A JOURNEY

IN

PURE MATHEMATICS

A JOURNEY

IN

PURE MATHEMATICS

MAT3006 & 3040 & 4002 Notebook

Dr. Daniel Wong

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 MAT3006,MAT3040,MAT4002 in spring semester, 2018-2019.

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 1

Week1

1.1. Monday

1.1.1. Introduction to Abstract Algebra

$$\left[\begin{array}{cc|c} 1 & 2 & 5 \\ 4 & 5 & 14 \end{array}\right] \Longrightarrow \left[\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & -3 & -6 \end{array}\right] \Longrightarrow \left[\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & 1 & 2 \end{array}\right] \Longrightarrow \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right].$$

The basic concepts include **groups, rings, fields**.

One topic is algebra, i.e., the solvability of polynomials. (From Galois Theory to analysis)

$$\text{Example: } \frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}\boldsymbol{x}} = g(\boldsymbol{x}) \implies D\boldsymbol{y} = g(\boldsymbol{x})$$

with operatior $D := \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{x}}$. The operator D forms a ring, i.e.,

$$\{a_n(x)D^n + a_{n-1}(x)D^{n-1} + \cdots + a_0(x)\} \mapsto \text{ring}$$

Second topic is number theory

Third topic is geometry, including *algebraic geometry, differential geometry, topology, finite geometry, affine geometry, algebraic graph theory,, combinatorics*, with applications to coding theory, physics, crystallography chemestry.

1.1.2. Group

Definition 1.1 [Group] A group $\mathcal{G}$ is a set equipped with a binary operation, i.e.,

$$* : \quad \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}$$

such that:

1. Associativity: $(a * b) * c = a * (b * c)$ for $\forall a, b, c \in \mathcal{G}$.
2. Existence of Identity: $\exists$ an identity $e \in \mathcal{G}$ s.t. $e * g = g * e = g$ for $\forall g \in \mathcal{G}$.
3. Existence of Inverse: $\forall g \in \mathcal{G}$, there exists an inverse g^{-1} s.t. $g^{-1} * g = g * g^{-1} = e$.

The size(order) of $\mathcal{G}$ is denoted by $|\mathcal{G}|$. ∎

R

- If $a * b = b * a$ for $\forall a, b$, then $\mathcal{G}$ is called an **abelian group**.
- If $|\mathcal{G}| = 1$, then $\mathcal{G}$ is said to be **trivial**, otherwise $\mathcal{G}$ is **nontrivial**.
- Similarly, the ternary operation means:

$$* : \quad \mathcal{G} \times \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}$$

- The semigroup definition only requires the (1) condition; and the menoid requies the (1) and (2) conditions.
- Is $\emptyset$ a group? By the second condition, it is not a group.

Given a set $\mathcal{S}$ with its associated operation $*$, to check $(\mathcal{S}, *)$ is a group, we need to check:

1. $\mathcal{S}$ is **closed** under the operation $*$, i.e., $a * b \in \mathcal{S}$ for $\forall a, b \in \mathcal{S}$
2. **Associativity**.
3. **Existence of Identity**
4. **Existence of Inverse**

Proposition 1.1 $(\mathbb{Q}, +)$ is a group.

Proof. 1. For $\forall a, b \in \mathbb{Q}$, it is easy to show $a + b \in \mathbb{Q}$.

2. Associativity: $(a+b)+c=a+(b+c)$ for $\forall a,b\in\mathbb{Q}$
3. Existence of Identity: Take the identity $0\in\mathbb{Q}$, we have $0+a=a+0=a$ for $\forall a\in\mathbb{Q}$.
4. Existence of Inverse: For $\forall a\in\mathbb{Q}$, it follows that $(-a)\in\mathbb{Q}$ s.t. $(-a)+a=a+(-a)=0$.

■

Note that $(\mathbb{Q},\cdot)$ is not a group since inverse does not exist.

R Note that the existence of identity is unique, which will be shown in the future.

Proposition 1.2 $(u_m,\cdot)$ is a group, where

$$u_m=\{1,\xi^m,\ldots,\xi_m^{m-1}\}$$

with $\xi^m=1$ and $\xi\neq 1$.

Proof.
1. Note that for $\forall\xi^j,\xi^k\in u_m$, we have

$$\xi^j\cdot\xi^k:=\xi^{j+k}=\begin{cases}\xi^{j+k}, j+k\leq m-1\\ \xi^{j+k-m}, j+k\geq m\end{cases}$$

2. The associativity is easy to show.
3. Take the identity $e=1$.
4. For $\forall\xi^k\in u_m$, we take the inverse ξ^{m-k}.

■

Proposition 1.3 The set $\mathcal{G}=\{\text{bijections of }\mathbb{R}\}$ associated with the **conposition** operator is a group.

Definition 1.2 [bijection] The bijection contains **injective**, i.e., $f(x)=f(y)$ implies $x=y$; and **supjective**, i.e., $\forall y\in\mathcal{B},\exists x\in\mathcal{A}$ s.t. $f(x)=y$. ■

Proof.
1. $\forall f,g\in\mathcal{G}$,

- Injective: take $x, y \in \mathbb{R}$ s.t. $(f \odot g)(x) = (f \odot g)(y)$, it follows that

$$f(g(x)) = f(g(y)) \implies g(x) = g(y) \implies x = y.$$

- Subjective: take $y \in \mathbb{R}$ s.t. $f(z) = y$. Hence, $\exists x \in \mathbb{R}$ s.t. $g(x) = z$, which implies $f(g(x)) = y$.

2. For any functions $f, g, h \in \mathcal{G}$,

$$((f \odot g) \odot h)(x) = (f \odot g)(h(x)) = f(g(h(x))), \forall x \in \mathbb{R}$$

Similarly,

$$(f \odot (g \odot h))(x) = f((g \odot h)(x)) = f(g(h(x))), \forall x \in \mathbb{R}$$

3. Define $e : x \mapsto x$. Then $e \in \mathbb{G}$. It follows that

$$(e * g)(x) = e(g(x)) = g(x)$$

Similarly, $(g * e)(x) = g(x)$. Hence, e is the identity.

4. For $\forall f \in \mathcal{G}$, take $f^{-1} : f(x) \mapsto x$. Firstly verify f^{-1} is a bijection. Then we have

$$f^{-1} \odot f = f \odot f^{-1} = e.$$

■

Recall a definition from Linear Algebra:

$$\mathrm{GL}(n, \mathbb{R}) := \{\boldsymbol{A} \in \mathcal{M}_n(\mathbb{R}) \mid \det(\boldsymbol{A}) \neq 0\}$$

where $\mathcal{M}_n(\mathbb{R})$ denotes the set of $n \times n$ matrices over $\mathbb{R}$.

Proposition 1.4 The set $\mathrm{GL}(n, \mathbb{R})$ associated with the matrix multiplication operator is the general linear group.

Proof. 1. $\forall \boldsymbol{A}, \boldsymbol{B} \in \mathrm{GL}(n, \mathbb{R})$, we have $\boldsymbol{AB} \in \mathrm{GL}(n, \mathbb{R})$ since

$$\det(\boldsymbol{AB}) = \det(\boldsymbol{A}) \det(\boldsymbol{B}) \neq 0$$

2. Associativity of matrix multiplication is easy to verify
3. Take the identity $e := \boldsymbol{I}_n$
4. Inverse is $\boldsymbol{A}^{-1}$.

■

R $\mathrm{SL}(n, \mathbb{R}) := \{\boldsymbol{A} \in \mathcal{M}_n(\mathbb{R}) \mid \det(\boldsymbol{A}) = 1\}$ is a special linear group.

Proposition 1.5 Let $n \in \mathbb{Z}^+$, for the set

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$

associated with the operation

$$+_n \text{ such that } \quad a +_n b = \begin{cases} a + b, \text{ if } a + b \leq n - 1 \\ a + b - n, \text{ if } a + b \geq n \end{cases}$$

Proof. 1. Closed under operation

2. Associativity:

$$(a +_n b +_n c) = a + b + c \in \mathbb{Z}_n \text{ or } a + b + c - n \in \mathbb{Z}_n \text{ or } a + b + c - 2n \in \mathbb{Z}_n$$

3. Identity?
4. Inverse?

■

In the future we abuse the operator $+$ to denote the $+_n$ for $\mathbb{Z}_n$.

Theorem 1.1 Given a sequence of elements $g_1, \ldots, g_n$ in the group $\mathcal{G}$ associated with $\cdot$, the product is independent from adding brackets.

Proof. We show it by induction. Let $\mathcal{P}(n)$ denotes the product is the same whatever different ways of putting brackets on $g_1, \ldots, g_n$

1. Easy to verify $\mathcal{P}(1)$ is true.
2. Assume $\mathcal{P}(n)$ is true for $n \leq k$. Consider $n = k+1$. For $\forall m \leq n$, we have

$$\begin{aligned}
&(g_1 g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1}) \\
&\qquad = (g_1(g_2 \cdots g_m))(g_{m+1} \cdots g_{k+1}) \\
&\qquad = g_1((g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1})) \\
&\qquad = g_1(g_2 \cdots g_{k+1}) \\
&\qquad = g_1 \cdots g_{k+1}
\end{aligned}$$

■

R Theorem (1.1) shows that given a sequence of elements multiplied together, we do not need to specify the order of operations that performed.

Moreover, for **abelian** groups, the group is unqiue regardless of the ordering of elements.

Theorem 1.2 Each group $(\mathcal{G}, *)$ has the unique identity.

Proof. Let $e, e' \in \mathcal{G}$ be two identites. By definition,

$$e' = e' * e = e.$$

■

Theorem 1.3 Let $\mathcal{G}$ be a group, then g^{-1} is unique for any $g \in \mathcal{G}$.

Proof. Let h_1, h_2 be two inverses of $g \in \mathcal{G}$, by definition,

$$h_1 = h_1 \cdot e = h_1 \cdot (g h_2) = (h_1 g) h_2 = e \cdot h_2 = h_2.$$

■

R Due to Theorem(1.1) to (1.3), it makes sense to define

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}, \qquad g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}, \qquad g^0 := e.$$

Proposition 1.6 Let $(\mathcal{G}, \cdot)$ be a group, then

1. $(g^{-1})^{-1} = g, \forall g \in \mathcal{G}$
2. $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in \mathcal{G}$
3. $g^m \cdot g^n = g^{m+n}$, $\forall g \in \mathcal{G}, m, n \in \mathbb{Z}$.

In fact, we can redefine groups as the semigroups with a weaker condition.

Definition 1.3 [Group]

- A group $\mathcal{G}$ is a **semigroup** with a binary operation $\cdot$ such that
  - There exists a left identity $e \in \mathcal{G}$ s.t.

$$e \cdot a = a, \quad \forall a \in \mathcal{G}$$

  - For each $a \in \mathcal{G}$, there exists a left inverse $a^{-1} \in \mathcal{G}$ s.t.

$$a^{-1}a = e.$$

- A set $\mathcal{G}$ equipped with a binary operation $\cdot$ is said to be a **semigroup** if
  1. It is closed under the operation $\cdot$
  2. It satisfies the associativity.

■

Proposition 1.7 The definition(1.1) adn definition(1.3) are equivalent.

Proof. It suffices to show that the left identity and left inverse are essentially identity and inverse, respectively.

1. Suppose a^{-1} is the left inverse of a, we have

$$(a^{-1})^{-1}a^{-1}a = ((a^{-1})^{-1}a^{-1})a = ea = a$$

   It follows that

$$\begin{aligned} aa^{-1} &= (a^{-1})^{-1}a^{-1}aa^{-1} \\ &= (a^{-1})^{-1}(a^{-1}a)a^{-1} \\ &= (a^{-1})^{-1}ea^{-1} \\ &= e \end{aligned}$$

2. Suppose e is the left identity, it follows that

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

■

Similarly, we can define a group with help of right identities and right inverses; but we cannot define a group by left identities and right inverses. Here is a counterexample:

■ **Example 1.1** Let $(\mathcal{G}, *)$ be a group with at least 2 elements such that

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

Note that $\mathcal{G}$ is closed under $*$ and associative. The group $\mathcal{G}$ has left identities and rihgt inverses. But $\mathcal{G}$ is not a group by definition. ■

If a group is **finite**, then its operation can be described by its Cayley table, or multiplication table.

■ **Example 1.2** For a group $\mathcal{G} = \{e, a\}$ equipped with $*$, its Cayley table is given by:

$*$	e	a
e	e	a
a	a	e

For a group $(\mathbb{Z}_6, +)$, its Cayley table is given by:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

■

R Note that a group can be described by a cayley table. But not all cayley tables define a group.

R It is usually messy to check whether the cayley table defines a group. There are a few necessary conditions we can examine (to exclude Cayley Tables that don't define groups):

- It has a row and column that is identical to the list of the elements
- The elements in each row and each column must be all distinct.