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 2

Week2

2.1. Tuesday

2.1.1. Review

Note that a group has the property of closeness, associatity, identity and its inverse

2.1.2. Cyclic groups

Definition 2.1 [Ablian] Let $(\mathcal{G}, *)$ be a group, it is said to be **ablian** if

$$a * b = b * a, \quad \forall a, b \in \mathcal{G}$$

Definition 2.2 [Order] Let $\mathcal{G}$ be a group with the identity e. The **order** if an element $g \in \mathcal{G}$ is denoted by $|g|$, i.e., the smallest $n \in \mathbb{N}^+$ such that $g^n = e$. If $|g| = \infty$, then g has **infinite order**.

Definition 2.3 [Periodic Group] A group is said to be

1. **periodic** (torsion) if every element from this group is of finite order.
2. **torsion-free** if every non-identity has infinite order.

Note that not torsion is not equivalent to torsion-free; not torsion-free is not equivalent to torsion.

Proposition 2.1 If $|\mathcal{G}| < \infty$, then $|g| < \infty$ for $\forall g \in \mathcal{G}$.

Proof. If $|g| = \infty$, then

$$\{e, g, g^2, \cdots, g^n, \dots\} \subseteq \mathcal{G},$$

which implies $|\mathcal{G}| = \infty$. ∎

Proposition 2.2 Let $\mathcal{G}$ be a group with identity e. If $g^n = e$ for some $n \in \mathbb{N}^+$, then $|g| | n$.

Proof. Let $m := |g| \leq n$. Recall the ideas from discrete mathematics:

Theorem 2.1 — well-ordering principle. Any $S \subseteq \mathbb{N}$ has a least element (Axiom).

Theorem 2.2 — Division Theorem. For $\forall m \in \mathbb{Z}$ and $n \in \mathbb{N}^+$, there always $\exists\ q, r \in \mathbb{Z}$ such that

$$m = nq + r,$$

where $0 \leq r < n$.

Note that the power g^n can be rewritten as:

$$g^n := g^{mq+r} = (g^m)^q \cdot g^r = e.$$

Since $(g^m)^q$ equals to e, we imply $g^r = e, r < m$, i.e., $r = 0$. ∎

R Not that the condition $n \in \mathbb{N}^+$ can be relaxed into $n \in \mathbb{Z}$.

Definition 2.4 [cyclic] A group $\mathcal{G}$ is **cyclic** if there $\exists g \in \mathcal{G}$ such that for $\forall x \in \mathcal{G}$, there always $\exists n \in \mathbb{Z}$ such that

$$x = g^n.$$

We rewrite the group as $\mathcal{G} = < g >$, we call g as the **generator** of $\mathcal{G}$. The notation $< g >$

means:

$$< g > := \{\cdots, g^{-2}, g^{-1}, e.g, g^2, \cdots\}$$

Proposition 2.3 Given a group $\mathcal{G}$ and $g \in \mathcal{G}$, we have $| < g > | = |g|$.

Proof.
- If $|g| = \infty$, the result is trivial.
- If $|g| = n$, we imply $| < g > | = |\{e, g, \ldots, g^{n-1}\}| = n$.

∎

Definition 2.5 Let $a, b \in \mathbb{Z}$ not all zero. The greatest common divisor is defined as:

$$\text{gcd}(a, b) := \text{the greatest integer that divides } a \text{ and } b.$$

Theorem 2.3 — Bezout. Provided with $a, b \in \mathbb{Z}$ not all zero. Then there exists $s, t \in \mathbb{Z}$ such that

$$sa + tb = \text{gcd}(a, b)$$

Example 2.1
1. $(\mathbb{Z}, +)$ is **cyclic** with generator ± 1
2. $(\mathbb{Z}_n, +) =< k >$, where $\text{gcd}(k, n) = 1$. This is because we can always find $s > 0$ and $t < 0$ such that $sa + tb = 1$, i.e.,

$$1 = \underbrace{k + \cdots + k}_{s \text{ terms}} \in \mathbb{Z}_n$$

3. $(u_m, \cdot) =< \xi_m^k >$, where $\xi_m = \exp(\frac{2\pi i}{m})$ and $\text{gcd}(k, m) = 1$. This is because we can similarly consturct $s > 0$ s.t. $(\xi_m^k)^s = \xi_m$.

Proposition 2.4 Every cyclic group is abelian.

Proof. As $\mathcal{G} =< g >$, for $\forall x, y \in \mathcal{G}$, we have

$$x \cdot y = g^m \cdot g^n = g^{m+n} = g^n \cdot g^m = y \cdot x.$$

■

R The converse of proposition(2.4) is not true. For example, $(\mathbb{Q}, +)$ is abelian, but it is not cyclic, i.e., if $(\mathbb{Q}, +) =< \frac{n}{m} >$, we find $\frac{n}{2m} \notin < \frac{n}{m} >$.

Definition 2.6 Let X be a set. A **permutation** of X is a **bijection** of X. We denote

$$\mathrm{Sym}(X) = \{\text{all permutations of } X\}$$

Proposition 2.5 $\mathrm{Sym}(X)$ is a group under composition operation.

Proof.

1. For $\forall \alpha, \beta \in \mathrm{Sym}(X)$, we have $\alpha \circ \beta \in \mathrm{Sym}(X)$ as the composition of bijections is also bijection.
2. For $\forall \alpha, \beta, \gamma \in \mathrm{Sym}(X)$, we have $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.
3. identity = id∈Sym(X)
4. For $\forall \sigma \in \mathrm{Sym}(X)$, we choose $\rho \in \mathrm{Sym}(X)$ s.t.

$$\rho : \sigma(x) \mapsto x, \forall x \in X$$

It follows that $\rho \circ \sigma = \mathrm{id}$, since

$$\sigma \circ \rho(\sigma(x)) = \sigma(\rho \circ \sigma(x)) = \sigma(x)$$

■

Let $X = \{1,2,\dots,n\}$, we denote $\mathbb{S}_n = \mathrm{Sym}(X)$. Describe $\sigma \in \mathbb{S}_n$ by:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Note that $|\mathbb{S}_n| = n!$

■ **Example 2.2** Consider $\mathcal{G} := \mathbb{S}_3$, then $\sigma, \beta \in \mathcal{G}$:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} := (1,2,3) \qquad \beta := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} := (1,2)$$

Then we compute the composite $\sigma \circ \beta$:

$$\sigma \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

and $\beta \circ \sigma$:

$$\beta \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

and $\sigma \circ \sigma \circ \sigma$:

$$\sigma \circ \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}^3 = \mathrm{id},$$

which is said to be **3-cycle**, which will be talked in future. ■

(R) In general, $\mathbb{S}_n$ is not **ablian** for $n \geq 3$.

In general, we write the k-cycle permutation as:

$$\alpha = (i_1, \dots, i_k)$$

where $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_k \mapsto i_1$.

■ **Example 2.3** Consider $\sigma = (15)(246) \in \mathbb{S}_6$, i.e.,

$$\sigma = 1 \mapsto 5 \mapsto 1; \qquad 2 \mapsto 4 \mapsto 6 \mapsto 2; \qquad 3 \mapsto 3$$

and $\alpha = (13)(45) \in \mathbb{S}_6$. We study the composition $\sigma \circ \alpha$:

$$\sigma \circ \alpha = [(15)(246)] \circ [(13)(45)] = (135624)$$

and

$$\alpha \circ \sigma = (13)(45)(15)(246) = (146253)$$

■

Proposition 2.6 Each $\sigma \in \mathbb{S}_n$ is either a cycle or a product of disjoint cycle.

Disjoint cycles commute with one another.

Definition 2.7 2-cycle is called a **transposition** ■

Proposition 2.7 $\sigma \in \mathbb{S}_n$ can be written as a product of transpositions.

Proof. Due to proposition(2.6) and

$$(i_1 i_2 \cdots i_k) = (i_1 i_k) \cdots (i_1 i_3)(i_1 i_2)$$

■

For $\sigma \in \mathbb{S}_n$, we have

$$\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$$