A FIRST COURSE

IN

ABSTRACT ALGEBRA

A FIRST COURSE

IN

ABSTRACT ALGEBRA

MAT3004 Notebook

Dr. Guang Rao

The Chinese University of Hongkong, Shenzhen

香港中文大學（深圳）
The Chinese University of Hong Kong, Shenzhen

Contents

Acknowledgments

This book is from the MAT3004 in fall semester, 2018.

CUHK(SZ)

Notations and Conventions

$\mathbb{R}^n$	n-dimensional real space
$\mathbb{C}^n$	n-dimensional complex space
$\mathbb{R}^{m\times n}$	set of all $m \times n$ real-valued matrices
$\mathbb{C}^{m\times n}$	set of all $m \times n$ complex-valued matrices
x_i	ith entry of column vector $\boldsymbol{x}$
a_{ij}	(i,j)th entry of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i$	ith column of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i^{\mathrm{T}}$	ith row of matrix $\boldsymbol{A}$
$\mathbb{S}^n$	set of all $n \times n$ real symmetric matrices, i.e., $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ and $a_{ij} = a_{ji}$ for all i,j
$\mathbb{H}^n$	set of all $n \times n$ complex Hermitian matrices, i.e., $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ and $\bar{a}_{ij} = a_{ji}$ for all i,j
$\boldsymbol{A}^{\mathrm{T}}$	transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{T}}$ means $b_{ji} = a_{ij}$ for all i,j
$\boldsymbol{A}^{\mathrm{H}}$	Hermitian transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{H}}$ means $b_{ji} = \bar{a}_{ij}$ for all i,j
$\mathrm{trace}(\boldsymbol{A})$	sum of diagonal entries of square matrix $\boldsymbol{A}$
$\mathbf{1}$	A vector with all 1 entries
$\mathbf{0}$	either a vector of all zeros, or a matrix of all zeros
$\boldsymbol{e}_i$	a unit vector with the nonzero element at the ith entry
$\mathcal{C}(\boldsymbol{A})$	the column space of $\boldsymbol{A}$
$\mathcal{R}(\boldsymbol{A})$	the row space of $\boldsymbol{A}$
$\mathcal{N}(\boldsymbol{A})$	the null space of $\boldsymbol{A}$
$\mathrm{Proj}_{\mathcal{M}}(\boldsymbol{A})$	the projection of $\boldsymbol{A}$ onto the set $\mathcal{M}$

Chapter 3

Week3

3.1. Tuesday

Definition 3.1 [Cartesian Product]

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in S_i\}$$

Theorem 3.1 $\prod_{i=1}^{n} G_i$ is a group under the operation

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

Proof.

- It's obvious that the operation is closed.
- Check inverse and identity.

$$\text{identity} = (e_1, e_2, \ldots, e_n)$$

- Check the operation is associate:

$$\begin{aligned}
[(g_1, \ldots, g_n)(h_1, \ldots, h_n)](k_1, \ldots, k_n) &= (g_1 h_1, \ldots, g_n h_n)(k_1, \ldots, k_n) \\
&= (g_1 h_1 k_1, \ldots, g_n h_n k_n) \\
&= (g_1, \ldots, g_n)(h_1 k_1, \ldots, h_n k_n) \\
&= (g_1, \ldots, g_n)[(h_1, \ldots, h_n)(k_1, \ldots, k_n)]
\end{aligned}$$

■

Ⓡ If the operation of each G_i is the **addition**, then

$$\prod_{i=1}^{n} G_i := \oplus_{i=1}^{n} G_i$$

■ **Example 3.1** 1. $G = (S_3 \times \mathbb{Z}_2, \cdot)$ is not abelian, e.g.,

$$((12),0) \cdot ((23),0)$$

2. $G = (\mathbb{Z}_2 \times \mathbb{Z}_3, +) = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic

$$d(1,1) = (0,0) \implies d = 6k$$

3. The **Klein** 4-group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic

$$d(x,y) = (0,0)$$

■

Theorem 3.2 $G = \mathbb{Z}_m \times \mathbb{Z}_n$ is **cyclic** iff $gcd(m,n) = 1$.

Proof. Let $k = lcn(m,n) = \frac{mn}{gcd(m,n)} \leq mn$.

Necessity. Consider $(a,b) \in G$:

$$k(a,b) = (ka,kb) := (msa,ntb) = (0,0),$$

i.e., $|(a,b)| \leq k$. In particular, $mn \leq k$, thus $k = mn$, i.e., $gcd(m,n) = 1$.

Sufficiency. Consider $(1,1) \in G$: $d(1,1) = (0,*) \implies d = xm$; and $d(1,1) = (*,0) \implies d = yn$. Thus $|(1,1)| = lcm(m,n) = mn$, i.e., this group is cyclic. ■

Corollary 3.1 $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic iff (m_i, m_j) are mutually coprime.

Definition 3.2 Let G be a group, S a non-empty subset.

$$< S > := \{a_1^{m_1}, \ldots, a_n^{m_n} \mid n \in \mathbb{Z}^+, m_i \in \mathbb{Z}, a_i \in S\}$$

If S is finite, then $< S >$ is **finitely generated**.

Verify that this is a group, i.e., a subgroup of G. Note that a_i's need not to be distinct. e.g.,

$$S = \{a, b\} \implies a^{-1}bab^2 \in < S >$$

Proposition 3.1

$$< S > = \bigcap_{\{H \mid S \subseteq H \subseteq G\}} H$$

Example 3.2

1. $< \text{cycles in } S_n > = S_n = < \text{transpositions} >$
2. $S_n = < (12), (1, 2, \ldots, n) >$.

   hint: $(i, i+1) \in S_n, (i, j) \in S_n$
3. $D_n = < r, s >$

Proposition 3.2 $\mathbb{Q}$ is not finitely generated.

Theorem 3.3 — **Fundamental Theorem of Finitely Generated Abelian Groups.** Any finitely generated abelian group (is isomorphic to)

$$\prod_{i=1}^{m} \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}^n,$$

$r_i, n \in \mathbb{N}$.

■ **Example 3.3** abelian group of order $360 = 2^3 3^2 5$:

$$G_2 \times G_3 \times G_5$$

$G_5 = \mathbb{Z}_5$, $G_3 = \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8$.

Thus there are 6 possible abelian groups of order 360. ■

How about abelian group of order 7^5?

Definition 3.3 [Partition] Let $S \neq \emptyset$. A **partition** P of S is $\{S_i \mid i \in I\}$ such that

1. $S_i \neq \emptyset, \forall i \in I$
2. $S_i \bigcap S_j = \emptyset, \forall i \neq j$
3. $\bigcup_{i \in I} S_i = S$

Also, we denote $S = \bigsqcup_{i \in I} S_i$ ■

Definition 3.4 [Equivalence Relation] An **equivalence relation** on S is a relation $\sim$ such that

1. Reflexive: $a \sim a, \forall a \in S$
2. Symmetric: $a \sim b$ implies $b \sim a$
3. Transitive: $a \sim b, b \sim c$ implies $a \sim c$.

■

Equivalence relation is essentially the same meaning of partition:

- Partition implies equivalence relation: Define $a \sim b$ if $a, b \in S_i$
- Equivalence relation implies partition: Define $C_a := \{b \in S \mid b \sim a\}$. (For the symmeticity part, show that $C_a \bigcap C_b \neq \emptyset$ implies $C_a = C_b$.)

We call C_a the **equivalence class** with the representative a. If $b \in C_a$, then $C_b = C_a$, so any element in an equivalence class can be its representative.

Proposition 3.3 Any $\sigma \in S_n$ is a product of disjoint cycles.

Proof. Given $a, b \in X = \{1, 2, \ldots, n\}$, define $a \sim b$ if $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$. ■