Study Notes of Topology

Pei Zhong

Update on November 23, 2023

Contents

Preface

The notes mainly refer to the following materials:

- Abstract Algebra by Sun Zhiwei
- lecture notes from berkeley
- algebra II notes from mit
- algebra I notes from mit
- lecture notes by feog

Part I

Group Theory

Part II

Ring Theory

Chapter 1

The Concept and Basic Properties of Rings

Definition 1.1

A ring is a set R endowed with addition and multiplication, usually denote " $+$ " and " $\cdot$ ", satisfying (1)-(3):
(1) R is an abelian group with respect to addition : addition is associative and commutative, there is an additive identity 0_R such that $0_R + a = a + 0_R = a$ for all $a \in R$, and every element has an additive inverse.
(2) R is an semigroup with respect to multiplication : Multiplication is associative.
(3) Addition and multiplication satisfy distributivity: for all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ (b + c) \cdot a = b \cdot a + c \cdot a.$$

Most often we will also impose some additional conditions on our rings, as follows:

(4) There exists an element, denoted 1, which has the property that $a \cdot 1 = 1 \cdot a = a$ for all a in R, 1 is called the unity of R.
A ring satisfying (4) is called a ring with unity (or sometimes a unital ring).

(5) multiplication is commutative : $a \cdot b = b \cdot a$ for all $a, b \in R$.
A ring satisfying (5) is called a commutative ring.

Remark. We always denote $a \cdot b$ by ab.

Remark. As usual we use exponents to denote compounded multiplication; associativity guarantees that the usual rules for exponents apply. However, with rings (as opposed to multiplicative groups), we must use a little caution, since a^k may not make sense for $k < 0$, as a is not guaranteed to have a multiplicative inverse.

Definition 1.2

Let a, b be in a ring R. If $a \neq 0$ and $b \neq 0$ but $ab = 0$, then we say that a and b are zero divisors. A commutative unital ring without zero divisors is called integral domain.

There are many familiar examples of rings:

Example 1.1: The ring of integers

$\mathbb{Z}$: the integers ..., $-2, -1, 0, 1, 2$, ..., with usual addition and multiplication, form a ring.

Example 1.2: The ring of residue classes modulo n

$\mathbb{Z}/n\mathbb{Z}$: The integers mod n. These are equivalence classes of the integers under the equivalence relation "congruence mod n". If we just think about addition, this is exactly the cyclic group of order n. However, when we call it a ring, it means we are also using the operation of multiplication.

$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nZ \to \mathbb{Z}/nZ$ is given by $\overline{a} + \overline{b} = \overline{a+b}$. $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nZ \to \mathbb{Z}/nZ$ is given by $\overline{a}\overline{b} = \overline{ab}$.

Example 1.3: The ring of integer polynomials

$\mathbb{Z}[x]$: this is the set of polynomials whose coefficients are integers. It is an "extension" of $\mathbb{Z}$ in the sense that we allow all the integers, plus an "extra symbol" x, which we are allowed to multiply and add, giving rise to x^2, x^3, etc., as well as $2x, 3x$, etc. Adding up various combinations of these gives all the possible integer polynomials.

Example 1.4: The ring of matrices

$M_n(\mathbb{R})$ (non-commutative): the set of $n \times n$ matrices with entries in $\mathbb{R}$. These form a ring, since we can add, subtract, and multiply square matrices. This is the first example we've seen where the order of multiplication matters: AB is not always equal to BA (usually it's not).

Remark. Similar with example**??** and example**??**, for ring R, we can define $R[x]$ as the set of polynomials whose coefficients are in the field of R and $M_n(R)$ the set of $n \times n$ matrices with entries in the field of R. Since, $R[x]$ an "extension" of R, they have many similar properties:

- If R is unital ring, then $R[x]$ is unital ring.
- If R is commutative ring, then $R[x]$ is commutative ring.
- If R is integer domain, then $R[x]$ is integer domain.

However, there are many difference between R and $M_n(R)$.

- If R is unital ring, then $M_n(R)$ is unital ring.
- If R is a commutative ring, $M_n(R)$ may not be a commutative ring.
- If R is an integer domain, $M_n(R)$ may not be an integer domain.

Chapter 2

Homomorphism and Ideals

Just as with groups, when we study rings, we are only concerned with functions that “preserve the structure” of a ring, and these are called ring homomorphisms. Maybe you can guess what the definition should be, by analogy with the case of groups.