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 vii

Notations ix

1 Week1 1

1.1 Monday 1

1.1.1 Introduction to Abstract Algebra 1

1.1.2 Group 1

2 Week2 11

2.1 Tuesday 11

2.1.1 Review 11

2.1.2 Cyclic groups 11

3 Week3 17

3.1 Tuesday 17

3.2 Thursday 22

3.2.1 Cyclic Groups 22

3.2.2 Symmetric Groups 25

3.2.3 Dihedral Groups 28

3.2.4 Free Groups 29

4 Week4 31

4.1 Subgroups 31

4.1.1 Cyclic subgroups 32

4.1.2 Direct Products 36

4.1.3 Generating Sets 37

5 Week4 41

5.1 Reviewing 41

5.1.1 Theorem of Lagrange 43

6 Week5 49

6.1 Monday 49

6.1.1 Derived subgroups 52

6.2 Thursday 57

6.2.1 Homomorphisms 57

6.2.2 Classification of cyclic groups 61

6.2.3 Isomorphism Theorems 62

7 Week6 67

7.1 Ring 67

7.1.1 Modular Arithmetic 70

7.1.2 Rings of Polynomials 72

7.1.3 Integral Domains and Fields 73

7.1.4 Field of fractions 78

8 Week7 81

8.1 Field of Fractions 81

8.1.1 Homomorphisms 82

8.2 Thursday 90

8.2.1 Principal Ideal Domainas 90

8.2.2 Qotient Ring 92

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 $\mathcal{M}$

8.2. Thursday

8.2.1. Principal Ideal Domainas

For a fixed finite set of elements $a_1, \ldots, a_n$ in a commutative ring R, let $\langle a_1, \ldots, a_n \rangle$ denote the subset:

$$\{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$

Proposition 8.10 The set $\langle a_1, \ldots, a_n \rangle$ is an ideal of R.

Proof.

1. It forms a group.
2. Given any $\sum_i r_i a_i \in I$, for any $r \in R$, we have

$$r \sum_i r_i a_i = \sum_i (r r_i) a_i \in I.$$

∎

Definition 8.9 We call $\langle a_1, \ldots, a_n \rangle$ the ideal **generated** by $a_1, \ldots, a_n$. An ideal $\langle a \rangle = \{ar \mid r \in R\}$ generated by one element $a \in R$ is called the **principal ideal**.

R Note that $R = \langle 1 \rangle$ and $\{0\} := \langle 0 \rangle$ are both principal ideals.

Theorem 8.3 Every ideal in the ring $\mathbb{Z}$ is a principal ideal.

Proof. w.l.o.g., suppose I contains nonzero element, say a. Then $-1 \in \mathbb{Z}$ implies that $-a \in I$, and therefore I contains at least one positive integer. Suppose I contains a positive integer d that is smaller than any other elements that is positive in I. We claim $I = \langle d \rangle$.

For any $a \in I$, we have $a = dp + r$ for $0 \leq r < d$, which implies that $r = a - dp$ lies in I, since I is an ideal, which implies $d = 0$, i.e., $a = dq$. Thus $I \subseteq \langle d \rangle$.

On the other hand, we have $dr \in I$ for any $r \in \mathbb{Z}$, i.e., $\langle d \rangle \subseteq \mathbb{Z}$ ∎

Proposition 8.11 Given a, b in a commutative ring R. If $b = au$ for some unit $u \in R$, then $\langle a \rangle = \langle b \rangle$. If R is an integral domain and $\langle a \rangle = \langle b \rangle$, then $b = au$ fo some unit $u \in R$.

Proof. For the case $b = 0$, we imply $a = 0$ and the result is trivial.

For $b \neq 0$, there exists $u, v \in R$ such that $b = au$ and $a = bv$. Thus

$$b = buv \implies b(1 - uv) = 0$$

Since R is an integral domain, and $b \neq 0$, we have $1 - uv = 0$, which implies $uv = 1$, o.e., u is a unit. ■

Definition 8.10 [PID] If R is an integral domain in which every ideal is principal, we say that R is a **principal integral domain**.

We claim that for any field k, the ring of polynomails $k[x]$ is also a PID.

Proposition 8.12 Let R be a commutative ring. For $\forall d, f \in R[x]$ such that the leading coefficient of d is a unit in R, then there exists $q, r \in R[x]$ such that

$$f = qd + r,$$

with $\deg r < \deg d$.

Proof. We prove this theorem by induction.

If $\deg f < \deg d$, take $r = f$ and $q = 0$

Let $d = \sum_{i=0}^{n} a_i x^i \in R[x]$ be fixed, where a_n is a unit of R. For any given $f = \sum_{i=0}^{m} b_i x^i \in R[x]$, $m \geq n$, suppose the claim holds for any f' with $\deg f' < \deg f$.

Construct $f' = f - a_n^{-1} b_m x^{m-n} d$, thus there exists $q', r' \in R[x]$ with $\deg r' < \deg d$ such that

$$f - a_n^{-1} b_m x^{m-n} d = q'd + r'$$

which implies

$$f = (q' + a_n^{-1} b_m x^{m-n})d + r'$$

■

Theorem 8.4 Let k be a field, then $k[x]$ is a PID.

Proof. Let I be an ideal of $k[x]$. Let d be a nonzero polynomial in I with the least leading degree. The existence of this polynomial is because the leading degree of a polynomail is a non-negative integer. I is clear that $\langle d \rangle \subseteq I$. It suffices to show $I \subseteq \langle d \rangle$

For $\forall f \in I$, we have $f = qd + r$ for some $q, r \in k[x]$ such that $\deg(r) < \deg(d)$. Then $r = f - qd$ lines in I. Since d has the least degree, we imply $r = 0$. Thus $f = qd$, which implies $f \in \langle d \rangle$. Thus $I \subseteq \langle d \rangle$. ■

8.2.2. Qotient Ring

Let R be a commutative ring. Let I be an ideal of R. Define a relation $\sim$ on R as follows:

$$a \sim b, \text{ if } b - a \in I$$

Definition 8.11 [Congruent modulo] If $a \sim b$, we say that a is congruent modulo I to b, and write

$$a \equiv b (\operatorname{mod} I)$$

■

Proposition 8.13 Congruence modulo I is an equivalence relation.

Proof.
1. $a - a = 0 \in I$
2. $a - b \in I$ implies $b - a = (-1)(a - b) \in I$
3. $a - b, b - c \in I$ implies $(a - b) + (b - c) \in I$

■

Definition 8.12 [Residue] Let R/I be the set of equivalence classes of R w.r.t. the relation $\sim$. Each element in R/I has the form

$$\bar{r} = r + I = \{r + a \mid a \in I\}, \qquad r \in R$$

We call $\bar{r}$ as the **residue** of r in R/I. Note that $r \in I$ implies $\bar{r} = \bar{0}$.

Observe that

$$(r+a) + (r'+a') \in (r+r') + I = \overline{r+r'}$$
$$(r+a)(r'+a') \in rr' + I = \overline{rr'}$$

Thus we define binary operation on R/I:

$$\bar{r} + \bar{r'} = \overline{r+r'}$$
$$\bar{r} \cdot \bar{r'} = \overline{rr'}$$

Proposition 8.14 The set R/I equipped with the addition and multiplicaiton defined above, is a **commutative ring**.

Proposition 8.15 The mapping $\pi : R \to R/I$, defined by

$$\pi(r) = \bar{r}, \quad \forall r \in R$$

is a surjective ring homomorphism with the kernel $\ker(\pi) = I$.

Let m be a natural number. The set

$$m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$$

is an ideal of $\mathbb{Z}$.

Proposition 8.16 The quotient ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}_m$.

Proof. Define r_m to be the remainder of the division of r by m.

It is clear that $\bar{r} = \bar{r_m}$. We define a mapping $\phi : \mathbb{Z}_m \to \mathbb{Z}/m\mathbb{Z}$:

$$\phi(r) = \bar{r}, \qquad \forall r \in \mathbb{Z}_m$$

We claim it is a homomorphism:

- $\phi(1) = \bar{1} = 1_{\mathbb{Z}/m\mathbb{Z}}$
- $\phi(r +_m r') = \overline{r +_m r'} = \overline{(r + r')_m} = \overline{r + r'} = \phi(r) + \phi(r')$
- $\phi(r \cdot_m r') = \phi(r)\phi(r')$

Then we show that ϕ is bijective:

For any $\bar{r}$ in $\mathbb{Z}/m\mathbb{Z}$, we have $\phi(r_m) = \bar{r}$

Suppose $\phi(r) = \bar{r} = 0$ in $\mathbb{Z}/m\mathbb{Z}$, then $r \in m\mathbb{Z}$, which implies $r = 0$.

■

Proposition 8.17 Let $\phi : R \to R'$ be a ring homomorphism, then the image of ϕ

$$\text{im}\phi = \{r' \in R' \mid r' = \phi(r) \text{ for some } r \in R\}$$

is a ring.

Theorem 8.5 — First Isomorphism Theorem. Let R be a commutative ring, let $\phi : R \to R'$ be a ring homomorphism, then

$$R/\text{ker}\phi \cong \text{im}\phi$$

Corollary 8.1 If the ring homomorphism is surjective, $\phi : R \to R'$, then

$$R' \cong R/\text{ker}\phi$$

■ **Example 8.7** For the map $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(n) = n_m$ for $\forall n \in \mathbb{Z}$, it is clear that ϕ is a surjective ring homomorphism, and $\ker\phi = m\mathbb{Z}$. Thus

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$$

question

■ **Example 8.8** The ring $\mathbb{Z}[i]/(1+3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

Define a mpap $\phi : \mathbb{Z} \to \mathbb{Z}[i]/(1+3i)$:

$$\phi(n) = \bar{n}$$

Show that $\ker\phi = 10\mathbb{Z}$, and therefore

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$$

■ **Example 8.9** The rings $\mathbb{R}[x]/(x^2+1)$ and $\mathbb{C}$ are isomorphic.

Define a map from $\mathbb{R}[x]$ to $\mathbb{C}$:

$$\phi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k i^k$$

Question: PID of $\mathbb{R}[x]$ implies $\ker\phi = \langle p \rangle$ for some $p \in \mathbb{R}[x]$. Then show that $\ker\phi = \langle x^2+1 \rangle$.

By isomorphism theorem, $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.