Ring Theory

S. William

1 Basic Concepts

We show the definition of general rings.

Definition 1.1 (Ring) *A ring R is an Abelian group with $+$ and zero 0, together with another binary operation $*$ such that for all $a, b, c \in R$,*

*1) a *(b*c) = (a*b) * c*

*2) a * (b+c) = (a*b) + (a*c)*

*3) (a+b) * c = (a*c) + (b*c)*

As usual, we denote $ab = a * b$.

It is easy to see $0a = a$. The identity of a ring is denoted always with 1 (or 1_R for emphasizing the ring), that $1a = a1 = a$. A ring with 1 is called a unitary ring, but we are used to saying ring has 1. Moreover, an integer n in a ring means $\overbrace{1 + 1 + \cdots + 1}^{n}$.

Remark 1.1 (Rng and Ring) *We claim that rings must have $1 \neq 0$. A ring unnecessarily possessing 1 should be called a rng (or rong) that will be used in the ideal theory. A rng can be embedded into a ring. Let R be a rng and $R' = \{(r, n), r \in R, n \in \mathbb{Z}\}$ with the multiplication $(r, m)(s, n) = (rs + ms + nr, mn)$, then R' is a ring with the identity $(0, 1)$ and $R \subset R'$ up to isomorphism.* Rng *and* Ring *denote the category of rngs and the category of rings respectively and $R \mapsto R'$ is the functor.*

Ring is a (not full) sub-category of Rng. The homomorphisms of Ring are homomorphisms of Rng mapping 1 in a ring to 1 in another ring.

Remark 1.2 *More general then ring is so-called semiring where $(R, +)$ is a commutative semigroup (or monoid) in Definition 1.1.* $\mathbb{N}$ *is a semiring.*

Left (right) zero divisors are the elements that $ax = 0$ ($xa = 0$) for some $x \neq 0$. 0 is a trivial zero divisor. Zero divisors are both left and right zero divisors. 1 is not a zero divisor.

Definition 1.2 *A commutative ring R is a ring that $ab = ba$ for all $a, b \in R$. A domain R is a commutative ring that has no zero divisors.*

Example 1.1 *$\mathbb{Z}$ is most common number ring. Other number rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. Set of $n \times n$ complex matrices $\mathbb{C}^{n\times n}$ is a ring. Based on a given ring, we can construct new rings. $\mathcal{M}_n(R)$ is the matrix ring on R, $R[x]$ is the polynomial ring, $R[x, x^{-1}]$ is the Laurent polynomial ring, $R[[x]]$ is the ring of formal series, direct sum of rings is a ring and R^X the set of R-valued functions is also a ring.*

In the following discussion, rings are commutative.

Definition 1.3 *In a ring R, if there is some $c \in R$ that $b = ca$, then a divides exactly b, denoted with $a \mid b$. a is called the divisor of b. The set of divisors of b is denoted with $D(b)$. a divides properly b, if $a \mid b$ but $b \nmid a$.*

Definition 1.4 *A unit in R is an invertible element that for some $c \in R, 1 = ca$ or $a \mid 1$. $U(R)$ denotes the set of units in R. It is indeed a group. a associates with b, denoted as $a \sim b$, means for some $c \in U(R)$ that $a = cb$, namely $a \mid b$ and $b \mid a$. Thus $a \in U(R)$ iff $a \sim 1$.*

Obviously, $a \mid b$ is a po and $a \sim b$ is an equivalent relation.

Note that a divides properly b means for some $c \notin U(R)$ that $a = cb$, also say b is a proper divisor of a. The set of proper divisors of a is denoted as $D^*(a)$. For convenience, sometimes $D(S)$ refers to the common divisors of the set S. Moreover, unites and elements associating a must divides a, that are called ordinary divisors, while others called inordinacy divisors denoted with $D^+(a)$.

Definition 1.5 *p is a prime element of R, if it is not zero or a unit and if $p \mid ab$ for some $a, b \in R$, then $p \mid a$ or $p \mid b$.*

If $D^\sharp(a)$ denotes the set of prime divisors or a, then $D^\sharp(a) \cup D^\sharp(b) = D^\sharp(ab)$.

Definition 1.6 *p is an irreducible element of R, denoted $p \in \mathrm{Irr}(R)$, if p cannot be written as an product of elements $\prod_i a_i$ that $a_i \mid p$ properly. Simply speaking, if $p = ab$, then $a \sim p$ (meanwhile $b \in U(R)$) or $b \sim p$ (meanwhile $a \in U(R)$), namely p only has ordinary divisors, write $D(p) = pU(R) \cup U(R)$.*

In an integral domain (domain for short), every prime is irreducible but the converse is not true in general. However, in unique factorization domains, or more generally in GCD domains, primes and irreducibles are the same.

In commutative rings, we have Euclidean domain $\Rightarrow$ principal ideal domain $\Rightarrow$ unique factorization domain $\Rightarrow$ GCD domain $\Rightarrow$ Schreier domain $\Rightarrow$ (integral) domain. principal ideal domain $\Rightarrow$ Bézout domain $\Rightarrow$ GCD domain.

Definition 1.7 *a unique factorization domain (UFD) is a commutative ring in which every non-zero non-unit element can be written as a product of irreducible elements (prime elements), uniquely up to order and units.*

Lemma 1.1 *If R is a domain, then it is a unique factorization domain iff it is factorized and the irreducible elements $\mathrm{Irr}(R)$ are prime. Note that a ring is factorized if every non-zero non-unit element can be decomposed into the product of irreducible elements.*

Lemma 1.2 *In UFDs, $D^\sharp(a) \cap D^\sharp(b) = \emptyset$ iff a, b are coprime.*

Definition 1.8 *A ring is a division ring, if all elements are unites except 0. If it is as well as commutative, then it is a field.*

2 Ideal

Ideal may be the most important concept in the ring theory.

Definition 2.1 (Ideal) *Given I a left (right) ideal of a general ring R, if it is a sub-rng of R and $RI \subset R$ ($IR \subset I$). An (two-sided) ideal is a both left and right ideal.*

Thus, a left (right) ideal can be seen as an invariant sub-rng under the left (right) multiplication. It is easy to see that $I \cap J, I + J$ are ideals where I, J are ideals of a ring.

We introduce some simple kinds of ideals.

Definition 2.2 *Generated ideal by S, $(S) = \bigcap\{S \subset I, I \text{ is an ideal}\}$. If S is finite, then (S) is called the finitely generated ideal. Specially when $S = \{a\}$, (a) is called the principal ideal that can be expressed explicitly as $\{\sum_{i,j<\infty} r_i a r_j + r_k a + a r_l + na, n \in \mathbb{Z}, r_i, r_j, r_k, r_l \in R\}$. If R has 1 (be a ring), then $(a) = RaR = \{\sum_{i,j<\infty} r_i a r_j, r_i, r_j \in R\}$, generally $(S) = RSR$.*

$\{0\}, R$ are two trivial ideas. Others are called the nontrivial ideas. In a ring R, $I = R$ iff $1 \in I$, namely $(1) = I$ so as an ideal R is also called the unit ideal. Proper ideals refer to the ideals except R.

Before we show the ideals, we denote the quotient rings with R/I that is defined as in Abelian groups where I is an ideal of R. Notice that if R is a (commutative) ring then R/I is also a (commutative) ring.

Definition 2.3 (Ideals and their basic properties) *A proper ideal I is called a maximal ideal if there exists no other proper ideal J with I a proper subset of J. The factor ring of a maximal ideal R/I is a simple ring in general and is a field for commutative rings. A nonzero ideal is called minimal if it contains no other nonzero ideal.*

Prime ideal: A proper ideal I is called a prime ideal if for any a and b in R, if $ab \in I$, then $a \in I$ or $b \in I$. The factor ring of a prime ideal R/I is a prime ring in general and is an integral domain for commutative rings.

Primary ideal: An ideal I is called a primary ideal if for all $a, b \in R$, if $ab \in I$, then at least one of $a \in I$ or $b^n \in I$ for some natural number n. Every prime ideal is primary, but not conversely. A semiprime primary ideal is prime.

Irreducible ideal: An ideal is said to be irreducible if it cannot be written as an intersection of ideals which properly contain it. Every prime ideal is irreducible. Every irreducible ideal of a Noetherian ring is a primary ideal, and consequently for Noetherian rings an irreducible decomposition is a primary decomposition. Every primary ideal of a principal ideal domain is an irreducible ideal. Every irreducible ideal is a primal ideal.

Coprime ideals: Two ideals I, J are said to be coprime if $a + b = 1$ for some $a \in I, b \in J$.

Nil ideal: An ideal is a nil ideal if each of its elements is nilpotent.

Remark 2.1 *Primitive ideal: A left primitive ideal is the annihilator of a simple left module. A right primitive ideal is defined similarly. Actually (despite the name) the left and right primitive ideals are always two-sided ideals. Primitive ideals are prime. A factor rings constructed with a right (left) primitive ideals is a right (left) primitive ring. For commutative rings the primitive ideals are maximal, and so commutative primitive rings are all fields.*

We turn to the commutative rings (with 1**).** In such rings, the principal ideal $(a) = Ra = aR$. And $(a) \subset (b)$ iff $b \mid a$, $(a) = (b)$ iff $a \sim b$. the facts translate the concepts of number theory to the ring theory. Furthermore, we have the following results.

Theorem 2.1 *(p) is prime iff p is prime. (p) is irreducible iff p is irreducible.*

The principal ideals of a ring is an opset under $\subset$. Now we define the well-known great common divisor.

Definition 2.4 (Great common divisor) *If $(S) = (a)$, then a is the gcd(great common divisor) of S.*

Tabel 1 shows the correspondence of three types of statements that are employed in different contexts.

3 Ring Extension

If R is a subring (or a ring isomorphic to a subring) of ring S, then S/R denotes the ring extension. In the definition, we can not get something more than subring concept. Howsoever, it indicates that we can study a ring at the position of its sup-ring.

Remark 3.1 *The ring extension can be regarded as a category denoted with **Rxt** (**Rxt**$_R$ if R is fixed). The homomorphism $\phi : S/R \to S'/R'$ is the homomorphism*

Table 1: The correspondence of three styles of statements

ideal style	number style	set style
$(a) \subset (b), a \in (b)$ (properly)	$b \mid a$ (properly)	$b \in D(a)\,(b \in D^*(a))$
$(a, b) = (1)$	a, b is coprime	$D(\{a, b\}) = U(R)$
$(a) = (b)$	$a \sim b$	$D(a) = D(b)$
$(a) = (1), 1 \in (a)$	$a \sim 1, a \mid 1$	$a \in U(R), D(a) = U(R)$
$a \in (0)$	$a = 0$	$D(0) = \{0\}, 0 \notin D(b), b \neq 0$
$(S) \subset (a)$	$a \mid S$	$a \in D(S)$
$(S) = (a)$		a is the gcd of S

$\phi : S \to S'$ that $\phi|_R : R \to R'$ is a homomorphism. When $\phi, \phi|_R$ are both isomorphisms, ϕ is the isomorphism of ring extension. Particularly, if an homomorphism (isomorphism) of R that $\phi|_R = \mathrm{id}_R$, then it is called Galois homomorphism (isomorphism). $\mathrm{Gal}(S/R)$ *denotes the group of Galois isomorphisms.*

Before going further, we introduce the following theorem that is a fundamental principle for ring extension. In fact, it indicates the morphism of **Rxt**.

Theorem 3.1 (Embedding Theory) *If R is a subring of S, $(S \setminus R) \cap R' = \emptyset, R \simeq R'$, then there exists $S \simeq S', R'$ is a subring of S'. We say R' is embedded into S and S/R' is a ring extension up to isomorphisms.*

Proof. Take $S' = (S \setminus R) \cup R'$. It is indeed a ring. Now let

$$\psi(x) = \begin{cases} \phi(x) & x \in R, \\ x & x \in S \setminus R. \end{cases} : S \to S' \text{ where } \psi : R \simeq R'.$$

It is easy to check that $\psi : S \simeq S'$. The detail is left for readers. □

Following is an interesting application.

Corollary 3.1 *Let R be a commutative ring and let $1 \in D$ be a multiplicatively closed subset of R without 0 or any zero divisors. Define the (total) ring of fractions of D as $D^{-1}R = \{a/p, a \in R, p \in D\}$ where $a/p \sim b/q$ means $qa = pb$. Then $D^{-1}R$ is a ring and an extension of R.*

Proof. We denote $\frac{a}{p} \in D^{-1}R$ as usual. Let $S = D^{-1}R$. It is easy to see $R \simeq \{\frac{r}{1}, r \in R\}$ is a subring of S. We have extension S/R. □

Example 3.1 *Laurent polynomial* $R[x, x^{-1}] = \{x^n, n \in \mathbb{N}\}^{-1}R[x]$.

Moreover, D regarded as $\{\frac{d}{1}, d \in D\}$ consists of units of S. Now define $\mathrm{Frac}(R) = D^{-1}R$ where $D = R \setminus \{0\}$ for the domain R. $\mathrm{Frac}(R)$ is a field — the field of fractions with respective to R. Fields of fractions are applied in the polynomials. One also see that Frac is a functor from the category of domains to the category of fields.

Remark 3.2 *Consider the general version — localization. Let R is a general commutative ring (rng) and $1 \in D$ be a multiplicatively closed subset. Denote $S = D \times R/\sim$ where $(a,p) \sim (b,q)$ means there exists $t \in D$ that $t(qa-pb) = 0$. We have the universal property: the ring homomorphism $j : R \to S$ maps every element of S to a unit in S, and if $f : R \to T$ is some other ring homomorphism which maps every element of S to a unit in T, then there exists a unique ring homomorphism $g : S \to T$ such that $f = gj$.*

Remark 3.3 *It is easy to define rng extension. In Remark 1.1, R'/R is an example of rng extension.*

4 Polynomial

It is easy to see that ploynomial rings also give ring extension. For the domain extension S/R, $a \in S$ is integral over R iff a is a root of $f(x) \in R[x]$ called the annihilation polynomial of a usually. The annihilation polynomials form an ideal of $F[x]$. The set of integral elements over R is a subring of S, named integral closure of R. If the integral closure of R is R itself, then R is integrally closed.

Keep in mind that we only study the polynomials of commutative rings.

Theorem 4.1 *If R is UFD, then so is $R[x]$.*

Definition 4.1 *Let $f(x) = \sum_i a_i x^i$, then $c(f) = (\{a_i\})$. If $c(f) = (1)$, then f is named the primitive polynomial.*

Actually, the definition is only useful when R is a domain.

Lemma 4.1 (Gauss) *If $f, g \in R[x]$ are primitive, then fg is primitive, where R is an integral domain.*

5 Comment

In rings, an ideal is proper if and only if it does not contain 1 or equivalently it does not contain a unit. The set of ideals of any ring are partially ordered via subset inclusion, in fact they are additionally a complete modular lattice in this order with join operation given by addition of ideals and meet operation given by set intersection. The trivial ideals supply the least and greatest elements: the largest ideal is the entire ring, and the smallest ideal is the zero ideal. The lattice is not, in general, a distributive lattice. Unfortunately Zorn's lemma does not necessarily apply to the collection of proper ideals of R. However when R has identity 1, this collection can be reexpressed as "the collection of ideals which do not contain 1". It can be checked that Zorn's lemma now applies to this collection, and consequently there are maximal proper ideals of R. With a little more work, it can be shown that every proper ideal is contained in a maximal ideal. See Krull's theorem at

maximal ideal. The ring R can be considered as a left module over itself, and the left ideals of R are then seen as the submodules of this module. Similarly, the right ideals are submodules of R as a right module over itself, and the two-sided ideals are submodules of R as a bimodule over itself. If R is commutative, then all three sorts of module are the same, just as all three sorts of ideal are the same. Every ideal is a pseudo-ring. The ideals of a ring form a semiring (with identity element R) under addition and multiplication of ideals.

6 More Rings

Definition 6.1 (Rings with endomorphisms or anti-endomorphisms) *A ring R with a set Φ of its endomorphisms or anti-endomorphisms are called the $\Phi-$ring (σ-ring denotes $\{\sigma\}$-ring). Specially $*$-ring R^* is a ring with an anti-automorphism $*$ called conjugate. Ring* denotes the category of $*$-rings with homomorphisms of rings that $\phi(a^*) = \phi(a)^*, a \in R$.*

Definition 6.2 $\Re a = \frac{a^*+a}{2}$ *where* 2 *invertable in *-ring* R *(or* $2|a^* + a$*).*

Let $Her(R) = \{a \in R \,|\, a = a^*\} = \Re[R]$. $R/Her(R)$ is a ring extention.

Fact 6.1 *For any $x \in R$, we have $x = a + bi$, where $a, b \in Her(R), i^* = -i$.*

References