix}$$

$$\xrightarrow{r_4 \to r_4 + r_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Example

$$PMQ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -16 & 6 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 & 1 \\ 1 & -1 & 3 & 1 \\ 0 & -3 & 7 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Example

$$PMQ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -16 & 6 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 & 1 \\ 1 & -1 & 3 & 1 \\ 0 & -3 & 7 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$\text{cok}(M) \simeq \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/13 \times \mathbb{Z} \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}.$$

Example

$$PMQ = D$$

Example

$$PMQ = D$$

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\big\downarrow{\scriptstyle \wr} & & {\scriptstyle P}\big\downarrow{\scriptstyle \wr} & & \vdots\,\downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(D) & \longrightarrow & 0,
\end{array}
$$

Example

$$PMQ = D$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(M) & \longrightarrow & 0 \\
 & & {\scriptstyle Q^{-1}}\downarrow\wr & & {\scriptstyle P}\downarrow\wr & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \mathrm{cok}(D) & \longrightarrow & 0,
\end{array}$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -16 & 6 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{P} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ -3a + b \\ -16a + 6b + c \\ a + b + c + d \end{pmatrix} \to \begin{pmatrix} -16a + 6b + c \\ a + b + c + d \end{pmatrix}$$

$$\mathrm{cok}(M) \simeq \mathrm{cok}(D) \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}$$