# Math 361

March 22, 2023

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



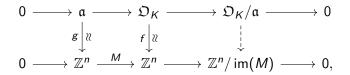
► Smith normal form

#### Motivation

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

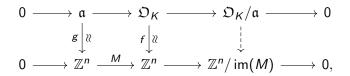
#### Motivation

**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:  $N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|.$ 



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

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

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

**Definition.** The *cokernel* of *M* is

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

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

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

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

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

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

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

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

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

Examples.

$$\mathsf{cok}(M) = \mathbb{Z}^2 / \operatorname{Span} \left\{ \left( egin{array}{c} 2 \\ 0 \end{array} 
ight), \left( egin{array}{c} 0 \\ 3 \end{array} 
ight) 
ight\} \stackrel{\sim}{ o} \mathbb{Z} / 2\mathbb{Z} \oplus \mathbb{Z} / 3\mathbb{Z}$$
 $(a, b) \mapsto (a \mod 2, b \mod 3).$ 

• Let M = diag(0, 0, 1, 2, 3). Then

 $\operatorname{cok}(M) \simeq \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}0\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$  $(a, b, c, d, e) \mapsto (a, b, d, e).$ 

**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).

**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  $i \neq j$ .

**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.

**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 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.

**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  $det(Q) = \pm 1$ ),

**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  $i \neq j$ .

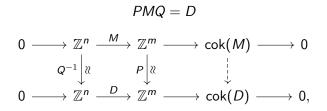
Start with the the identity matrix  $I_m$  and perform all of the same row operations on  $I_m$  as used in the reduction of M to D to create a matrix P.

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.

$$PMQ = D$$



$$PMQ = D$$

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

$$Q^{-1} \downarrow \mathfrak{U} \qquad P \downarrow \mathfrak{U} \qquad \downarrow$$

$$0 \longrightarrow \mathbb{Z}^{n} \xrightarrow{D} \mathbb{Z}^{m} \longrightarrow \operatorname{cok}(D) \longrightarrow 0,$$

Changing basis in domain and codomain.

$$PMQ = D$$

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

$$Q^{-1} \downarrow \mathfrak{U} \qquad P \downarrow \mathfrak{U} \qquad \downarrow$$

$$0 \longrightarrow \mathbb{Z}^{n} \xrightarrow{D} \mathbb{Z}^{m} \longrightarrow \operatorname{cok}(D) \longrightarrow 0,$$

Changing basis in domain and codomain.

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

$$PMQ = D$$

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

$$Q^{-1} \downarrow \mathfrak{U} \qquad P \downarrow \mathfrak{U} \qquad \downarrow$$

$$0 \longrightarrow \mathbb{Z}^{n} \xrightarrow{D} \mathbb{Z}^{m} \longrightarrow \operatorname{cok}(D) \longrightarrow 0,$$

Changing basis in domain and codomain.

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

Discuss algorithm.

Apply the algorithm to

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

$$\begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \xrightarrow{c_1 \to c_1 + c_2} \begin{pmatrix} 1 & -1 & -1 & 0 \\ 3 & 4 & -1 & -2 \\ -2 & -1 & 3 & -1 \\ -2 & -2 & -1 & 3 \end{pmatrix}$$
$$\xrightarrow{c_2 \to c_2 + c_1}_{c_3 \to c_3 + c_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 7 & 2 & -2 \\ -2 & -3 & 1 & -1 \\ -2 & -4 & -3 & 3 \end{pmatrix}$$
$$\xrightarrow{r_2 \to r_2 - 3r_1}_{r_3 \to r_3 + 2r_1, r_4 \to r_4 + 2r_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix}$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -2 \\ 0 & -6 & 1 & -1 \\ 0 & 5 & -3 & 3 \end{pmatrix}$$
$$\xrightarrow{c_3 \to c_3 - 2c_2}_{c_4 \to c_4 + 2c_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -6 & 13 & -13 \\ 0 & 5 & -13 & 13 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 2 & -2 \\ 0 & -3 & 1 & -1 \\ 0 & -4 & -3 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -2 \\ 0 & -6 & 1 & -1 \\ 0 & 5 & -3 & 3 \end{pmatrix}$$
$$\xrightarrow{c_3 \to c_3 - 2c_2}_{c_4 \to c_4 + 2c_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -6 & 13 & -13 \\ 0 & 5 & -13 & 13 \end{pmatrix}$$
$$\xrightarrow{r_3 \to r_3 + 6r_2}_{r_4 \to r_4 - 5r_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & -13 \\ 0 & 0 & -13 & 13 \end{pmatrix}$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & -13 \\ 0 & 0 & -13 & 13 \end{pmatrix} \xrightarrow{c_4 \to c_4 + c_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & -13 & 0 \end{pmatrix}$$
$$\xrightarrow{r_4 \to r_4 + r_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$PMQ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -16 & 6 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 & 1 \\ 1 & -1 & 3 & 1 \\ 0 & -3 & 7 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

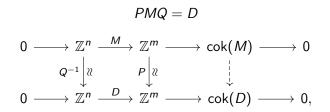
$$PMQ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ -16 & 6 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -2 \\ -1 & -1 & 3 & -1 \\ 0 & -2 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 & 1 \\ 1 & -1 & 3 & 1 \\ 0 & -3 & 7 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

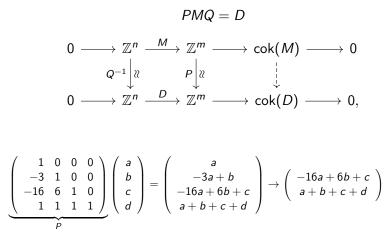
Therefore,

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



PMQ = D





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