7. Abelian groups.

A. Ushakov

MA503, March 9, 2022

Contents

Today we discuss finitely generated abelian groups and related topics.

- Matrices.
- Elementary matrix operations.
- Product.
- Row echelon form.
- Elementary row/column operations.
- Smith normal form.
- Free abelian groups.
- Free abelian groups: classification.
- Change of basis for an abelian group.
- Subgroups of a free abelian group.
- Classification of finitely generated abelian groups.
- Algebraic structure of U_n.

Matrix notation. Elementary operations on matrices.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{bmatrix}$$

Definition

An $m \times n$ **matrix** A is an $m \times n$ array of numbers (or other objects). In particular,

- A has m rows;
- A has n columns;

Notation. (a_{ij}) *or* $(a_{ij})_{m\times n}$ *– defines a matrix with entries* a_{ij}*.*

Definition

We say that matrices $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{m\times n}$ are **equal** if they have the same entries, i.e., $a_{ij} = b_{ij}$ for each i, j.

Consider two $m \times n$ matrices $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{m\times n}$ and a constant (scalar) k.

Sum *of* A *and* B *is a new matrix* $C = A + B = (a_{ij} + b_{ij})_{m\times n}$.

Scalar product *of* k *and* A *is a new matrix* $kA = (ka_{ij})_{m\times n}$.

Matrix notation. Elementary operations on matrices.

$$I = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & & & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & & & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

Definition

The $n \times n$ **identity matrix** I_n is the matrix $(\delta_{ij})_{n\times n}$, where δ_{ij} is the **Kronecker delta** defined as follows:

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Definition

Zero $m \times n$ **matrix** is defined by $(0)_{m\times n}$.

Definition

A **column matrix** is an $m \times 1$ matrix.

Definition

A **row matrix** is an $1 \times n$ matrix.

An $m \times n$ matrix can be viewed as

- a system of m rows,
- a system of n columns.

Product of matrices

Product of matrices $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{n\times k}$ is a new matrix $C = (c_{ij})_{m\times k}$ defined by $c_{ij} = a_{i1}a_{1j} + \ldots + a_{in}a_{nj}$ which can be recognized as dot product of the ith row in A and jth column in B

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1j} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2j} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{ij} & \ldots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mj} & \ldots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1j} & \ldots & b_{1k} \\ b_{21} & b_{22} & \ldots & b_{2j} & \ldots & b_{2k} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{i1} & b_{i2} & \ldots & b_{ij} & \ldots & b_{ik} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{nj} & \ldots & b_{nk} \end{bmatrix} = (c_{ij})_{m\times k}.$$

In general, $AB \neq BA$.

For instance,

$$\begin{bmatrix} 1 & 2 \\ -1 & 3 \\ 0 & 5 \end{bmatrix} \cdot \begin{bmatrix} -3 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 5 \\ 6 & 5 \\ 5 & 10 \end{bmatrix}$$

The product below makes no sense (incompatible dimensions)

$$\begin{bmatrix} -3 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ -1 & 3 \\ 0 & 5 \end{bmatrix}$$

Matrices: row echelon form

Definition

A matrix is in **row echelon form** if

1. all nonzero rows (rows with at least one nonzero element) are above any rows of all zeroes (all zero rows, if any, belong at the bottom of the matrix), and
2. the **leading coefficient** (the first nonzero number from the left, also called the **pivot**) of a nonzero row is always strictly to the right of the leading coefficient of the row above it (some texts add the condition that the leading coefficient must be 1).

For instance, the following matrix is in row echelon form:

$$\begin{bmatrix} 1 & a_0 & a_1 & a_2 & a_3 \\ 0 & 0 & 2 & a_4 & a_5 \\ 0 & 0 & 0 & 1 & a_6 \end{bmatrix}$$

Many properties of matrices (e.g. the rank) can be easily deduced from their row echelon form.

Gaussian elimination *(or* **row reduction***) is a process of reducing a given matrix to a row echelon form.*

Matrices: elementary row/column operations

(Elementary row operations)

- **Row addition**: *a row can be replaced by the sum of that row and a integer-multiple of another row.*
- **Row switching**: *switch two rows.*
- **Row inversion**: *multiply a row by* -1.

We use elementary row operations to reduce the matrix to a row echelon form.

(Elementary column operations)

- **Column addition**: *a column can be replaced by the sum of that column and a integer-multiple of another column.*
- **Column switching**: *switch two column.*
- **Column inversion**: *multiply a column by* -1.

Elementary column operations correspond to change of basis, discussed later.

Smith normal form

$$\begin{pmatrix} \alpha_1 & & & & & \\ & \alpha_2 & & & 0 & \\ & & \ddots & & & \\ & & & \alpha_k & & \\ & & & & 0 & \\ & 0 & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

Definition

A diagonal $k \times n$ matrix shown on the left is in **Smith normal form** if

- $\alpha_i \geq 0$
- $\alpha_i \mid \alpha_{i+1}$.

Proposition

Any matrix M with entries from $\mathbb{Z}$ can be transformed into Smith normal form using elementary row and column operations.

First, it is proved that any matrix M can be transformed into a matrix of the form shown on the right, where α_1 divides every $y_{i,j}$. Then the proof goes by induction on dimensions of M.

$$\begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & y_{2,2} & \dots & y_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & y_{k,2} & \dots & y_{k,n} \end{pmatrix}$$

(Uniqueness of Smith normal form)

There are infinitely many ways to transform a given M to a Smith normal form. The result is always the same.

Smith normal form: example

Consider the matrix below (denote columns x_1, x_2, x_3 and rows y_1, y_2, y_3)

$$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 10 \end{pmatrix}$$

Applying elementary column/row operations we get matrices:

$$\overset{y_1 \leftarrow y_1 + y_2}{\longrightarrow} \begin{pmatrix} 6 & 8 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 10 \end{pmatrix} \overset{x_2 \leftarrow x_1 + x_2}{\longrightarrow} \begin{pmatrix} 6 & 2 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 10 \end{pmatrix} \overset{x_1 \leftrightarrow x_2}{\longrightarrow} \begin{pmatrix} 2 & 6 & 0 \\ 8 & 0 & 0 \\ 0 & 0 & 10 \end{pmatrix}$$

$$\overset{y_2 \leftarrow y_2 - 4y_1}{\longrightarrow} \begin{pmatrix} 2 & 6 & 0 \\ 0 & -24 & 0 \\ 0 & 0 & 10 \end{pmatrix} \overset{x_2 \leftarrow x_2 - 3x_1}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -24 & 0 \\ 0 & 0 & 10 \end{pmatrix} \overset{x_2 \leftarrow -x_2}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & 10 \end{pmatrix}$$

In a similar way we get

$$\rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 120 \end{pmatrix}$$

The obtained matrix is in the Smith normal form.

Free abelian groups

Definition

An abelian group G is called a **free abelian group** if it has a subset $X \subseteq G$ such that $G = \langle X \rangle$ and for all distinct $x_1, \ldots, x_n \in X$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 0 \quad \Leftrightarrow \quad \alpha_1 = \ldots = \alpha_n = 0.$$

Such set X is called a **free basis** for G.

- The trivial group is free abelian.
- $\mathbb{Z}$ is a free abelian group. It has two free bases: $\{1\}$ and $\{-1\}$.
- $\mathbb{Z}^n$ is a free abelian group. The standard basis for $\mathbb{Z}^n$ is $\{e_1, \ldots, e_n\}$, where

$$\begin{cases} e_1 = (1, 0, 0, \ldots, 0) \\ e_2 = (0, 1, 0, \ldots, 0) \\ \ldots \\ e_n = (0, 0, 0, \ldots, 1). \end{cases}$$

- $\mathbb{Z}_5$ is not free abelian because $5a =_{\mathbb{Z}_5} 0$ for every $a \in \mathbb{Z}_5$. Therefore, no element $a \in \mathbb{Z}_5$ can be a part of a free basis for $\mathbb{Z}_5$.

If $X = \{x_1, \ldots, x_n\}$ is a free basis for abelian G, then every $g \in G$ can be uniquely expressed as $g = \alpha_1 x_1 + \ldots + \alpha_n x_n$.

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = \beta_1 x_1 + \ldots + \beta_n x_n \quad \Leftrightarrow \quad (\beta_1 - \alpha_1) x_1 + \ldots + (\beta_n - \alpha_n) x_n = 0.$$

Free abelian groups: classification

If $X = \{x_1, \ldots, x_n\}$ is a basis of a free abelian group G. Then $G \simeq \mathbb{Z}^n$.

$\varphi : \mathbb{Z}^n \to G$ defined by $(\alpha_1, \ldots, \alpha_n) \overset{\varphi}{\mapsto} \alpha_1 x_1 + \ldots + \alpha_n x_n$ is an isomorphism.

$\mathbb{Z}^m \simeq \mathbb{Z}^n$ if and only if $m = n$.

$\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}_2) = 2^n$.

Corollary

All free bases for G have the same size n. The number n is called the **rank** *of G.*

Change of basis for an abelian group

Suppose $G = \langle x_1, \ldots, x_n \rangle$ is abelian. We treat $x_1, \ldots, x_n$ as a sequence here. Then

(B1) $\{\ldots, x_{i-1}, x_i + cx_j, x_{i+1}, \ldots\}$ *is a basis for* G.

$$\begin{aligned} v &= \alpha_1 x_1 + \ldots + \alpha_n x_n && \text{in original basis} \\ &= \alpha_1 x_1 + \ldots + \alpha_i(x_i + cx_j) + \ldots + (\alpha_j - c\alpha_i)x_j + \alpha_n x_n && \text{in new basis.} \end{aligned}$$

(B2) $\{\ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots\}$ *is a basis for* G.

$$\begin{aligned} v &= \alpha_1 x_1 + \ldots + \alpha_n x_n && \text{in original basis} \\ &= \alpha_1 x_1 + \ldots + \alpha_j x_j + \ldots + \alpha_i x_i + \ldots + \alpha_n x_n && \text{in new basis.} \end{aligned}$$

(B3) $\{\ldots, x_{i-1}, -x_i, x_{i+1}, \ldots\}$ *is a basis for* G.

$$\begin{aligned} v &= \alpha_1 x_1 + \ldots + \alpha_n x_n && \text{in original basis} \\ &= \alpha_1 x_1 + \ldots - \alpha_i(-x_i) + \ldots + +\alpha_n x_n && \text{in new basis.} \end{aligned}$$

$\mathbb{Z}^n$ has infinitely many bases (if $n \geq 2$). The **standard basis** is the set $\{e_1, \ldots, e_n\}$.

Transformations (B1), (B2), (B3) are reversible. Hence, the following are equivalent

- *we can transform a basis* $\{x_1, \ldots, x_n\}$ *into a basis* $\{y_1, \ldots, y_n\}$,
- *we can transform a basis* $\{y_1, \ldots, y_n\}$ *into a basis* $\{x_1, \ldots, x_n\}$.

Changing to any basis

Theorem

Every free basis for $\mathbb{Z}^n$ can be obtained by a sequence of transformations (B1), (B2), (B3) starting from the standard basis $\{e_1, \ldots, e_n\}$.

$$\begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \ldots & x_{nn} \end{pmatrix}$$

For a free basis $\{x_1, \ldots, x_n\}$ construct a matrix M of row-vectors $\{x_1, \ldots, x_n\}$. We prove that we can transform the basis $\{x_1, \ldots, x_n\}$ into $\{e_1, \ldots, e_n\}$ and its matrix to I.

$$\begin{aligned} e_1 \in \langle x_1, \ldots, x_n \rangle &\Rightarrow e_1 = \alpha_1 x_1 + \ldots + \alpha_n x_n \\ &\Rightarrow 1 = \alpha_1 x_{11} + \ldots + \alpha_n x_{n1} \\ &\Rightarrow 1 = \gcd(x_{11}, \ldots, x_{n1}). \end{aligned}$$

Hence, we can get the matrix on the right

$$\begin{pmatrix} 1 & y_{12} & \ldots & y_{1n} \\ 0 & y_{22} & \ldots & y_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & y_{n2} & \ldots & y_{nn} \end{pmatrix} \begin{matrix} = y_1 \\ = y_2 \\ \vdots \\ = y_n \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & y_{22} & \ldots & y_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & y_{n2} & \ldots & y_{nn} \end{pmatrix}$$

$(0, y_{12}, \ldots, y_{1n}) = \beta_2 y_2 + \ldots + \beta_n y_n$ for some $\beta_1, \ldots, \beta_n \in \mathbb{Z}$.

Hence, using (B1) transformations we can get the matrix on the left.

Proceed by induction to get I.

Subgroup of a free abelian group is free abelian

Fix $H \leq \mathbb{Z}^n$.

If $\overline{a} = (a_1, \ldots), \overline{b} = (b_1, \ldots) \in H$ with $a_1, b_1 \neq 0$, then there is $(\gcd(a_1, b_1), \ldots) \in H$.

$\gcd(a_1, b_1) = \alpha a_1 + \beta b_1$ for some $\alpha, \beta \in \mathbb{Z}$. Hence, $\alpha\overline{a} + \beta\overline{b} = (\gcd(a_1, b_1), \ldots) \in H$.

$H \leq \mathbb{Z}^n$ is free abelian of rank at most n .

Induction on n.

- Find any $\overline{a} = (a_1, \ldots) \in H$ with the least positive a_1.
- Let $H_1 = \{\overline{r} \in H \mid \overline{r} = (0, r_1, \ldots)\} \leq H$. Dropping the first zero, H_1 is a subgroup of $\mathbb{Z}^{n-1}$. By induction, H_1 has a free basis $\{\overline{r}_1, \ldots, \overline{r}_m\}$.
- Then for any $\overline{b} = (b_1, \ldots) \in H$ we have $b_1 = qa_1$ and $\overline{b} = q\overline{a} + \overline{r}$ for some $\overline{r} \in H_1$. Notice that q is uniquely defined.
- Hence, $\{\overline{a}, \overline{r}_1, \ldots, \overline{r}_m\}$ is a free basis of H. □

The obtained system of row vectors $\{\overline{a}, \overline{r}_1, \ldots, \overline{r}_m\}$ defines a matrix M_H. By construction, M_H is in row echelon form.

Our next goal: Show that for every $H \leq \mathbb{Z}^n$ we can find a basis for $\mathbb{Z}^n$ in which H has a very simple description. We can manipulate with the description of H as follows:

- *change basis for H (elementary row transformations of M_H),*
- *change basis for $\mathbb{Z}^n$ (elementary column transformations of M_H).*

Changing bases for $\mathbb{Z}^n$ and H

Applying transformations (B1), (B2), (B3) to the basis of H we can get any other basis of H. Each transformation changes M_H as follows:

- (B1) performs row addition.
- (B2) performs row switching.
- (B3) performs row inversion.

Applying transformations (B1), (B2), (B3) to the basis of $\mathbb{Z}^n$ we can get any other basis of $\mathbb{Z}^n$. Each transformation changes M_H as follows:

- (B1) performs column addition.
- (B2) performs column switching.
- (B3) performs column inversion.

Changing the bases for $\mathbb{Z}^n$ and H we can transform M_H to its Smith normal form.

M_H encodes the generators of H. Thus, for any $H \leq \mathbb{Z}^n$ we can find a basis for $\mathbb{Z}^n$ such that

$$H = \langle \alpha_1 e_1, \ldots, \alpha_k e_k, 0 \ldots \rangle,$$

where $\alpha_i \mid \alpha_{i+1}$.

Abelian groups: classification

Let $G = \langle x_1, \ldots, x_n \rangle$ be an abelian group. $\overline{r} = (\alpha_1, \ldots, \alpha_n)$ is called a **relation** in G if
$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 0.$$

The set of relations R in G is a subgroup of $\mathbb{Z}^n$.

- $\overline{0}$ is a relation;
- if $\overline{r}$ is a relation, then $-\overline{r}$ is a relation;
- if $\overline{r}_1, \overline{r}_2$ are relations, then $\overline{r}_1 + \overline{r}_2$ is a relation.

We've seen before that changing the bases we can get a very easy description of R. As a consequence we get $\{y_1, \ldots, y_n\}$ for G in which
$$\alpha_1 y_1 = 0, \alpha_2 y_2 = 0, \ldots, \alpha_k y_k = 0$$

Theorem

If G is a finitely generated abelian group, then $G \simeq \mathbb{Z}_{\alpha_1} \times \ldots \times \mathbb{Z}_{\alpha_k} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$, where $\alpha_i \mid \alpha_{i+1}$.

Corollary

If G is a finitely generated abelian group, then
$$G \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}} \times \mathbb{Z} \times \ldots \times \mathbb{Z},$$
where p_i are prime numbers (some of them can be equal) and $a_i \in \mathbb{Z}$.

Algebraic structure of U_n

Theorem

The following holds:

- U_2 *is trivial.*
- $U_4 \simeq \mathbb{Z}_2$.
- $U_{2^k} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$.
- $U_{p^k} \simeq \mathbb{Z}_{p^{k-1}(p-1)}$ *for an odd prime* p.

Lemma

$\gcd(n, m) = 1 \quad \Rightarrow \quad U_{nm} \simeq U_n \times U_m$.

$$a \in U_{mn} \quad \Leftrightarrow \quad \gcd(a, mn) = 1 \quad \Leftrightarrow \quad \begin{matrix} \gcd(a, m) = 1 \\ \gcd(a, n) = 1 \end{matrix} \quad \Leftrightarrow \quad \begin{matrix} a \in U_m \\ a \in U_n \end{matrix}$$

That defines a map $\varphi : U_{mn} \to U_n \times U_m$ as $a \mapsto (a, a)$, which is an isomorphism.

Corollary

If $\mathrm{PPF}(n) = p_1^{k_1} \dots p_s^{k_s}$, *then* $U_n \simeq U_{p_1^{k_1}} \times \dots \times U_{p_s^{k_s}}$.