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 9

Week8

9.1. Friday

9.1.1. Classification in Chapter 7

Definition 9.1 A ring $R = (R, +, \cdot)$ means that:

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a semi-group
3. R satisfies the **distributive law**

- In addiction, if R has a **multiplicative identity** $1 \in R$, then R is a **unital ring**.
- A ring R is said to be commutative if its multiplication is commutative.

Proposition 9.1 Let $(R, +)$ is a group, and $(R, \cdot)$ is a monoid, and $(R, +, \cdot)$ satisfies the distributive laws, then $+$ is **commutative**.

Proof. Consider distributive laws in $(1+1)(x+y)$ ■

Since $(\mathbb{Z}_m, \cdot)$ is not necessarily a group, we assume

- $(\mathbb{Z}_m, +)$ is a group
- $(\mathbb{Z}_m, +, \cdot)$ is a ring. (unital and commutative)
- $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$

Proposition 9.2 Question on $a \equiv c(\bmod m)$ and $b \equiv d(\bmod m)$ implies

$$a + b \equiv c + d(\bmod m), ab \equiv cd(\bmod m)$$

Definition 9.2 [Ring of polynomials] Let R be a **commutative ring**, then a polynomial over R is

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

with $a_i \in R$. Here $f(x) \in R[x]$.

R The image on R does not necessarily define a function f, e.g.,

$$f(x) = 1 + x + x^2, g(x) = 1 \in \mathbb{Z}_2[x]$$

Definition 9.3 Let D be a ring.

- A nonzero element $r \in D$ is called a **zero divisor** if there exists a nonzero $s \in D$ such that $rs = 0$ or $sr = 0$
- If D has no zero divisors, then D is called a **domain**
- If D has no zero divisors, i.e., the product of two nonzero elements is always nonzero, and D is commutative, then D is called an **integral domain**.

R

- R is an integral domain iff $R[x]$ is an integral domain
- $\mathbb{Z}_6$ is not an integral domain. Note that $\mathbb{Z}_m$ is an integral domain iff m is a prime.
- $C[-1,1]$ is not an integral domain, e.g., $f = (x)^+, g = (x)^-$.

Proposition 9.3 Let D be a commutative ring, TFAE

- D is an integral domain
- For any nonzero $a, b \in D$, we have $ab \neq 0$
- D satisfies the cancellation law: $ca = cb$ and $c \neq 0$ implies $a = b$.

Proof. Consider the distributive laws on $c[a + (-b)] = 0$; and $ab = a0$. ■

R Generalization into non-commutative rings.

Definition 9.4 Let R be a ring, then $a \in R$ is a unit if it has a multiplicative inverse $a^{-1} \in R$.

Definition 9.5 A **divison field** R is a ring that all its nonzero elements are units.

If R is a commutative ring in which every nonzro element is a unit, then R is a field

R The quaternion is not commutative, and thus not a field.

- $\{\text{zero divisors in } \mathbb{Z}_m\} = \{k \in \mathbb{Z}_m^* \mid gcd(k, m) > 1\}$
- $\{\text{units in } \mathbb{Z}_m\} = \{k \in \mathbb{Z}_m^* \mid gcd(k, m) = 1\}$

Proposition 9.4 All finite integral domain D is a field

Proof. For $D = \{a_1, \ldots, a_n\}$, consider $a^n = a^m$ for $a \neq 0$, which implies $1 \in D$. Then consider the set

$$\{aa_1, \ldots, aa_n\}$$

■

Definition 9.6 [Char] Define

$$n \circ a = \underbrace{a + \cdots + a}_{n \geq 1}, \qquad 0 \circ a = 0_R$$

If there exists smallest positive n such that

$$n \circ a = 0, \forall a \in R,$$

then n is the **characteristic of the ring** R. Otherwise R is of characteristic 0. In particular, if $R = F$ is a field, then it is the characteristic of the field.

Proof. $\mathrm{char}(\mathbb{Z}_n) = n$ ∎

Proposition 9.5 The characteristic of an integral domain is either 0 or a prime.

Proof. Consider $n = km$, then $n \circ 1 = (k \circ 1)(m \circ 1)$ ∎

Theorem 9.1 The characteristic for a **unital** ring is either the smallest n s.t. $n \circ 1 = 0$, or 0.

Proof. $n \circ a = a(n \circ 1) = 0$ ∎

Given an integral domain, we want to enlarge it into a field by adding some multiplicative inverses.

Equivalence Relation. For the set $R \times R_{\neq 0} = \{(a,b) \mid a,b \in R, b \neq 0\}$, define the operation

$$(a,b) \sim (c,d) \text{ if } ad = bc$$

Definition 9.7 [Quotient Set] Given the equivalence relation $\sim$, the quotient set $S/\sim$ is the set of all equivalence classes of S.

Define the operation

$$(a,b) + (c,d) = (ad + bc, bd)$$
$$(a,b)(c,d) = (ac, bd)$$

we have $(a,b) \sim (a',b'), (c,d) \sim (c',d')$ implies

- $(a,b) + (c,d) \sim (a',b') + (c',d')$
- $(a,b)(c,d) \sim (a',b')(c',d')$

Definition 9.8 [Fraction Field] Define $\text{Frac}(R) = (R \times R_{\neq 0})/\sim$, and

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$
$$[(a,b)][(c,d)] = [(ac, bd)]$$

it forms a field, with additive identity $0 := [(0,1)]$, and multiplicative identity $1 := [(1,1)]$. The multiplicative inverse of a nonzero $[(a,b)] \in \text{Frac}(R)$ is $[(b,a)]$

R $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$, if identify $[(a,b)] := a/b \in \mathbb{Q}$.

9.1.2. Classificiation on Chapter 8

Definition 9.9 [Ring Homomorphism] A map $\phi : R \to R'$ is a ring homomorphism if

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

- **Unital homomorphism**: R, R' are also unital and $\phi(1_R) = 1_{R'}$
- If ϕ is bijective, then ϕ is an **isomorphism**, $R \cong R'$
- R, R' are unital but ϕ does not have to be unital:

$$\phi : a \mapsto 0_{R'}$$

- $\phi(0_R) = 0_{R'}$: $\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R)$
- $\phi(-a) = -\phi(a)$: $0_{R'} = \phi(a + (-a)) = \phi(-a) + \phi(a)$
- If ϕ is unital, then $[\phi(u)]^{-1} = \phi(u^{-1})$ for each unit $u \in R$:

$$1_{R'} = \phi(u)\phi(u^{-1})$$

- $\text{Im}(R) = \phi(R)$ is a subring of R'

R Let R be a ring, then $\phi : \mathbb{Z} \to R$ is uniquely determined by

$$\phi(1) = a \in R,$$

since $\phi(n) = n \circ a$ and $\phi(-n) = -n \circ a = n \circ (-a)$

Proposition 9.6 The ring $\mathbb{Q}$ and $\mathbb{Z}$ cannot be isomorphism, but the fields $\mathbb{Q}$ and $\text{Frac}(\mathbb{Z})$ are isomorphic.

Proof. Consider the map $\phi : \mathbb{Q} \to \text{Frac}(\mathbb{Z})$:

$$\phi(a/b) = [(a,b)]$$

First it is well-defined. Second it is homorphism. Third it is one-to-obe and onto. ■

Theorem 9.2 Let F be a field, then $\text{Frac}(F) \cong F$.

Proof. Consider the map $\phi : F \to \text{Frac}(F)$:

$$\phi(s) = [(s,1)], \quad \forall s \in F.$$

■

Definition 9.10 [Subring] Let R be a ring, a subset S of R is a **subring** if it is a ring under the same operations of R. Or equivalently,

- $a,b \in S$ implies $a - b \in S$
- $a,b \in S$ implies $ab \in S$

To check S is unital, we need to check S contains a multiplicative identity 1_S (not necessaruly 1_R)

Proposition 9.7 For ring R and subring S, we have $0_S = 0_R$

Definition 9.11 [Kernel] The kernel of ϕ is $\ker(\phi) = \{a \in R \mid \phi(a) = 0_{R'}\}$

Proposition 9.8 For a ring homomorphism ϕ,

- S is a subring implies $\phi(S)$ is a subring
- S' is a subring implies $\phi^{-1}(S')$ is a subring.
- $\text{im}(\phi)$ is a subring.

Corollary 9.1 If R, R' are isomorphic, then $\phi(1_R) = 1_{R'}$

R For unital S', the $\phi^{-1}(S')$ is not necessarily unital. Example: $\phi : 3\mathbb{Z} \to \mathbb{Z}_6$ defined by $\phi(x) = \bar{x}$.

Proposition 9.9 A ring homomorphism is one-to-one iff $\ker\phi = \{0_R\}$

Definition 9.12 [Ring of polynomials]

$$R[x,y] = \left\{ \sum_i \sum_j a_{ij} x^i y^j \middle| a_{ij} \in R \right\}$$

Proposition 9.10

$$R[x,y] \cong (R[x])[y]$$

Proof. Construct the mapping

$$\phi\left(\sum_i \sum_j a_{ij} x^i y^j\right) = \sum_j \left(\sum_i a_{ij} x^i\right) y^j$$

■

Proof. It is clear that is a homomorphism. The one-to-one is by showing

$$\ker\phi = \{0\}$$

To show the onto, define $g = \sum_{j=0}^{n} p_j y^j$, and let $m = \max_j \deg p_j$, which implies

$$g = \sum_{j=0}^{n} (\sum_{i=0}^{m} a_{ji} x^i) y^j$$

■

Proposition 9.11 A subring of a field is an integral domain.

Proof. For the subring $R \subseteq F$, suppose $a, b \in R, ab = 0, a, b \neq 0$, we have

$$b = a^{-1}(ab) = 0$$

■

R The integral domain $\mathbb{Z}$ is a subring of field $\mathbb{Q}$.

Definition 9.13 [Ideal] A subset I in a ring R is an ideal if

- $(I, +)$ is a group
- For each $r \in R$, $rI \subseteq I$ and $Ir \subseteq I$

If I is a prpoper subset, then I is a proper ideal.

R

- Improper ideal: R, trivial ideal $\{0\}$, containing any proper non-trivial ideals: simple.
- The first condition is replaced by:

$$0 \in I, \quad x - y \in I, \forall x, y \in I$$

- an ideal I containing 1 implies $I = R$
- $I = m\mathbb{Z}$ is an ideal of ring $\mathbb{Z}$ since $mn_1 - mn_2 = m(n_1 - n_2) \in I$, and $d \cdot mn = mn \cdot d \in I$ for $\forall d \in I$.

- $I = \{f \in R \mid f(1/2) = 0\} \subseteq C[-1,1]$ is an ideal.

Now we seek a special subring I such that R/I forms a new ring.

Theorem 9.3 R is a commutative ring, I is an ideal. Let R/I denote the set of equivalence classes of R, and each element has the form $r + I$ for $r \in R$.

$$(a+I)+(b+I) = (a+b)+I$$

$$(a+I)(b+I) = ab+I$$

then R/I forms a ring.

Proof. Check it forms a group, associative multiplication, distributive laws. ∎

R $\bar{a} = \bar{b}$ is written as $a \equiv b (\bmod I)$

Every ideal is a subring, and the converse does not necessarily hold. If the converse is true, then it is a Hamiltonian ring.

9.1.3. Classificatin on Chapter 10

Proposition 9.12 The **canonical homomorphism** $\pi : R \to R/I$ defined by $\pi(r) = \bar{r}$ is a surjective homomorphism with $\ker(\pi) = I$.

Theorem 9.4 — First Isomorphism Theorem. Let $\phi : R \to R'$ be a ring homomorphism, then e=ker(ϕ) is an ideal of R, and

$$R/\ker\phi \cong \mathrm{im}(\phi)$$

Proof. Construct the mapping

$$\bar{\phi}(\bar{a}) = \phi(a), \quad \forall a \in R$$

Then show the well-defined, homomorphism, surjective, and one-to-one:

$$a' := \phi(a) = \bar{\phi}(\bar{a})$$

$$\bar{a} \in \ker(\bar{\phi}) \implies \phi(a) = 0, \bar{a} = \bar{0}$$

■

Corollary 9.2 Let ϕ be a surjective ring homomorphism, then

$$R/\ker(\phi) \cong R'$$

R Define a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m$ by $\phi(n) = \bar{n}$. Thus ϕ is surjective and $\ker(\phi) = m\mathbb{Z}$, and therefore $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$

Proposition 9.13

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i]/(1+3i)$$

Proof. Construct a mapping $\phi : \mathbb{Z} \to \mathbb{Z}[i]/(1+3i)$ by

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

It's clear that ϕ is a homomorphism.

- Note that $1+3i \equiv 0(\text{mod} < 1+3i >)$ implies $i \equiv 3(\text{mod} < 1+3i >)$. Thererfore,

$$\overline{a+bi} = \overline{a+3b} = \phi(a+3b) \implies \phi \text{ is surjective}$$

- Suppose $\phi(n) = \bar{0}$, then

$$n = (a+bi)(1+3i) = (a-3b) + (3a+b)i$$

If $3a+b=0$, then $n = 10a$, which implies $\ker(\phi) \subseteq 10\mathbb{Z}$

- For each $m \in \mathbb{Z}$,

$$\phi(10m) = \overline{10m} = \overline{1+3i}\,\overline{(1-3i)m} = \bar{0} \implies 10\mathbb{Z} \subseteq \ker(\phi)$$

Thus $\ker(\phi) = 10\mathbb{Z}$. Applying First Isomorphic Theorem. ■

■ **Example 9.1** $R[x]/(x^2+1) \cong \mathbb{C}$.

Define the map $R[x] \to \mathbb{C}$ by:

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

Check homomorphism, surjective. Let $f(x) \in \ker(\phi)$, then

$$f(i) = 0 \implies f(-i) = 0 \implies (x^2+1)|f(x) \implies \ker(\phi) \subseteq < x^2+1 >$$

On the other hand,

$$f(x) = (x^2+1)g(x) \implies f(i) = 0 \implies < x^2+1 > \subseteq \ker(\phi)$$

■

Definition 9.14 [Maximal] An ideal M in ring R is **maximal** if the only ideal that properly contains M is R it self. ■

Proposition 9.14 A unital commutative ring R is **simple** iff it is a division ring.

Proof. Consider a nonzero ring R.

- For nonzero $a \in R$, the principle ideal $< a >= aR = \{0\}$ or R.

$$a = 1a \in < a > \implies < a >= aR = R$$

  Thus there exists $x \in R$ such that $ax = xa = 1_R$

- For the converse, consider the $aa^{-1} \in R$

■

R It says that a field is simple, and a simple unital commutative ring forms a field.

> **Theorem 9.5** A proper ideal M of a unital commutative ring R is **maximal** iff R/M is a fied.

Proof. It suffices to show M is maximal iff R/M is simple. ■

R When R is not unital, the theorem will not hold. For $R = 2\mathbb{Z}$, $M = 4\mathbb{Z}$ is a maximal ideal of R. R/M is not a field since $\bar{2} \in R/M$ and $\bar{2}\bar{2} = \bar{0}$. The converse also holds.

Question about second.

R Consider $R = \mathbb{Z}_{12}$, we have proper ideals

$$I_1 = \{0,2,4,8,10\} \quad I_2 = \{0,3,6,9\}, \quad I_3 = \{0,4,8\}, \quad I_4 = \{0,6\}$$

Here I_1, I_2 are maximal, and $R/I_1 \cong F_2$, and $R/I_2 \cong F_3$.