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 6

Week5

6.1. Monday

Let G be a finite group with $H \leq G$. Then G can be partitioned into the left cosets or the right cosets of H. However, the left cosets and the right cosets are usually different.

■ **Example 6.1** Let $G = S_3$ and $H = \{(), (12)\}$, it is eaily seen that

$$G = H \sqcup (13)H \sqcup (23)H = H \sqcup H(13) \sqcup H(23)$$

However, we see that

$$(13)H \neq H(13), \quad (23)H \neq H(23)$$

We are interested in the case when the left coset of H and the right coset of H are always the same. ■

Definition 6.1 [normal subgroup] Let G be a group. A subgroup $H \leq G$ is **normal** if

$$aH = Ha, \quad \forall a \in G$$

We denote this by $H \trianglelefteq G$ and $H \triangleleft G$ when $H < G$. ■

Normal subgroups have several equivalent definitions:

Theorem 6.1 Let G be a group and $H \leq G$. The following statements are equivalent:

1. $H \trianglelefteq G$
2. $a^{-1}Ha \subseteq H$, for $\forall a \in G, h \in H$
3. $a^{-1}Ha = H$, for $\forall a \in G$.

Proof. The non-trivial case is (2) implies (3). Since (2) holds for all $a \in G$, it holds for a^{-1}, i.e.,

$$(a^{-1})^{-1}Ha^{-1} \subseteq H \implies aHa^{-1} \subseteq H \implies H \subseteq a^{-1}Ha$$

■

■ **Example 6.2**
1. Any group G contains the trivial normal subgroups, i.e. ,1 and G
2. Let $G = S_3, N = \{(), (123), (132)\}, H_1 = \{(), (12)\}, H_2 = \{(), (13)\}, H_3 = \{(), (23)\}$, then $N \triangleleft G$ but H_i's are not.
3. Let $n \in \mathbb{N}^+$, then $\mathrm{SL}(n, \mathbb{R}) \triangleleft \mathrm{GL}(n, \mathbb{R})$
4. Let $n \in \mathbb{N}^+$, then $A_n \triangleleft S_n$. (question)
5. Let H, K be groups and $G = H \times K$. Then $H \times 1$ and $1 \times K$ are normal subgroups of G.

■

Proposition 6.1 Let i, j, k be such that

$$i^2 = j^2 = k^2 = ijk = -1 \in \mathbb{R},$$

show that the **quaternion group**

$$Q_8 = \langle i, j, k \rangle$$

has order 8, and every its subgroup is normal.

Proof. Since $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, any element from the set Q_8 can be written as the form $\pm i^{m_1} j^{m_2} k^{m_3}$ for $m_i \in \mathbb{N}$ with $m_1 + m_2 + m_3 = 1$. Hence, the set Q_8

has at most 8 elements, i.e., the order should be no more than 8. Furthermore, note that $\pm 1, \pm i, \pm j, \pm k \in Q_8$, which means the $|Q_8| = 8$.

Also, due to Lagrange's theorem, every subgroup can only have order 1,2,4,8, and the subgroup with order 1 or 8 are trivial normal subgroups; the subgroup with order 4 has index 2, i.e., is normal. After computation, we find the only one subgroup with order 2 is $\{1, -1\}$, which is normal obviously. ■

R Every subgroup of an abelian group is normal, but the converse is not true (e.g., see example above). In general, a group G is **Dedekind** if every its subgroups is normal; and if G is non-abelian but with all normal subgroups, then G is **Hamiltonian group**.

Theorem 6.2 Let G be a group with $H \trianglelefteq G$, then the set $[G : H]$ forms a **quotient group** (factor group) G/H under the operation defined as:

$$(aH)(bH) := (ab)H, \qquad \forall a, b \in G$$

Note that the proof is incomplete, we need to check the well-defineness of operation.

Proof. To examine that G/H is indeed a group:

- $(ab)H$ is also a left cosets
- associative
- H is identity
- $a^{-1}H$ is inverse

■

■ **Example 6.3** For $n \in \mathbb{N}^+$, the abelian group $\mathbb{Z}$ contains a normal subgroup $n\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n. ■

Proposition 6.2 Let G be a group, then the **center**

$$Z(G) := \{z \in G \mid zg = gz, \forall g \in G\}$$

forms a normal subgroup of G.

Question for Proposition 3.5

Proof. First, show that $z_1, z_2 \in Z(G)$ implies $z_1 z_2^{-1} \in Z(G)$. Next, show that $g^{-1}zg = z$ for all $g \in G$ and $z \in Z(G)$. ∎

Example 6.4
1. Let G be an abelian group, then $Z(G) = G$, i.e., $Z(G)$ is essentially the largest abelian subgroup of G
2. Let $n \geq 3$ be an integer, then $Z(S_n) = 1$.
3. Let $n \geq 3$ be an integer, then $Z(\mathbb{Z}_n \times S_n) = \mathbb{Z}_n \times 1$.
4. $$Z(\mathsf{GL}(2,\mathbb{R})) = \{\mathrm{diag}(a,b) : ab \neq 0\}$$

6.1.1. Derived subgroups

Definition 6.2 [derived subgroup] Let G be a group and $a, b \in G$. The **commutator** of a, b is:

$$[a,b] := a^{-1}b^{-1}ab$$

The **derived subgroup** (**commutator subgroup**) of G is

$$G' := \langle [a,b] | a, b \in G \rangle$$

Proposition 6.3 The G'-coset partition defines an equivalence relation on G such that $ab \sim_{G'} ba$ for $\forall G$.

Proof. First show that $x \sim_{G'} y$ iff $xy^{-1} \in G'$.

Then it's trivial that $aba^{-1}b^{-1} \in G'$. ■

Note that the L-coset parititon $a \sim_L b$ means that $aH = bH$.

R If $G' \lhd G$, then G/G' is an abelian group. Note that G' is normal since

$$a^{-1}ha = [a, h^{-1}]h \in G'$$

Theorem 6.3 Let G be a group, then $G' \lhd G$ and G/G' is abelian.

Corollary 6.1 Let G be a group such that $G'' = 1$, then G is abelian

Proof. $\{\{a\} \mid a \in G\}$ is abelian implies G is abelian. ■

R The derived subgroup is the smallest normal subgraoup such that the quotient group G/G' is abelian, i.e., any quotient group G/H is abelian iff H contains G'.

Theorem 6.4 Let G be a group and $H \lhd G$, then G/H is abelian iff $G' \leq H$.

Proof. Necessity. Since G/H is abelian, we have

$$abH = baH \implies abh_1 = bah_2 \implies [a,b] = h_2 h_1' \in H \implies \langle [a,b] | a, b \in G \rangle \in H$$

Suffiency. Note that

$$a^{-1}b^{-1}ab \in G' \subseteq H \implies a^{-1}b^{-1}ab = h \implies ab \sim_H ba, \forall a, b \in G$$

■

Theorem 6.5 Let $n \in \mathbb{N}^+$, then $A_n = S_n'$ (A_n denotes the group of even permutations). Moreover, when $n \geq 5$, $A_n' = A_n$.

Recall that a permutation is called an even permutation if it can be written as a product of an even number of transpositions.

Proof. Note that $S_n / A_n = A_n \sqcup \tau A_n$, and therefore abelian. Thus $A_n \geq S_n'$. It suffices to show $S_n' \geq A_n$, Note that

$$A_n = \langle (12i) | i = 3, \ldots, n \rangle$$

Therefore $(12i) = (12)^{-1}(1i)^{-1}(12)(1i) \in S_n'$ implies $A_n \leq S_n'$.

When $n \geq 5$, note that $A_n' \leq A_n$. On the other hand,

$$(12i) = (1a2)^{-1}(1bi)^{-1}(1a2)(1bi) \in A_n' \implies A_n \leq A_n'$$

■

R In general, a group satisfying $G' = G$ is perfect. The alternating groups are concrete examples of perfect groups.

Proposition 6.4 The group $\mathrm{SL}(2, \mathbb{R})$ is perfect.

Proof. Note that any element is a product of $\begin{pmatrix} 1 & x \\ 0 & x \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ and these two basis can be written as the form $[a, b]$.,e.g.,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = [\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (\sqrt{2})^{-1} & 0 \\ 0 & \sqrt{2} \end{pmatrix}]$$

■

Definition 6.3 [Simple] Every group G contains the trivial normal subgroups 1 and G. If these are only normal subgroups contained in G, then we say G is **simple**. ■

Definition 6.4 [Conjugacy Class] Let G be a group and $a,b \in G$. If there exists $g \in G$ such that $g^{-1}ag = b$, then a,b are **conjugate**, and b is a conjugate of a. The conjugacy class with representative a is a collectio nof all conjugates of a:

$$\mathrm{Cl}(a) = \{g^{-1}ag \mid g \in G\}$$

Proposition 6.5 The conjugacy class defines an equivalence relation on G; and $\mathrm{Cl}(z) = \{z\}$ for each $z \in G$.

Theorem 6.6 Let G be a finite group with r disjoint conjugacy classes of size $c_1, \dots, c_r \geq 2$. Let $|Z(G)| = c_0$, then

$$|G| = \sum_{i=0}^{r} c_i$$

Proof. Note that $x \in Cl(z)$ with $z \in Z(G)$ iff $x = z$. Hence the conjugacy class with only one element must be of the form $\{z\}$, $z \in Z(G)$. Thererfore,

$$|G| = \sum_{i=0}^{r} c_i$$

■

Theorem 6.7 The alternating group A_5 is simple.

Solution. Let $\sigma \in N \triangleleft A_5$ be non-identity, then if we can show that $N = A_5$, which is a contradiction, then we show that A_5 is simple.

Note that A_5 is generated by the $3-$cycles, i.e., every element σ of A_n can be written as

$$\sigma = C_1 C_2 \cdots C_k,$$

with C_i to be 3-cycles.

Note that N contains a non-trivial even permutation σ, which must be of the form $(abcde)$ or $(ab)(cd)$ or (abc).

- When $\sigma = (abcde)$, let $\alpha = (ab)(cd)$. then N also contains:

$$\alpha\sigma\alpha^{-1} = (ab)(cd)(abcde)(ab)(cd) = (adceb)$$

  and therefore contains

$$\sigma\sigma^{-1} = (aec)$$

- When $\sigma = (ab)(cd)$, let $\beta = (abe)$, then N also contains

$$\sigma' = \beta\sigma\beta^{-1} = (becd)$$

  and therefore contains

$$\sigma\sigma^{-1} = (abe)$$

If N contains a signle 3-cycles, since 3-cycles are mutually conjugate, N will contain any other 3-cycles. Therefore $N = A$, which is a contradiction. ■

Solution 2. Let N be a normal subgroup of A_5, then it is a union of some of the conjugacy classes of A_5. Since the order of N must divide 60, a short calculation shows that no union of some of these conjugacy classes that includes $\{e\}$ has order a divisor of 60, unless $A_5 = \{e\}$ or A_5. ■