

# Math 412      Smith Normal Form

①

Last time we saw that  $S(P, s) \cong \mathbb{Z}V/\tilde{\mathbb{Z}}$  where

$\tilde{\mathbb{Z}} = \text{image}(\tilde{\Delta})$ . By computing the Smith Normal form of  $\tilde{\Delta}$ , we find the elementary divisors of  $S(P, s)$ , and classify it as an Abelian group.

Def. An  $m \times n$  integer matrix  $(a_{ij})$  is in **Smith Normal Form** if

①  $a_{ij} = 0$  if  $i \neq j$     ②  $a_{ii} > 0$  for  $i \leq r$ ;  $a_{ii} = 0$  for  $i > r$ ;

and  $a_{ii} | a_{i+1, i+1}$  for  $i < r$ :

$$\begin{bmatrix} a_{11} & & & 0 \\ & a_{22} & \dots & \\ & & \ddots & \\ 0 & & & a_{rr} \\ & & & 0 \\ & & & \ddots \\ & & & 0 \end{bmatrix}$$

$$a_{11} | a_{22} | \dots | a_{rr}.$$

Def. An integer row (resp., column) operation on an integer matrix is one of the following

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

Write  $A \sim B$  for integer matrices  $A$  and  $B$  if one can be obtained from the other via a sequence of  $\sim$  <sup>integer</sup> row and column operations. Then  $\sim$  is an equivalence relation.

Thm. Each equivalence class of  $m \times n$  matrices under  $\sim$  has a unique matrix in Smith Normal form.

Pf/ We first prove existence by describing an algorithm. Let  $A$

(3)

an  $m \times n$  matrix. If  $A = 0$ , we are done. Otherwise,

- ① by permuting rows and column, we may assume that  $a_{11}$  is the smallest nonzero entry in absolute value. By adding multiples of the first row to other rows or the first column to other columns, attempt to make all entries in the first column and first row except the 1-1 entry equal to zero. If during this process a nonzero matrix entry appears with smaller absolute value than the 1-1 entry, you may permute rows and columns in order to bring that entry to the 1-1 position. Since the 1-1 entry is nonzero and decreasing in magnitude, the process eventually terminates with a matrix of the form
- where  $A'$  is a  $(m-1) \times (n-1)$  matrix.

$$\begin{bmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & & & & \\ 0 & & & & \\ \vdots & & & & \\ 0 & & & & A' \end{bmatrix} \star$$

(4)

② If there is any entry of  $A''$  that is not divisible by  $a_{11}$ , say  $a_{ij}$ , then add column  $j$  to column 1 and go back to step 1. Again, since the  $1-1$  entry increases in magnitude, this new process stops, delivering a matrix of the form  $\star$ , such that all the entries of  $A'$  are divisible by  $a_{11}$ .

③ Apply steps ① and ② to  $A'$ , and thus, by recursion, we get a matrix equivalent to  $A$  but in Smith normal form, (multiplying rows by  $-1$ , if necessary, to make all entries positive).

Note: Let  $S = I_m$  and  $T = I_n$  be identity matrices.

Consider the sequence of elementary row operations leading from  $A$  to its Smith normal form. Whenever a row operation is made, perform the same operation to  $S$  and whenever a column operation

(5)

is performed, perform the same operation to  $T$ . In this way  $S$  and  $T$  are transformed to matrices  $U$  and  $V$  respectively such that  $UV$  is the Smith normal form of  $A$ .

Since integer row and column operations are invertible, the matrices  $U$  and  $V$  are invertible over the integers. Letting  $D$  be the

Smith normal form of  $A$ , we have the following commutative diagram:

$$\begin{array}{ccccccc} \mathbb{Z}^n & \xrightarrow{A} & \mathbb{Z}^m & \rightarrow & \text{cok}(A) & \rightarrow 0 \\ V^{-1} \downarrow \text{??} & \text{??} \downarrow \text{??} & U \downarrow \text{??} & \text{??} \downarrow \text{??} & \downarrow \text{??} & & \\ \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \rightarrow & \text{cok}(D) & \rightarrow 0, & \end{array}$$

inducing an isomorphism  $\text{cok}(A) \rightarrow \text{cok}(D)$ . But  $D = \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & \ddots & \\ & & & & d_s \end{bmatrix}$

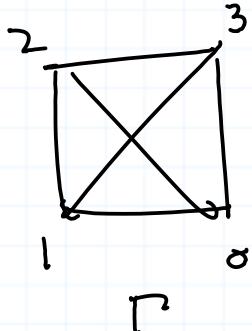
with  $d_1 | d_2 | \dots | d_r$ . So

$$\text{cok}(D) = \frac{\mathbb{Z}^m}{\text{im } c(D)} \stackrel{\star}{=} \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{m-r}$$

(6)

For uniqueness, note that  $d_i$  is the smallest positive integer  $d$  such that  $d \text{cok}(A)$  is minimally generated by at most  $m-i$  elements.  $\square$

Example



$$\tilde{\Delta} = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

$$u \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow{\hspace{10em}} \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

$$\tilde{\Delta} \quad \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 3 & -1 \\ -3 & -1 & -1 \\ 1 & -1 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ -3 & 8 & -4 \\ 1 & -4 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 8 & -4 \\ 0 & -4 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 8 \\ 0 & -4 & -4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & -4 & 4 \end{bmatrix}$$

$$v \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 0 \\ -1 & 3 & -1 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow{\hspace{10em}} \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 3 \\ 0 & -1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 2 \end{bmatrix}$$

7

$$\begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} = U$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & -4 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} = D$$

$$\begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 2 \end{bmatrix} = V$$

Check:

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 2 \end{bmatrix}}_{\left[ \begin{array}{ccc} 3 & -1 & -1 \\ 8 & 0 & -4 \\ 4 & 0 & 0 \end{array} \right]} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -1 & -1 \\ 8 & 0 & -4 \\ 4 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

$$\begin{array}{ccc} \mathbb{Z}^3 & \xrightarrow{\tilde{\Delta}} & \mathbb{Z}^3 \rightarrow S(\Gamma, O) \\ v^{-1} \downarrow & \downarrow u & \downarrow \\ \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \end{array}$$

So  $S(\Gamma, O) \stackrel{\cong}{\longrightarrow} \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$   
 $(a, b, c) \mapsto (3a+b, 2a+b+c)$ .

$$(a, b, c) \mapsto \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}}_{\text{orange}} = \begin{bmatrix} a \\ 3a+b \\ 2a+b+c \end{bmatrix}$$