MAT301: Extra Topics

QiLin Xue

August 8, 2021

Contents

Free Abelian Groups

> **Definition Set of $\mathbb{Z}$ linear combinations of elements of S**
> Let $(A,+)$ be an abelian group. Note that if $S\subseteq A$, then
>
> $$\langle S\rangle = \left\{\sum_{i=1}^m k_i a_i : m\in\mathbb{Z}_{\geq 0},\, a_i\in S, k_i\in\mathbb{Z}\right\}$$
>
> where the right hand side can be denoted as $\text{span}_{\mathbb{Z}}(S)$, which is the set of all $\mathbb{Z}$ linear combinations of elements of S.

Since empty sets are trivial, we have

$$\text{span}_{\mathbb{Z}}(\emptyset) = \{0\} \tag{1}$$

> **Definition Linear Independence, Span, Basis**
> Let $S\subseteq A$.
>
> 1. S is linearly independent (over $\mathbb{Z}$) if for any $m\in\mathbb{Z}_{>0}$, $a_1,\dots,a_m\in S$, and $k_1,\dots,k_m\in\mathbb{Z}$,
>
> $$\sum_{i=1}^m k_i a_i = 0 \implies a_1=\cdots=a_m=0,$$
>
>   or equivalently if every element of A can be written as a $\mathbb{Z}$-linear combination of elements of S in at most one way.
> 2. S spans A (over $\mathbb{Z}$) if $A=\text{span}_{\mathbb{Z}}(S)$, or equivalently every element of A can be written as a $\mathbb{Z}$-linear combination of elements of A in at least one way.
> 3. S is a basis (or $\mathbb{Z}$-basis) of A if S is linearly independent and spans A, or equivalently if every element of A can be written as a $\mathbb{Z}$-linear combination of elements of S in exactly one way.

■ **Example 1:** $e_1, \ldots, e_m$ is a basis of $\mathbb{Z}^m$.

Definition Free Abelian Group
A free abelian group is an abelian group that has a basis.

A free abelian group of finite rank is an abelian group that has a finite basis.

■ **Example 2:** $\mathbb{Z}^m$ is a free abelian group of finite rank for all $m \in \mathbb{Z}_{\geq 0}$. Note that $\mathbb{Z}^0 = \{0\}$.

■ **Example 3:** If $\{v_1, \ldots, v_m\} \subseteq \mathbb{R}^n$ is linearly independent over $\mathbb{R}$ and A is the subgroup of $\mathbb{R}^n$ generated by $\{v_1, \ldots, v_n\}$, i.e. $A = \langle v_1, \ldots, v_n = \operatorname{span}_{\mathbb{Z}}(\{v_1, \ldots, v_n\})$, then $\{v_1, \ldots, v_n\}$ is a $\mathbb{Z}$-basis of A, so A is a free abelian group of finite rank.

■ **Example 4:** If $\{G_i\}_{i \in I}$ is a set of groups, then

$$\prod_{i \in I}{}' G_i := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \,\middle|\, g_i = e_{G_i} \text{ for all but finitely many } i \in I \right\}$$

is a subgroup of the direct product $\prod_{i \in I} G_i$. If the G_i are abelian, then we denote $\prod'_{i \in I} G_i$ by $\bigoplus_{i \in I} G_i$, and call it the direct sum of $\{G_i\}_{i \in I}$.
If I is infinite and $G_i = \mathbb{Z}$ for all $i \in I$, then $\bigoplus_{i \in I} G_i = \bigoplus_{i \in I} \mathbb{Z}$ is a free abelian group that is not of finite rank (it has an infinite basis but no finite basis).

Note that free abelian groups are like vector spaces over $\mathbb{Z}$.

■ Corollary

For all $m, n \in \mathbb{Z}_{>0}$, we have $\mathbb{Z}^m \cong \mathbb{Z}^n$ if and only if $m = n$.

■ Proposition 1

Let A be a finitely generated group. Then A is of finite rank if and only if A is a finite group.

Proof: The "only if" direction is immediate. Suppose A is a finite group and let $\{g_1, \ldots, g_m\}$ be a generating set of A. Let $\{a_i\}_{i \in I}$ be a basis of A. There is a finite subset $\{a_{i_1}, \ldots, a_{i_n}\}$ of $\{a_i\}_{i \in I}$ such that

$$\{g_1, \ldots, g_m\} \subseteq \operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\} \right). \tag{2}$$

Then

$$A = \operatorname{span}_{\mathbb{Z}}(\{g_1, \ldots, g_m\}) \subseteq \operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\} \right) \subseteq A, \tag{3}$$

so $\operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\} \right) = A$. Since $\{a_{i_1}, \ldots, a_{i_n}\} \subseteq \{a_i\}_{i \in I}$ and $\{a_i\}_{i \in I}$ us linearly independent, it follows that $\{a_{i_1}, \ldots, a_{i_n}\}$ is linearly independent. Therefore, $\{a_{i_1}, \ldots, a_{i_n}\}$ is a basis of A, so A is of finite rank. ■

Warning! Here are a few misconceptions. Take $\mathbb{Z}$ for example. THen:

- $\{2, 3\}$ is a minimal spanning subset of $\mathbb{Z}$, but it is not a basis as it is linearly dependent.
- $\{2, 3\}$ spans $\mathbb{Z}$, but does not contain a basis of $\mathbb{Z}$.
- $\{2\}$ is a maximal linearly independent subset of $\mathbb{Z}$, but it is not a basis because its span is $2\mathbb{Z} \subsetneq \mathbb{Z}$.
- $\{2\}$ is linearly independent, but it is not contained in a basis of $\mathbb{Z}$.

Proposition 2: Homomorphisms and Bases

Let A be a free abelian group and let $\{a_i\}_{i\in I}$ be a basis of A.
Let B be an abelian group and let $\{b_i\}_{i\in I}$ be a family of elements of B.
Then there exists a unique homomorphism $\phi : A \to B$ such that $\phi(a_i) = b_i$ for all $i \in I$. IT is surjective if and only if $\{b_i\}_{i\in I}$ spans B, it is injective if and only if $\{b_i\}_{i\in I}$ is linearly independent, and it is an isomorphism iff $\{b_i\}_{i\in I}$ is a basis of B.

Let A be a free abelian group of finite rank n. For any basis $\alpha = \{a_1, \dots, a_n\}$ of A there exists a unique isomorphism:

$$\theta_\alpha : A \to \mathbb{Z}^n \tag{4}$$

such that $\theta(a_i) = e_i$ for all $i = 1, \dots, n$. Note that:

- $\theta_\alpha^{-1}(k_1, \dots, k_n) = \sum_{i=1}^{n} k_i a_i$
- For all $a \in A$, let us write $[a]_\alpha = \theta_\alpha(a) \in \mathbb{Z}^n$.

Proposition 3

Let A, B be free abelian groups of finite ranks n and m, respectively. Let $\alpha = \{a_1, \dots, a_n\}$ be a basis of A and $\beta = \{b_1, \dots, b_m\}$ be a basis of B. For all homomorphisms $\phi : A \to B$ there exists a unique matrix

$$[T]_\beta^\alpha \in \mathrm{Mat}_{m\times n}(\mathbb{Z}) \tag{5}$$

such that for all $a \in A$ we have

$$[Ta]_\beta = [T]_\beta^\alpha [a]_\alpha. \tag{6}$$

Let C be a free abelian group of finite rank p and let $\gamma = \{c_1, \dots, c_p\}$ be a basis of C. If $T : A \to B$ and $S : B \to C$ are homomorphisms, then

$$[S \circ T]_\gamma^\alpha = [S]_\gamma^\beta [T]_\beta^\alpha \tag{7}$$

Proof: Let $T : A \to B$ be a homomorphism. Define

$$[T]_\beta^\alpha = [[Ta_1]_\beta \cdots [Ta_n]_\beta]. \tag{8}$$

The rest is straightforward. ■

Corollary

A homomorphism $T : A \to B$ is an isomorphism if and only if there exists $N \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$ such that

$$[T]_\beta^\alpha n = I_m \text{ and } N[T]_\beta^\alpha = I_n \tag{9}$$

in which case $m = n$.

Invertible Element of $\mathrm{Mat}_{n\times n}(\mathbb{Z})$

Definition **Invertible Element of $\mathrm{Mat}_{n\times n}(\mathbb{Z})$**
Let n be a positive integer and $M \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. We say that M is an invertible element of $\mathrm{Mat}_{n\times n}(\mathbb{Z})$ if there exists $N \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ such that

$$MN = I_n = NM, \tag{10}$$

in which case N is unique, denoted by M^{-1}, and called the *inverse of M*. We denote the subset of invertible elements of $\mathrm{Mat}_{n\times n}(\mathbb{Z})$ by $\mathrm{GL}_n(\mathbb{Z})$.

Note that $M \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ is invertible if and only if it is invertible in $\mathrm{Mat}_{n\times n}(\mathbb{Q})$ and $M^{-1} \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$.

Proposition 4

$$\mathsf{GL}_n(\mathbb{Z}) = \{M \in \mathsf{Mat}_{n\times n}(\mathbb{Z}) | \det(M) \in \{\pm 1\} \tag{11}$$

Proof: If $M \in \mathsf{GL}_n(\mathbb{Z})$, then

$$\det(M)\det\left(M^{-1}\right) = \det(I_n) = 1 \tag{12}$$

Since $\det(M), \det\left(M^{-1}\right) \in \mathbb{Z}$, it follows that $\det(M) = \det\left(M^{-1}\right) = \pm 1$.

If $M \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$ and $\det(M) = \pm 1$, then the usual formula for $M^{-1} \in \mathsf{Mat}_{n\times n}(\mathbb{Q})$ shows that $M^{-1} \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$. Thus, $M \in \mathsf{GL}_n(\mathbb{Z})$. ■

Proposition 5

For each free abelian group A of finite rank, every subgroup B of A is a free abelian group and

$$\operatorname{rank} B \leq \operatorname{rank} A \tag{13}$$

Remarks: One can drop the assumption that A is of finite rank.

Proof: We will proceed by induction on $m = \operatorname{rank}(A)$.

If $m \geq 0$ and assume that for each abelian group of rank m, every subgroup of it is a free abelian group of rank at most m.

Let A be a free abelian group of rank $m+1$ and let $B \leq A$. We can choose a basis $\alpha = \{a_1, \ldots, a_{m+1}\}$ of A and define

$$A' = \operatorname{span}_{\mathbb{Z}}(\{a_1, \ldots, a_m\}) \leq A \tag{14}$$

Then A' is a free abelian group of rank m. ■

Second Reduction Theorem

Let A be a finitely generated abelian group, $\phi : \mathbb{Z}^m \to A$ is a surjective homomorphism, and $B = \ker\phi \leq \mathbb{Z}^m$. Recall that it suffices to construct an isomorphism $\mathbb{Z}^m \to \mathbb{Z}^m$ that maps B to

$$d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\} \leq \mathbb{Z}^m$$

for some positive integers $d_1 | \cdots | d_n$.

Since $B \leq \mathbb{Z}^m$, we now know that B is a free abelian group of rank $n \leq m$. Let $r = m - n$. It then suffices to prove the following theorem (too lazy to write proof, can be found in Lec 20):

Let C be a free abelian group of finite rank m and let $B \leq C$. Then B is a free abelian group of rank at most m. Let $n = \operatorname{rank}(B) \leq m$.

Then, there exists bases $\beta = \{b_1, \ldots, b_n\}$ of B and $\gamma = \{c_1, \ldots, c_m\}$ of C and positive integers $d_1 | \cdots | d_n$ such that

$$b_i = d_i c_i \tag{15}$$

for all $i = 1, \ldots, n$. Moreover, $d_1, \ldots, d_n$ are unique.

Indeed, suppose that this theorem holds and apply it to $B = \ker\phi \leq \mathbb{Z}^n = C$. The isomorphism

$$\mathbb{Z}^m = C \xrightarrow{[\cdot]_\gamma} \mathbb{Z}^m \tag{16}$$

maps $b_i = d_i c_i$ to $d_i e_i$ for all $i = 1, \ldots, n$. Therefore, the isomorphism maps B to $d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\}$.

We will prove a more general theorem.

Let B and C be free abelian groups of finite ranks n and m, respectively. Let $\Psi : B \to C$ be a homomorphism.

Then there exists bases $\beta = \{b_1, \ldots, b_n\}$ of B and $\gamma = \{c_1, \ldots, c_m\}$ of C, there exists a positive integer

$r \leq m, n$ and there exists positive integers $d_1 | \cdots | d_r$ such that

$$\Psi(b_i) = \begin{cases} d_i c_i & 1 \leq i \leq r \\ 0 & r < i \leq n \end{cases} \tag{17}$$

or equivalently

$$[\Psi]_\gamma^\beta = \left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right] \tag{18}$$

Moreover, $r, d_1, \ldots, d_r$ are unique.

Let β_0, γ_0 be bases of B, C, respectively. The theorem is equivalent to the assertion that there exists matrices $P \in \mathsf{GL}_m(\mathbb{Z})$, $Q \in \mathsf{GL}_n(\mathbb{Z})$ such that

$$P[\Psi]_{\gamma_0}^{\beta_0} Q = \left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right] \tag{19}$$

for some positive integers $d_1 | \cdots | d_r$, and $r, d_1, \ldots, d_r$ are unique. It turns out that slightly more is true.

Theorem: Smith Normal Form

Let $M \in \mathsf{Mat}_{m \times n}(\mathbb{Z})$. There exist a sequence of integral elementary row and column operations that transform M to a matrix of the form

$$\left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right], \tag{20}$$

where $d_1 | \cdots | d_n$ are positive integers. Moreover, $r = \operatorname{rank}(M)$ and for all $i = 1, \ldots, r$, $d_i = d_i(M)/d_{i-1}(M)$. In particular, $r, d_1, \ldots, r_r$ are unique.

Definition i^{th} determinant divisor of M

For $i = 1, \ldots, \min\{m, n\}$, define

$$d_i(M) := \gcd\{\text{determinants of } i \times i \text{ minors of } M.\} \tag{21}$$

and define $d_0(M) = 1$. The number $d_i(M)$ is called the i^{th} determinant divisor of M.

Note that if $i < \operatorname{rank}(M)$, then $d_i(M) > 0$.

Integral Elementary Row Operations

There are three main operations:

- To interchange row i and row j, this is equivalent to multiplying on the left by $P_{i,j}$.
- To multiply row i by -1, we multiply on the left by D_i.
- To replace row i with row i plus k times row j, we multiply on the left by $E_{ij}(k)$.

Note that if we were to act on the columns instead, the elementary matrices should be multiplied on the right.

The integral elementary matrices $P_{ij}, D_i, E_{ij}(k)$ generate the group $\mathsf{GL}_n(\mathbb{Z})$.

Smith Normal Form Algorithm

If $M = 0$, we are done. Assume $M \neq 0$.

1. Let $\delta(M) = \min\{|M_{ij}| : M_{ij} \neq 0\}$. Choose $M_{ij} \neq 0$ such that $|M_{ij}| = \delta(M)$.
2. If M_{ij} does not divide an entry in its row, say $M_{i\ell}$, and $M_{i\ell} = gM_{ij} + r$ where $q, r \in \mathbb{Z}$ and $0 < r < |M_{ij}|$, then replace col$_\ell$ with col$_\ell - q$col$_j$:
3. This results in a matrix M' with $M'_{i\ell} = r$ and $\delta(M') \leq r < |M_{ij}| = \delta(M)$. Let M denote M' now. Go to the previous step.
4. If M_{ij} does not divide an entry in its column, we do the same thing analogous to the previous step.
5. If M_{ij} divides every entry in its row and column, we can clear the other entries in row i and column j using M_{ij} (i.e. all the other entries are 0). Let M denote the resulting matrix.
6. If M_{ij} divides every entry in M, skip this step. Otherwise, choose $M_{k\ell}$ such that $M_{ij} \nmid M_{k\ell}$. Then replace row i with row$_i$ + row$_j$. Let M denote the new matrix. Go to the first step.
7. M_{ij} divides every entry of M. Swap row 1 and row i and swap column 1 and column j. If $M_{ij} < 0$, multiply row by -1.

   We look at the resulting matrix M' in the bottom right corner inside the larger matrix. Let M denote M'.
8. Repeat steps 1 to 6 until M' in the previous step is the empty matrix.

Torsion Subgroup

Definition Torsion subgroup of A
Let A be an abelian group. For each $n \in \mathbb{Z}_{>0}$, we define the n-torsion subgroup of A to be

$$A[n] := \{a \in A : na = 0\} \tag{22}$$

we define the n-power torsion subgroup of A to be

$$A[n^\infty] := \left\{a \in A : n^k a = 0 \text{ for some } k \in \mathbb{Z}_{\geq 0}\right\} \tag{23}$$

and we define the torsion subgroup of A to be

$$\text{Tor}(A) := \{a \in A : ma = 0 \text{ for some } m \in \mathbb{Z}_{>0}\} = \bigcup_{n \in \mathbb{Z}_{>0}} A[n]. \tag{24}$$

Proposition 6

Let A be a finitely generated group. If $A \cong \mathbb{Z}^r \times T$, where $r \in \mathbb{Z}_{\geq 0}$ and T is a finite abelian group, then $T \cong \text{Tor}(A)$ and $\mathbb{Z}^r \cong A/\text{Tor}(A)$.

Consequently, T is unique up to isomorphism and r is unique.

Proof: First, note that if $\phi : B \to C$ is an isomorphism between abelian groups, then $\phi(\text{Tor}B) = \text{Tor}C$, so ϕ restricts to an isomorphism $\phi : \mathrm{Tor}B \to \mathrm{Tor}C$.

Let $\phi : A \to \mathbb{Z}^r \times T$ be an isomorphism as in the proposition statement.

Since $\mathrm{Tor}(\mathbb{Z}^r \times T) = \{(0, \ldots, 0)\} \times T \cong T$, we have $\mathrm{Tor}(A) \cong \{0\} \times T \cong T$.

Also since $\phi(\mathrm{Tor}A) = \{0\} \times T$, the map

$$\begin{aligned} A/\mathrm{Tor}A &\to \mathbb{Z}^r \times T/(\{0\} \times T) \\ a + \mathrm{Tor}A &\mapsto \phi(a) + (\{0\} \times T) \end{aligned}$$

is a well defined isomorphism. Therefore,

$$\begin{aligned} A/\mathrm{Tor}A &\cong \mathbb{Z}^r \times T/(\{0\} \times T) \\ &\cong \mathbb{Z}^r/\{0\} \times T/T \\ &\cong \mathbb{Z}^r \times \{0\} \\ &\cong \mathbb{Z}^r \end{aligned}$$

■

■ Proposition 7

Let A be a finitely generated abelian group. If $A \cong \mathbb{Z}^r \times P \times B$, where $r \in \mathbb{Z}_{\geq 0}$, P is a finite abelian group with $|P| = p^k$ for some prime p, and B is a finite abelian group with $p \nmid |B|$, then

$$A[p^\infty] \cong P \tag{25}$$