Math 361

March 24, 2023

Today

- Structure theorem for finitely generated abelian groups.
- Consequences.

Structure theorem for finitely generated abelian groups

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

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

Structure theorem for finitely generated abelian groups

Theorem (Structure theorem for finitely generated 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 finitely generated 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 $r \geq 0$. **Uniqueness:** These integers may be required to satisfy either of the following two conditions, and in either case they are uniquely determined by the isomorphism class of the group.

Structure theorem for finitely generated abelian groups

Theorem (Structure theorem for finitely generated 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 $r \geq 0$. **Uniqueness:** These integers may be required to satisfy either of the following two conditions, and in either case they are uniquely determined by the isomorphism class of the group.

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 finitely generated 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 $r \geq 0$. **Uniqueness:** These integers may be required to satisfy either of the following two conditions, and in either case they are uniquely determined by the isomorphism class of the group.

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 finitely generated 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 $r \geq 0$. **Uniqueness:** These integers may be required to satisfy either of the following two conditions, and in either case they are uniquely determined by the isomorphism class of the group.

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

Compare the result for finitely generated $\mathbb{Z}$-modules with the result for finitely generated K-modules over a field K.

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group with generators $\{a_1, \ldots, a_m\}$.

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group with generators $\{a_1, \ldots, a_m\}$.

We get a surjective group homomorphism

$$\mathbb{Z}^m \xrightarrow{\pi} A$$

$$e_i \mapsto a_i$$

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group with generators $\{a_1, \ldots, a_m\}$.

We get a surjective group homomorphism

$$\mathbb{Z}^m \xrightarrow{\pi} A$$

$$e_i \mapsto a_i$$

Since $\mathbb{Z}^m$ is Noetherian, every subgroup of $\mathbb{Z}^m$ is finitely generated.

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group with generators $\{a_1, \ldots, a_m\}$.

We get a surjective group homomorphism

$$\mathbb{Z}^m \xrightarrow{\pi} A$$

$$e_i \mapsto a_i$$

Since $\mathbb{Z}^m$ is Noetherian, every subgroup of $\mathbb{Z}^m$ is finitely generated. In particular, the kernel of π is finitely generated, say by $\{b_1, \ldots, b_n\}$.

Structure theorem for finitely generated abelian groups

Let A be a finitely generated abelian group with generators $\{a_1, \ldots, a_m\}$.

We get a surjective group homomorphism

$$\mathbb{Z}^m \xrightarrow{\pi} A$$

$$e_i \mapsto a_i$$

Since $\mathbb{Z}^m$ is Noetherian, every subgroup of $\mathbb{Z}^m$ is finitely generated. In particular, the kernel of π is finitely generated, say by $\{b_1, \ldots, b_n\}$. Define

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

where M is the $m \times n$ integer matrix with i-th column b_i.

Structure theorem for finitely generated abelian groups

We get a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \xrightarrow{\pi} A \longrightarrow 0$$

Structure theorem for finitely generated abelian groups

We get a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \xrightarrow{\pi} A \longrightarrow 0$$

The sequence is exact: the image of M is the kernel of π and π is surjective.

Structure theorem for finitely generated abelian groups

We get a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \xrightarrow{\pi} A \longrightarrow 0$$

The sequence is exact: the image of M is the kernel of π and π is surjective.

Recall that the *cokernel* of the matrix M is $\mathrm{cok}(M) := \mathbb{Z}^m/\mathrm{im}(M)$.

Structure theorem for finitely generated abelian groups

We get a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \xrightarrow{\pi} A \longrightarrow 0$$

The sequence is exact: the image of M is the kernel of π and π is surjective.

Recall that the *cokernel* of the matrix M is $\mathrm{cok}(M) := \mathbb{Z}^m/\mathrm{im}(M)$.

Then π induces an isomorphism

$$\begin{aligned} \mathrm{cok}(M) &\simeq A \\ \overline{e}_i &\mapsto a_i . \end{aligned}$$

Structure theorem for finitely generated abelian groups

We get a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \xrightarrow{\pi} A \longrightarrow 0$$

The sequence is exact: the image of M is the kernel of π and π is surjective.

Recall that the *cokernel* of the matrix M is $\mathrm{cok}(M) := \mathbb{Z}^m/\mathrm{im}(M)$.

Then π induces an isomorphism

$$\begin{aligned} \mathrm{cok}(M) &\simeq A \\ \overline{e}_i &\mapsto a_i. \end{aligned}$$

In this way, A is encoded in the matrix M.

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

There were choices in the construction of M:

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

There were choices in the construction of M: (i) generators for A

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

There were choices in the construction of M: (i) generators for A and (ii) generators for $\ker(\pi)$.

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

There were choices in the construction of M: (i) generators for A and (ii) generators for $\ker(\pi)$.

Different choices could produce a different $m \times n$ integer matrix N such that

$$\mathrm{cok}(M) \simeq \mathrm{cok}(N).$$

Structure theorem for finitely generated abelian groups

We have just seen that finitely generated abelian groups are exactly the groups

$$\mathrm{cok}(M)$$

where M is any $m \times n$ integer matrix.

There were choices in the construction of M: (i) generators for A and (ii) generators for $\ker(\pi)$.

Different choices could produce a different $m \times n$ integer matrix N such that

$$\mathrm{cok}(M) \simeq \mathrm{cok}(N).$$

The possible matrices are determined up to integer row and column operations.

Smith normal form

Through integer row and column operations, every $m \times n$ integer matrix M has a unique *Smith normal form*

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

where $s_1, \ldots, s_k$ are positive integers such that $s_i | s_{i+1}$ for all i.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.
2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.
2. If M is free and the quotient module M/N is finite, then M and N have the same rank.
3. Suppose that M and N are free, both of rank n. Fix isomorphisms $M \simeq \mathbb{Z}^n$ and $N \simeq \mathbb{Z}^n$ and consider the resulting commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

where W is an $n \times n$ integer matrix. Then

$$|M/N| = |\det(W)|.$$

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian $\Rightarrow$ N finitely generated.

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian $\Rightarrow$ N finitely generated.

Structure theorem:

$$N \simeq C \times \mathbb{Z}^r$$

where C is finite (a finite product of cyclic groups).

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian $\Rightarrow$ N finitely generated.

Structure theorem:

$$N \simeq C \times \mathbb{Z}^r$$

where C is finite (a finite product of cyclic groups).

$N \subseteq M \simeq \mathbb{Z}^n \Rightarrow$ no nonzero element of N can have finite order

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian $\Rightarrow$ N finitely generated.

Structure theorem:

$$N \simeq C \times \mathbb{Z}^r$$

where C is finite (a finite product of cyclic groups).

$N \subseteq M \simeq \mathbb{Z}^n \Rightarrow$ no nonzero element of N can have finite order $\Rightarrow C = 0$

Corollaries

Let M be a finitely generated $\mathbb{Z}$-module, and let $N \subseteq M$ be a $\mathbb{Z}$-submodule.

1. If M is free, then so is N.

Proof. M a finitely generated $\mathbb{Z}$-module $\Rightarrow$ M Noetherian $\Rightarrow$ N finitely generated.

Structure theorem:

$$N \simeq C \times \mathbb{Z}^r$$

where C is finite (a finite product of cyclic groups).

$N \subseteq M \simeq \mathbb{Z}^n \Rightarrow$ no nonzero element of N can have finite order $\Rightarrow C = 0 \Rightarrow N$ is free. $\square$

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Proof.
Choosing bases for M and N, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Proof.
Choosing bases for M and N, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

Smith normal form for W: $D = \operatorname{diag}(n_1, n_2, \ldots, n_k, \underbrace{0, \ldots, 0}_{m-k})$

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Proof.
Choosing bases for M and N, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

Smith normal form for W: $D = \operatorname{diag}(n_1, n_2, \ldots, n_k, \underbrace{0, \ldots, 0}_{m-k})$

$$M/N \simeq \operatorname{cok}(W) \simeq \operatorname{cok}(D) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^{n-k} \times \mathbb{Z}^{m-n}.$$

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Proof.
Choosing bases for M and N, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

Smith normal form for W: $D = \operatorname{diag}(n_1, n_2, \ldots, n_k, \underbrace{0, \ldots, 0}_{m-k})$

$$M/N \simeq \operatorname{cok}(W) \simeq \operatorname{cok}(D) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^{n-k} \times \mathbb{Z}^{m-n}.$$

Then M/N finite if and only if $k = m = n$.

Corollaries

2. If M is free and the quotient module M/N is finite, then M and N have the same rank.

Proof.
Choosing bases for M and N, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

Smith normal form for W: $D = \operatorname{diag}(n_1, n_2, \ldots, n_k, \underbrace{0, \ldots, 0}_{m-k})$

$$M/N \simeq \operatorname{cok}(W) \simeq \operatorname{cok}(D) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^{n-k} \times \mathbb{Z}^{m-n}.$$

Then M/N finite if and only if $k = m = n$. So M and N have the same rank n.

Corollaries

3. Suppose that M and N are free, both of rank n. Fix isomorphisms $M \simeq \mathbb{Z}^n$ and $N \simeq \mathbb{Z}^n$ and consider the resulting commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

where W is an $n \times n$ integer matrix. Then

$$|M/N| = |\det(W)|.$$

Corollaries

3. Suppose that M and N are free, both of rank n. Fix isomorphisms $M \simeq \mathbb{Z}^n$ and $N \simeq \mathbb{Z}^n$ and consider the resulting commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

where W is an $n \times n$ integer matrix. Then

$$|M/N| = |\det(W)|.$$

Proof. Smith normal form for W: $D = \operatorname{diag}(s_1, s_2, \ldots, s_n)$ with $PMQ = W$.

Corollaries

3. Suppose that M and N are free, both of rank n. Fix isomorphisms $M \simeq \mathbb{Z}^n$ and $N \simeq \mathbb{Z}^n$ and consider the resulting commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

where W is an $n \times n$ integer matrix. Then

$$|M/N| = |\det(W)|.$$

Proof. Smith normal form for W: $D = \operatorname{diag}(s_1, s_2, \ldots, s_n)$ with $PMQ = W$. Then
$|M/N| = |\operatorname{cok}(D)| = \prod_{i=1}^{n} s_i = \det(D)$

Corollaries

3. Suppose that M and N are free, both of rank n. Fix isomorphisms $M \simeq \mathbb{Z}^n$ and $N \simeq \mathbb{Z}^n$ and consider the resulting commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \vdots & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{W} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} W & \longrightarrow & 0 \end{array}$$

where W is an $n \times n$ integer matrix. Then

$$|M/N| = |\det(W)|.$$

Proof. Smith normal form for W: $D = \operatorname{diag}(s_1, s_2, \ldots, s_n)$ with $PMQ = W$. Then
$|M/N| = |\operatorname{cok}(D)| = \prod_{i=1}^{n} s_i = \det(D) = \det(W)$. □