Review on Rings and Fields

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday Jan 20, 2025

MATH4302, Algebra II, Course Outline

- Part I: Ring theory;
- Part II: Module theory.
- Part III: Field extensions and introduction to Galois theory;

References

- D. Dummit and R. Foote, *Abstract Algebra*, 3rd Edition, Parts II, III, IV;
- Frederick M. Goodman, “Algebra: Abstract and Concrete”, Edition 2.6, Chapters 6-10 (available online).

Outline

In this file: §1.1.

1. Review of basic definitions and examples of rings and fields;

§1.1 Review on Rings and fields

Definition. A ring is a set R together with two maps

$$R \times R \longrightarrow R : \quad (a, b) \longmapsto a + b,$$
$$R \times R \longrightarrow R : \quad (a, b) \longmapsto ab,$$

such that

1) $(R, +)$ is an abelian group with 0 denoting its identity element;
2) $(ab)c = a(bc)$ for all $a, b, c \in R$;
3) $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$ for all $a, b, c \in R$;
4) there exists $1 \in R$, $1 \neq 0$, such that $1a = a1 = a$ for all $a \in R$.

In this course we will mostly only deal with commutative rings, i.e., $ab = ba$ for all $a, b \in R$.

Definitions/facts.

- An element a in a ring R is called a unit if there exists $b \in R$ such that $ab = ba = 1$.
- The set of all units in a ring R is a group under multiplication in R.
- Two elements a and b in a commutative ring are said to be associates if $a = ub$ for some unit u in R.
- A field is a non-zero commutative ring F such that for any $a \in F, a \neq 0$, there exists $a^{-1} \in F$ such that $aa^{-1} = 1$.
- A field is thus a non-zero commutative ring in which every non-zero element is a unit.

Definitions.

- Let R be a ring. The characteristic of R, denoted by $\mathrm{char}(R)$, is the smallest positive integer n, if exists, such that

$$n \cdot 1 \stackrel{\text{def}}{=} \overbrace{1 + 1 + \cdots + 1}^{n} = 0.$$

  If such an integer does not exist, we say that $\mathrm{char}(R) = 0$.

- An element in a ring R is called a zero divisor if $a \neq 0$ and if there exists $b \in R\backslash\{0\}$ such that $ab = ba = 0$.

- A non-zero commutative ring R is called an integral domain if it has no zero divisor.

Lemma. If R is an integral domain, then $\mathrm{char}(R) = 0$ or a prime number.

Proof. Exercise.

Example: $R = \mathbb{Z}/n\mathbb{Z}$, where $n \geq 2$ is n integer. Have

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

- Case 1, n is prime: then $\mathbb{Z}/n\mathbb{Z}$ is a field. Indeed, for any $1 \leq k \leq n-1$, have $a, b \in \mathbb{Z}$ such that

$$ak + bp = 1,$$

  which implies that $\overline{a}\,\overline{k} = \overline{1}$.

- Case 2, n is not prime: if $n = ab$ with $1 < a, b < n$, then $\overline{a}$ and $\overline{b}$ are zero-divisors.

Definitions. Let R be a commutative ring.

- An ideal in R is a subset I of R closed under addition and such that $ab \in I$ whenever $a \in I$ and $b \in R$.

- An ideal I is said to be prime if $I \neq R$ and if for any $a, b \in R$, if $ab \in I$, then $a \in I$ or $b \in I$.

- An ideal I is said to be maximal if $I \neq R$ and if whenever M is an ideal in R such that $I \subset M \subset R$ then either $M = I$ or $M = R$.

- For $a \in R$, the ideal of R generated by a is denoted by aR or (a):

$$(a) = aR = \{ar : r \in R\},$$

  and is called a principal ideal of R.

Exercise: If R is an integral domain and $a, b \in R \backslash \{0\}$, then $(a) = (b)$ iff a and b are associates.

Counter ex: $\mathbb{Z}_6$, $2 = 2 \cdot 4$, $4 = 2 \cdot 2$, $(2) = (4)$

Definition of the quotient ring R/I: Let R be a commutative ring and $I \subset R$ an ideal. Define the equivalence relation on R by

$$r_1 \sim r_2 \quad \text{iff} \quad r_1 - r_2 \in I.$$

The set of equivalence classes $R/I = \{r + I : r \in R\}$ is a commutative ring:

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I, \qquad (r_1 + I)(r_2 + I) = r_1 r_2 + I,$$

and $R \to R/I : r \mapsto r + I$, is a ring homomorphism.

Example: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Lemma. Let R be a commutative ring and $I \subset R$ an ideal, $I \neq R$.

1. I is prime if and only if R/I is an integral domain;
2. I is maximal if and only if R/I is a field;
3. Maximal ideals are prime ideals;
4. The zero ideal $\{0\} \subset R$ is prime if and only if R is an integral domain, and $\{0\}$ is maximal if and only if R is a field.

Proof: Homework.

Definition of the field of fractions for an integral domain.

Let R be an integral domain. Define equivalence relation on $R \times (R \backslash \{0\})$:

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

and denote the equivalence class of (a, b) by $\frac{a}{b}$. Denote the set of all equivalence class by $\mathrm{Frac}(R)$, and define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Then $(\mathrm{Frac}(R), +, \cdot)$ is a field, called the fraction field of R, and

$$R \longrightarrow \mathrm{Frac}(R), \quad r \longmapsto \frac{r}{1}$$

is an injective ring homomorphism.

Example: $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$.

$\mathbb{F}[x] \longrightarrow \mathbb{F}(x)$

$\mathbb{F}[[x]] \longrightarrow \mathbb{F}((x))$

Constructions of new rings from old:

- Quotients by ideals.
- The sub-ring $\langle S \rangle$ of a ring R generated by a subset $S \subset R$:
  1. $\langle S \rangle$ is the smallest sub-ring of R contaning S;
  2. $\langle S \rangle$ is the intersection of all sub-rings of R containing S;
  3. $\langle S \rangle$ consists of all finite sums of products of elements in $\pm S$:

$$\langle S \rangle = \text{all finite sums of the form } s_1 s_2 \cdots s_n \text{ with } s_i \in \pm S.$$

Example: The sub-ring of $\mathbb{R}$ generated by $S = \mathbb{Z} \cup \{\sqrt{2}\}$ is

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} \qquad \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

$\mathrm{Frac}(\mathbb{Z}[\sqrt{2}]) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$

The polynomial ring $R[x]$:

Let R be a commutative ring. The ring of polynomials in x with coefficients in R is the set $R[x]$ consisting of all

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x],$$

where $a_0, a_1, \ldots, a_n \in R$ and $a_n \neq 0$.

- The degree of f is defined to be n and is denoted by $\deg(f)$.
- a_0 is the constant term of f and a_n the leading coefficient of f.
- Assume that R is an integral domain. Then for $f, g \in R[x]$ non-zero,
$$\deg(fg) = \deg(f) + \deg(g).$$
- For $f = 0$, define $\deg(f) = -\infty$.

As a consequence of

$$\deg(fg) = \deg(f) + \deg(g), \qquad f, g \in R[x],\ f \neq 0,\ g \neq 0,$$

we have

Lemma: Let R be an integra domain. Then

1. $R[x]$ is an integral domain;
2. $R[x_1, x_2] = R[x_1][x_2]$ is an integral domain;
3. For any integer $n \geq 1$,

$$R[x_1, x_2, \ldots, x_n] = R[x_1, \ldots, x_n][x_n]$$

is an integral domain.

4. If $F = \mathrm{FracR}$, then the fraction field of $R[x_1, x_2, \ldots, x_n]$ is

$$F(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, g_n)}{g(x_1, \ldots, x_n)} : f, g \in R[x_1, x_2, \ldots, x_n], g \neq 0 \right\}.$$

Examples of rings:

- Algebraic number theory: the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, consisting respectively of all integers, rational numbers, real numbers, and complex numbers, are commutative rings. All of them except $\mathbb{Z}$ are fields, and $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$.

- Sub-rings or quotient rings: for an integer $n \geq 1$,

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$

  is field if and only if n is a prime number; Also

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\} \quad \text{(the ring of Gaussian integers)},$$
$$\mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Q}\} \quad \text{(the field of Gaussian rationals)}.$$

Examples of rings:

- Polynomial rings: If R is a commutative ring, the multi-variable polynomial rings $R[x_1, \ldots, x_m] = R[x_1][x_2] \cdots [x_m]$ and their quotients lie at the foundation of Algebraic Geometry.

- Rings of functions: For a set X and $R = \mathbb{R}$ or $\mathbb{C}$, have function ring

$$\mathrm{Fun}(X; R) = \text{the set of all maps from } X \text{ to } R.$$

  When X is a topological space or a manifold, one has the sub-ring of continuous or differentiable functions on X.

- Matrix rings: if R is a ring, the set of all $n \times n$ matrices with entries in R is naturally a (typically non-commutative) ring with standard matrix addition and multiplication.

- Rings of formal power series $R[[x]]$: To be covered in tutorial.