Math 372

November 14, 2022

Cokernel of a matrix

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

Cokernel of a matrix

Let M be an $m \times n$ integer matrix. There is a corresponding $\mathbb{Z}$-linear function:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m.$$

Cokernel of a matrix

Let M be an $m \times n$ integer matrix. There is a corresponding $\mathbb{Z}$-linear function:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m.$$

The cokernel of M is

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

Cokernel of a matrix

Let M be an $m \times n$ integer matrix. There is a corresponding $\mathbb{Z}$-linear function:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m.$$

The cokernel of M is

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

Examples

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

Examples

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

If $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then

$$\mathrm{cok}(M) = \mathbb{Z}^2 / \mathrm{Span}\{(2,0),(0,3)\}$$

Examples

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

If $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then

$$\mathrm{cok}(M) = \mathbb{Z}^2 / \mathrm{Span}\{(2,0),(0,3)\} \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Examples

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

If $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then

$$\operatorname{cok}(M) = \mathbb{Z}^2 / \operatorname{Span}\{(2,0),(0,3)\} \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

If $M = \operatorname{diag}(0,0,1,2,3)$, then

$$\operatorname{cok}(M) \approx \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Examples

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

If $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then

$$\operatorname{cok}(M) = \mathbb{Z}^2 / \operatorname{Span}\{(2,0),(0,3)\} \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

If $M = \operatorname{diag}(0,0,1,2,3)$, then

$$\begin{aligned} \operatorname{cok}(M) &\approx \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ &\approx \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}. \end{aligned}$$

Examples

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

If $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then

$$\operatorname{cok}(M) = \mathbb{Z}^2/\operatorname{Span}\{(2,0),(0,3)\} \approx \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

If $M = \operatorname{diag}(0,0,1,2,3)$, then

$$\begin{aligned}\operatorname{cok}(M) &\approx \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ &\approx \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.\end{aligned}$$

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

Integer row and column operations

Integer row and column operations

- swap two rows (resp., columns);

Integer row and column operations

- swap two rows (resp., columns);
- negate a row (resp., column);

Integer row and column operations

- swap two rows (resp., columns);
- negate a row (resp., column);
- add one row (resp., column) to a different row (resp., column).

Integer row and column operations

- swap two rows (resp., columns);
- negate a row (resp., column);
- add one row (resp., column) to a different row (resp., column).

When M is regarded as a linear function, these row and column operations correspond to integer changes of bases on the codomain and domain of M, respectively.

Integer row and column operations

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

Integer row and column operations

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

To make the final form unique, we can insist that the diagonal elements satisfy $D_{i,i} | D_{i+1,i+1}$ for all i.

Integer row and column operations

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

To make the final form unique, we can insist that the diagonal elements satisfy $D_{i,i} | D_{i+1,i+1}$ for all i.

Perform the same row ops. to the $m \times m$ identity matrix to get a matrix U,

Integer row and column operations

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

To make the final form unique, we can insist that the diagonal elements satisfy $D_{i,i} | D_{i+1,i+1}$ for all i.

Perform the same row ops. to the $m \times m$ identity matrix to get a matrix U, and perform the same col. ops. to the $n \times n$ identity matrix to get a matrix V.

Integer row and column operations

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

To make the final form unique, we can insist that the diagonal elements satisfy $D_{i,i} | D_{i+1,i+1}$ for all i.

Perform the same row ops. to the $m \times m$ identity matrix to get a matrix U, and perform the same col. ops. to the $n \times n$ identity matrix to get a matrix V. Then

- $\det U = \pm 1$ and $\det V = \pm 1$,

Integer row and column operations

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

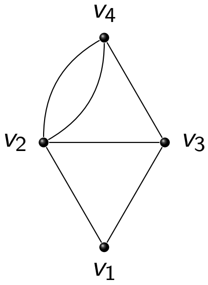
To make the final form unique, we can insist that the diagonal elements satisfy $D_{i,i} | D_{i+1,i+1}$ for all i.

Perform the same row ops. to the $m \times m$ identity matrix to get a matrix U, and perform the same col. ops. to the $n \times n$ identity matrix to get a matrix V. Then

- $\det U = \pm 1$ and $\det V = \pm 1$,
- and $UMV = D$.

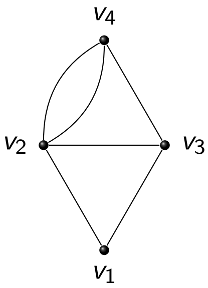
Example

Determine the structure of $\mathrm{Pic}(G)$ for the graph pictured below:



Example

Determine the structure of $\mathrm{Pic}(G)$ for the graph pictured below:



Recall $\mathrm{Pic}(G) \approx \mathrm{cok}(L)$ where L is the Laplacian matrix,

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

Example

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

Example

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

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

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

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

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

Example

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

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

Therefore,

$$\mathrm{Pic}(G) = \mathsf{cok}(L) \simeq \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z} \simeq \mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z}.$$

Example

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

Example

$$\mathrm{Pic}(G) = \mathbb{Z}^4 / \operatorname{im}(L) \to \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}$$

$$(a, b, c, d) \mapsto U \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ -3a + b \\ -16a + 6b + c \\ a + b + c + d \end{pmatrix}$$

Example

$$\mathrm{Pic}(G) = \mathbb{Z}^4/\operatorname{im}(L) \to \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}$$

$$(a, b, c, d) \mapsto U \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ -3a + b \\ -16a + 6b + c \\ a + b + c + d \end{pmatrix}$$

$$\begin{aligned} &\to \quad \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z} \\ &\mapsto (-16a + 6b + c, a + b + c + d). \end{aligned}$$

Example

To find the structure of $\mathrm{Jac}(G)$, first take the reduced Laplacian with respect to any vertex, then apply the procedure illustrated above.

Example

To find the structure of $\mathrm{Jac}(G)$, first take the reduced Laplacian with respect to any vertex, then apply the procedure illustrated above.

For instance, the reduced Laplacian with respect to v_1 is

$$\tilde{L} = \begin{pmatrix} 4 & -1 & -2 \\ -1 & 3 & -1 \\ -2 & -1 & 3 \end{pmatrix}.$$

Example

To find the structure of $\mathrm{Jac}(G)$, first take the reduced Laplacian with respect to any vertex, then apply the procedure illustrated above.

For instance, the reduced Laplacian with respect to v_1 is

$$\tilde{L} = \begin{pmatrix} 4 & -1 & -2 \\ -1 & 3 & -1 \\ -2 & -1 & 3 \end{pmatrix}.$$

The diagonalized version of $\tilde{L}$ will be

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 13 \end{pmatrix},$$

Example

To find the structure of $\mathrm{Jac}(G)$, first take the reduced Laplacian with respect to any vertex, then apply the procedure illustrated above.

For instance, the reduced Laplacian with respect to v_1 is

$$\tilde{L} = \begin{pmatrix} 4 & -1 & -2 \\ -1 & 3 & -1 \\ -2 & -1 & 3 \end{pmatrix}.$$

The diagonalized version of $\tilde{L}$ will be

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 13 \end{pmatrix},$$

and so $\mathrm{Jac}(G) \simeq \mathbb{Z}/13\mathbb{Z}$.

Abelian groups

An *abelian group* is a set A and an operation

$$A \times A \to A$$

satistfying

Abelian groups

An *abelian group* is a set A and an operation

$$A \times A \to A$$

satistfying

- $a + b = b + a$ for all $a, b \in A$.

Abelian groups

An *abelian group* is a set A and an operation

$$A \times A \to A$$

satistfying

- $a + b = b + a$ for all $a, b \in A$.
- There exists $0 \in A$ such that $a + 0 = a$ for all $a \in A$.

Abelian groups

An *abelian group* is a set A and an operation

$$A \times A \to A$$

satistfying

- $a + b = b + a$ for all $a, b \in A$.
- There exists $0 \in A$ such that $a + 0 = a$ for all $a \in A$.
- For all $a \in A$, there exists $b \in A$ such that $a + b = 0$. (Then $b := -a$.)

Abelian groups

An *abelian group* is a set A and an operation

$$A \times A \to A$$

satistfying

- $a + b = b + a$ for all $a, b \in A$.
- There exists $0 \in A$ such that $a + 0 = a$ for all $a \in A$.
- For all $a \in A$, there exists $b \in A$ such that $a + b = 0$. (Then $b := -a$.)
- $a + (b + c) = (a + b) + c$ for all $a, b, c \in A$.

Z-modules

If A is an abelian group, $a \in A$, and $n \in \mathbb{N}$, define

$$na = \underbrace{a + \cdots + a}_{n \text{ times}}$$

$\mathbb{Z}$-modules

If A is an abelian group, $a \in A$, and $n \in \mathbb{N}$, define

$$na = \underbrace{a + \cdots + a}_{n \text{ times}}$$

and if $n \in \mathbb{Z}_{<0}$, define

$$na = -(-n)a.$$

$\mathbb{Z}$-modules

If A is an abelian group, $a \in A$, and $n \in \mathbb{N}$, define

$$na = \underbrace{a + \cdots + a}_{n \text{ times}}$$

and if $n \in \mathbb{Z}_{<0}$, define

$$na = -(-n)a.$$

Then A is a $\mathbb{Z}$-module.

Z-modules

If A is an abelian group, $a \in A$, and $n \in \mathbb{N}$, define

$$na = \underbrace{a + \cdots + a}_{n \text{ times}}$$

and if $n \in \mathbb{Z}_{<0}$, define

$$na = -(-n)a.$$

Then A is a $\mathbb{Z}$-module.

Conversely, every $\mathbb{Z}$-module is an abelian group.

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A.

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A. In other words, if $a \in A$, then $a = \sum_{i=1}^{m} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$.

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A. In other words, if $a \in A$, then $a = \sum_{i=1}^{m} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$.

Define a $\mathbb{Z}$-linear mapping

$$\begin{aligned} \mathbb{Z}^m &\to A \\ e_i &\mapsto a_i \end{aligned}$$

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A. In other words, if $a \in A$, then $a = \sum_{i=1}^{m} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$.

Define a $\mathbb{Z}$-linear mapping

$$\begin{aligned} \mathbb{Z}^m &\to A \\ e_i &\mapsto a_i \end{aligned}$$

This mapping is surjective (why?)

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A. In other words, if $a \in A$, then $a = \sum_{i=1}^{m} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$.

Define a $\mathbb{Z}$-linear mapping

$$\begin{aligned} \mathbb{Z}^m &\to A \\ e_i &\mapsto a_i \end{aligned}$$

This mapping is surjective (why?) Let K be the kernel of this mapping.

Structure theorem for finitely-generated abelian groups

Suppose $a_1, \ldots, a_m$ generate A. In other words, if $a \in A$, then $a = \sum_{i=1}^{m} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$.

Define a $\mathbb{Z}$-linear mapping

$$\begin{aligned} \mathbb{Z}^m &\to A \\ e_i &\mapsto a_i \end{aligned}$$

This mapping is surjective (why?) Let K be the kernel of this mapping. Then we have a short exact sequence

$$0 \to K \to \mathbb{Z}^m \to A \to 0.$$

Structure theorem for finitely-generated abelian groups

$$0 \to K \to \mathbb{Z}^m \to A \to 0$$

Structure theorem for finitely-generated abelian groups

$$0 \to K \to \mathbb{Z}^m \to A \to 0$$

By a course in algebra, K is finitely generated, say with n generators.

Structure theorem for finitely-generated abelian groups

$$0 \to K \to \mathbb{Z}^m \to A \to 0$$

By a course in algebra, K is finitely generated, say with n generators. So as with A, there is a surjective mapping $\mathbb{Z}^n \to K$:

$$\begin{tikzcd}
\mathbb{Z}^n \arrow[rr, dashed, "M"] \arrow[dr, two heads] & & \mathbb{Z}^m \arrow[r] & A \arrow[r] & 0 \\
& K \arrow[ur, hook] & & &
\end{tikzcd}$$

Structure theorem for finitely-generated abelian groups

$$0 \to K \to \mathbb{Z}^m \to A \to 0$$

By a course in algebra, K is finitely generated, say with n generators. So as with A, there is a surjective mapping $\mathbb{Z}^n \to K$:

$$\begin{tikzcd}
\mathbb{Z}^n \arrow[rr, dashed, "M"] \arrow[dr, two heads] & & \mathbb{Z}^m \arrow[r] & A \arrow[r] & 0 \\
& K \arrow[ur, hook] & & &
\end{tikzcd}$$

The induced mapping $\mathbb{Z}^n \to \mathbb{Z}^m$ is represented by a matrix M, and

$$A \approx \mathrm{cok}(M).$$

Structure theorem for finitely-generated abelian groups

Suppose U and V are matrices, invertible over $\mathbb{Z}$ such that $UMV = N$. Then we have a commutative diagram inducing an isomorphism $\operatorname{cok}(M) \to \operatorname{cok}(N)$:

$$
\begin{tikzcd}
\mathbb{Z}^n \arrow[r, "M"] \arrow[d, "V^{-1}"', "\wr"] & \mathbb{Z}^m \arrow[r] \arrow[d, "U", "\wr"'] & \operatorname{cok} M \arrow[r] \arrow[d, dashed] & 0 \\
\mathbb{Z}^n \arrow[r, "N"] & \mathbb{Z}^m \arrow[r] & \operatorname{cok} N \arrow[r] & 0.
\end{tikzcd}
\tag{1}
$$

Structure theorem for finitely-generated abelian groups

Suppose U and V are matrices, invertible over $\mathbb{Z}$ such that $UMV = N$. Then we have a commutative diagram inducing an isomorphism $\mathrm{cok}(M) \to \mathrm{cok}(N)$:

$$\begin{tikzcd}
\mathbb{Z}^n \arrow[r, "M"] \arrow[d, "V^{-1}"', "\wr"] & \mathbb{Z}^m \arrow[r] \arrow[d, "U", "\wr"'] & \mathrm{cok}\, M \arrow[r] \arrow[d, dashed] & 0 \\
\mathbb{Z}^n \arrow[r, "N"] & \mathbb{Z}^m \arrow[r] & \mathrm{cok}\, N \arrow[r] & 0.
\end{tikzcd} \tag{1}$$

We can always choose U and V so that $N = UMV$ is diagonal.

Structure theorem for finitely-generated abelian groups

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$.

Structure theorem for finitely-generated abelian groups

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$.
Unique if either of the following:

Structure theorem for finitely-generated abelian groups

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$.
Unique if either of the following:

Condition 1: $n_i | n_{i+1}$ (n_i evenly divides n_{i+1}) for all i. In this case, the n_i are the *invariant factors* of the group.

Structure theorem for finitely-generated abelian groups

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$.
Unique if either of the following:

Condition 1: $n_i | n_{i+1}$ (n_i evenly divides n_{i+1}) for all i. In this case, the n_i are the *invariant factors* of the group.

Condition 2: There exist primes $p_1 \leq \cdots \leq p_k$ and positive integers m_i such that $n_i = p_i^{m_i}$ for all i. In this case, the n_i are the *elementary divisors* and the $\mathbb{Z}/n_i\mathbb{Z}$ are the *primary factors* of the group.

Structure theorem for finitely-generated abelian groups

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$.
Unique if either of the following:

Condition 1: $n_i | n_{i+1}$ (n_i evenly divides n_{i+1}) for all i. In this case, the n_i are the *invariant factors* of the group.

Condition 2: There exist primes $p_1 \leq \cdots \leq p_k$ and positive integers m_i such that $n_i = p_i^{m_i}$ for all i. In this case, the n_i are the *elementary divisors* and the $\mathbb{Z}/n_i\mathbb{Z}$ are the *primary factors* of the group.

The number r is the *rank* of the group.

Structure theorem for finitely-generated abelian groups

Theorem. (Chinese remainder theorem.) Let $m, n \in \mathbb{Z}$. Then

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

if and only if m and n are relatively prime. If $\gcd(m, n) = 1$, then an isomorphism is provided by $a \mapsto (a \bmod m, a \bmod n)$.

Structure theorem for finitely-generated abelian groups

Theorem. (Chinese remainder theorem.) Let $m, n \in \mathbb{Z}$. Then

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

if and only if m and n are relatively prime. If $\gcd(m, n) = 1$, then an isomorphism is provided by $a \mapsto (a \bmod m, a \bmod n)$.

Examples.

$$\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Structure theorem for finitely-generated abelian groups

Theorem. (Chinese remainder theorem.) Let $m, n \in \mathbb{Z}$. Then

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

if and only if m and n are relatively prime. If $\gcd(m, n) = 1$, then an isomorphism is provided by $a \mapsto (a \bmod m, a \bmod n)$.

Examples.

$$\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Structure theorem for finitely-generated abelian groups

Definition. An $m \times n$ integer matrix M is in *Smith normal form* if

$$M = \mathrm{diag}(s_1, \ldots, s_k, 0, \ldots, 0),$$

a diagonal matrix, where $s_1, \ldots, s_k$ are positive integers such that $s_i | s_{i+1}$ for all i. The s_i are called the *invariant factors* of M.

Structure theorem for finitely-generated abelian groups

Example. The matrix

$$M := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

is in Smith normal form with invariant factors $s_1 = 1$, $s_2 = 2$, and $s_3 = 12$.

Structure theorem for finitely-generated abelian groups

Example. The matrix

$$M := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

is in Smith normal form with invariant factors $s_1 = 1$, $s_2 = 2$, and $s_3 = 12$. We have

$$\operatorname{cok}(M) := \mathbb{Z}^5 / \operatorname{im}(M) \simeq \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}^2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}^2.$$

So $\operatorname{cok}(M)$ has rank $r = 2$ and its invariant factors are 2 and 12.