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 $\mathcal{M}$

Theorem 6.8 Let $n \geq 5$, then A_n is simple,and A_n is the only non-trivial proper normal subgroup of S_n.

It suffices to show that $1 < H \triangleleft S_n$ implies $H = A_n$.

6.2. Thursday

6.2.1. Homomorphisms

Definition 6.5 [Homomorphisms] Let $G = (G, *)$ and $\hat{G} = (\hat{G}, \bigodot)$, then a **homomorphisms** is a map $\phi : G \mapsto \hat{G}$ such that

$$\phi(a * b) = \phi(a) \bigodot \phi(b), \quad \forall a, b \in G$$

If ϕ is a **bijection**, then ϕ is said to be a **isomorphism**. We denote $G \cong^{\phi} \hat{G}$. ■

R

- homomorphisms is not necessarily injective or surjective.
- The isomorphism from G to $\hat{G}$ is not unique;
- isomorphism admits symmetry, i.e., $G \cong \hat{G}$ iff $\hat{G} \cong G$.

■ **Example 6.5**
- Let V, W be vector spaces over $\mathbb{R}$ (or $\mathbb{C}$), then ant linear transformation $\phi : V \mapsto W$ is a **homomorphism** $\phi : (V, +) \mapsto (W, +)$.

$$\phi(\lambda \boldsymbol{u} + \mu \boldsymbol{v}) = \lambda \phi(\boldsymbol{u}) + \mu(\boldsymbol{v}),$$

and let $\lambda = \mu = 1$, we derive the homomorphismness.

- The determinant $\det : \mathrm{GL}(n, \mathbb{R}) \mapsto \mathbb{R}^{\#} := \mathbb{R} \setminus \{0\}$ is a group homomorphism:

$$\phi : g \mapsto \det(g) \implies \phi(gh) = \phi(g) * \phi(h)$$

- For any $n \in \mathbb{Z}^+$, we have $n\mathbb{Z} \leq \mathbb{Z}$. Define the map $\phi : n\mathbb{Z} \mapsto \mathbb{Z}$ as $nk \mapsto k$, then

$$\phi(nh + nk) = \phi(n(h+k)) = h + k = \phi(nh) + \phi(nk)$$

Then we need to show it is bijection. Each element on the range has its input, i.e., surjective. Also, take $\phi(nh) = \phi(nk)$, then $n = k$, i.e., injective.

For $n > 1$, we have $n\mathbb{Z} < \mathbb{Z}$, i.e., a proper subgroup can be isomorphic to its parent group.

- The map $\mathbb{Z} \mapsto \mathbb{Z}$ defined by $k \mapsto nk$ is a homomorphism but not isomorphism unless $n = \pm 1$:

$$\phi(h+k) = n(h+k) = \phi(h) + \phi(k)$$

- The remainder map $\phi : \mathbb{Z} \mapsto \mathbb{Z}_n$ is defined as mapping k to its remainder $\bar{k}$divided by n. It is a surjective homomorphism: $\bar{k} \in \{0, \ldots, n-1\}$ always has its input

- The map ϕ defined as $k \mapsto k+1$ is not a homomorphism:

$$\phi(0) = 1, \phi(1) = 2, \phi(0+1) = 2$$

■

Proposition 6.6 The group

$$G = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} | \theta \in \mathbb{R} \right\}$$

is isomorphic to $H = \{z \in \mathbb{C} | |z| = 1\}$ under the map

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mapsto e^{i\theta}$$

Proof. First is to check the well-defineness of ϕ. i.e., different expression of the same input leads to the same output:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix} \implies \theta' = \theta + 2n\pi \implies e^{i\theta} = e^{i\theta'}$$

Then check homomorphism and bijection.

■

Proposition 6.7 Let $\phi : G \mapsto H$ be a group homomorphism, then

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = [\phi(g)]^{-1}$ for $\forall g \in G$
3. $\phi(g^n) = [\phi(g)]^n$ for $\forall g \in G$ and $n \in \mathbb{Z}$

Proof.

$$H \ni \phi(e_G) = \phi(e_G)\phi(e_G) \implies e_H = \phi(e_G)$$

■

Definition 6.6 [image] Let $\phi : G \mapsto H$ be a group homomorphism, then the **image** of ϕ is

$$\text{Im } \phi = \phi(G) = \{\phi(g) \mid g \in G\}$$

The **kernel** of ϕ is

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}$$

In particular, if $\ker \phi = G$, then we say the homomorphism is **trivial**.

R im $\phi \le H$ and $\ker G \lhd G$.

Proposition 6.8 Let ϕ defined above, then im $\phi \le H$ and $\ker \phi \le G$

Proof.

$$a, b \in \text{im } \phi \implies ab^{-1} = \phi(g)[\phi(h)]^{-1} = \phi(gh^{-1}) \in \text{im } \phi$$

■

Proposition 6.9 A group homomorphism $\phi : G \mapsto H$ is injective iff $\ker \phi = \{e_G\}$

Proof. Necessity.

Assume $a \neq e_G$ and $a \in \ker \phi$, then

$$\phi(g) = \phi(g)e_H = \phi(g)\phi(a) = \phi(g * a),$$

but $g \neq g * a$, which is a contradiction.

Sufficiency.

For any $\phi(g) = \phi(h)$, it suffices to show $g = h$:

$$\phi(g)[\phi(h)]^{-1} = e_H \implies \phi(gh^{-1}) = e_H \implies gh^{-1} = e_G \implies g = h.$$

■

Proposition 6.10 Let G, H be isomorphic groups, if G is cyclic, then so is H

Proof. Let $G = \langle g_0 \rangle \cong H$ and $\phi : G \mapsto H$. Define $h_0 = \phi(g_0)$. Take $h \in H$, there exists $n \in \mathbb{Z}$ s.t.

$$h = \phi(g_0^n) = [\phi(g_0)]^n := h_0^n$$

It follows that $H \subseteq \langle h_0 \rangle \subseteq H$, i.e., $H = \langle h_0 \rangle$ ■

Proposition 6.11 Let G, H be isomorphic groups, if G is abelian, then so is H

Proof. For any $h_1, h_2 \in H$, there exists $g_1, g_2 \in G$ such that

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_2)\phi(g_1) = h_2 h_1.$$

■

Note that D_6 is not isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$, since D_6 is not abelian.

R These two propositions above still remains true if replacing isomorphism by a surjective homomorphism.

Proposition 6.12 The restriction of a homomorphism $\phi : G \mapsto \hat{G}$ to a subgroup $H \leq G$ gives a homomorphism $\phi|_H : H \mapsto \hat{G}$ as well.

Proof. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$ for $g_1, g_2 \in H$ ■

Proposition 6.13 Let G, H be groups s.t. $G \cong_\phi H$, then $|\phi(g)| = |g|$ for each $g \in G$.

Proof. Note that $n = |g|$ implies

$$[\phi(g)]^n = e_H,$$

i.e., $|\phi(g)| \leq n$. On the other hand, assume we can take a positive integer $m < n$ s.t.

$$[\phi(g)]^m = e_H \implies \phi(g^m) = e_H,$$

with $g^m \neq e_G$, which implies ϕ is not one-to-one, which is a contradiction. ■

6.2.2. Classification of cyclic groups

Proposition 6.14 Let r_1 denote the anti-clockwise rotation by $\frac{2\pi}{n}$, then $H = \langle r_1 \rangle \leq D_n$. Then $H \cong \mathbb{Z}_n$.

Proof. Define $\phi : H \mapsto \mathbb{Z}_n$ with $\phi(r_1^k) = \bar{k}$, $k \in \mathbb{Z}$

- ϕ is well-defined:

$$r_1^{k_1} = r_1^{k_2} \implies k_2 = k_1 + nd,$$

  which is well-defined since $\overline{k_1 + nd} = \overline{k_1}$.

- ϕ is a homomorphism: for $i, j \in \{0, \dots, n-1\}$

$$\phi(r_1^i r_1^j) = \phi(r_1^{i+j}) = \overline{i+j} = i +_n j = \phi(r_1^i) +_n \phi(r_1^j)$$

- To show ϕ is a bijection. It suffices to show $\ker \phi = \{e_H\}$:

$$\phi(r_1^i) = 0 \implies i = nd, d \in \mathbb{Z} \implies r_1^i = r_0$$

■

Theorem 6.9 Let G be a cyclic group, then

1. If $|G| = \infty$, then $G \cong \mathbb{Z}$
2. If $|G| = n$, then $G \cong \mathbb{Z}_n$

Proof. Define $\phi : G \mapsto \mathbb{Z}$ with $g_0^k \mapsto k$

First show the well-defineness of ϕ; then show ϕ is homomorphic:

$$\phi(g_0^m * g_0^n) = \phi(g_0^m) + \phi(g_0^n)$$

Then show that ϕ is bijection, i.e., $\ker \phi = \{e_G\}$.

For the second case, define the map $\phi : \mathbb{Z}_n \mapsto G$ with $k \mapsto g_0^k$:

Check the well-defineness, which is clear since the expresion for k is unique.

ϕ is homomorphism:

$$\phi(h +_n k) = \phi(\overline{h+k}) = g_0^{\overline{h+k}} = g_0^{h+k} = g_0^h g_0^k = \phi(h)\phi(k)$$

Then show that it is bijection. A one-to-one function from a finite set to itself is onto. Then check one-to-one mapping.

■

Corollary 6.2 Let $G, \hat{G}$ be cyclic groups of the same order, then $G \cong \hat{G}$.

6.2.3. Isomorphism Theorems

The first and seond theorem is required in exam. (can we apply the corresponding theorem in the exam?)

Theorem 6.10 — **The First Isomorphism Theorem.** Let $G \mapsto H$ be a **surjective** group homomorphism, then $\ker \phi \lhd G$ and $G/\ker \phi \cong \operatorname{im} \phi$