Lectures Notes in Ring Theory

MOHAMMED ALABBOOD

University of Basrah-College of Science
Department of Mathematics

January 20, 2020

Ring

A **ring** is an ordered triple $(R, +, \cdot)$ such that R is a nonempty set and $+$ and $\cdot$ are two binary operations on R satisfying the following axioms:
(1) $(R, +)$ is abelian group,
(2) $(R, +)$ is semigroup,
(3) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$.

During the development of the theory of rings, multiplication is assumed to be performed before addition and we call 0, the **zero element** of the ring $(R, +, \cdot)$, and we write ab for $a \cdot b$, we write $a - b$ for $a + (-b)$. As an example, $ab + c$ stands for $(a \cdot b) + c$.

Commutative ring with unity

- A ring $(R, +, \cdot)$ is called **commutative** if $ab = ba$ for all $a, b \in R$. A ring $(R, +, \cdot)$ which is not commutative is called a **noncommutative ring**.
- For a ring $(R, +, \cdot)$, the set $C(R) = \{a \in R : ab = ba \text{ for all } b \in R\}$ is called the **center of** R. It follows that a ring R is commutative if and only if $R = C(R)$.
- Let $(R, +, \cdot)$ be a ring. An element $u \in R$ is called a **unity** if $ua = a = au$ for all $a \in R$. Note that a unity of a ring R (if it exists) is an identity element of the semigroup $(R, \cdot)$. Therefore, a ring cannot contain more than one unity. A unity of a ring (if it exists) is denoted by 1. In this case, A ring R is called a **ring with unity**. From now on, we assume that the identity element 1 (if it exists) is different from the zero element of the ring. It follows that if R is a ring with 1, then R has at least two elements, namely the additive and multiplicative identities.

Skew-field and field

- Let $(R, +, \cdot)$ be a ring with 1. An element $v \in R$ is called a **unit (or an invertible element)** if there exists $v' \in R$ such that $v'v = 1 = vv'$.
- A ring $(R, +, \cdot)$ with 1 is called a **division ring (skew-field)** if every nonzero element of R is a unit. A commutative division ring R is called a **field**.
- Note that a ring $(R, +, \cdot)$ is a division ring (or skew-field) if and only if $(R\backslash\{0\}, \cdot)$ is a group. Therefore, if $(R, +, \cdot)$ is a division ring, then for all $a \in R, a \neq 0$, there exists a unique element, denoted by $a^{-1} \in R$, such that $aa^{-1} = 1 = a^{-1}a$. We call a^{-1} the **multiplicative inverse** of a. In a similarly manner, a ring $(R, +, \cdot)$ is a field if and only if $(R\backslash\{0\}, \cdot)$ is a commutative group.

Integral domain

- A nonzero element a in a ring $(R, +, \cdot)$ is called a **zero divisor** if there exists $b \in R$ such that $b \neq 0$ and either $ab = 0$ or $ba = 0$. Not that an element in a ring R cannot be a unit and zero divisor at the same time. Thus, a field has no zero divisors.
- Let $(R, +, \cdot)$ be a commutative ring with 1. Then R is called an **integral domain** if R has no zero divisors.
- Let $(R, +, \cdot)$ be a ring. It is not difficult to prove that if R has no zero divisors, then the cancellation laws hold, i.e., for all $a, b, c \in R, a \neq 0, ab = ac$ implies $b = c$ (**left cancellation law**) and $ba = ca$ implies $b = c$ (**right cancellation law**). Moreover, if either cancellation law holds, then R has no zero divisors.
- A ring $(R, +, \cdot)$ is called a **finite ring** if R has only a finite number of elements; otherwise R is called an **infinite ring**.

Characteristic of a ring

- Let $(R, +, \cdot)$ be a ring. If there exists a positive integer n such that for all $a \in R, na = 0$, then the smallest such positive integer is called the **characteristic of** R. If no such positive integer exists, then R is said to be of **characteristic zero**. Note that the characteristic of an integral domain R is either zero or a prime.
- An element a in a ring $(R, +, \cdot)$ is called **idempotent** if $a^2 = a$ and **nilpotent** if $a^n = 0$ for some positive integer n.
- Let R and R' be rings. Define $+$ and $\cdot$ on $R \times R'$ by for all $(a, b), (c, d) \in R \times R', (a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$. Then $(R \times R', +, \cdot)$ is a ring which is called the **direct sum of** R **and** R' and is denoted by $R \oplus R'$.
- A ring R with 1 is called a **Boolean ring** if every element of R is an idempotent.

Subring and subfield and ideals

- Let $(R,+,\cdot)$ be a ring. Let R' be a subset of R. Then $(R',+,\cdot)$ is called a **subring** of $(R,+,\cdot)$ if $(R',+)$ is a subgroup of $(R,+)$, (2) for all $x,y\in R', x\cdot y\in R'$. When R' and R are fields, R' is called a **subfield** of R. Note that if R is a ring and R' is a nonempty subset of R, then R' is a subring of R if and only if $x-y\in R'$ and $xy\in R'$ for all $x,y\in R'$. Now if F is a field and S is nonempty subset of F, then S is a subfield of F if and only if (1) S contains more than one element, (2) $x-y, xy\in S$ for all $x,y\in S$, (3) $x^{-1}\in S$ for all $x\in S, x\neq 0$.
- It easy to prove that the intersection of any nonempty family of subrings (subfields) of a ring (field) R is a subring (subfield) of R.
- Let R be a ring. Let I be a nonempty subset of R. Then (1) I is called a **left ideal** of R if for all $a,b\in I$ and for all $r\in R, a-b\in I, ra\in I$, (2) I is called a **right ideal** of R if for all $a,b\in I$ and for all $r\in R, a-b\in I, ar\in I$, (3) I is called a **(two-sided)ideal** of R if I is both a left and a right ideal of R.

Ideals

- From the above definition of a left (right) ideal, it follows that if I is a left (right) ideal of R, then I is a subring of R. Also, if R is a commutative ring, then every left ideal is also a right ideal and every right ideal is a left ideal. Thus, for commutative rings every left or right ideal is an ideal.
- Let R be a ring. The subsets $\{0\}$ and R of R are (left, right) ideals. These ideals are called **trivial** ideals. All other (left, right) ideals are called **nontrivial**.
- An ideal I of a ring R is called a **proper ideal** if $I \neq R$.
- It is clear that the intersection of any nonempty collection of left (right) ideals of a ring R is again a left (right) ideal of R.
- if S is a nonempty subset of a ring R then (1) we define $\langle S \rangle_l$ to be the intersection of all left ideals of R and contain S. In fact, $\langle S \rangle_l$ forms a left ideal of R which is called the **left ideal generated by** S, (2) we define $\langle S \rangle_r$ to be the intersection of all right ideals of R and contain S. In fact, $\langle S \rangle_r$ forms a right ideal of R which is called the **right ideal generated by** S.

Finitely generated ideal and principal ideal

- We define $\langle S \rangle$ to be the intersection of all ideals of R which are both right and left ideals of R and contain S. In fact, $\langle S \rangle$ forms an ideal of R which is called the **ideal generated by** S.
- If $S = \{a_1, a_2, \ldots, a_n\}$, then the left $\langle S \rangle_l$, $\langle S \rangle_r$ and $\langle S \rangle$ are denoted by $\langle a_1, a_2, \ldots, a_n \rangle_l$, $\langle a_1, a_2, \ldots, a_n \rangle_r$ and $\langle a_1, a_2, \ldots, a_n \rangle$ respectively. In this case, we call $\langle S \rangle_l$ a **finitely generated left ideal**, we call $\langle S \rangle_r$ a **finitely generated right ideal**, and we call $\langle S \rangle$ a **finitely generated ideal**. As a special case, if $S = \{a\}$, then (1) $\langle a \rangle_l$ is called the **principal left ideal generated by** a, (2) $\langle a \rangle_r$ is called the **principal right ideal generated by** a, (3) $\langle a \rangle$ is called the **principal ideal generated by** a.
- It is not difficult to prove that if R is a commutative ring with 1, then R is a field if and only if R has no nontrivial ideals.
- A ring R is called a **simple ring** if $R \neq \{0\}$ and $\{0\}$ and R are the only ideals of R.

Quotient ring, nil and nilpotent ideal

- Let A and B be two nonempty subsets of a ring R. Define the **sum and product of A and B** as follows:

$$A+B=\{a+b : a\in A, b\in B\},$$
$$AB=\{a_1b_1+\cdots+a_nb_n : a_i\in A, b_i\in B, i=1,2,\ldots,n, n\in\mathbb{N}\}.$$

Thus, AB denotes the set of all finite sums of the form $\sum a_ib_i, a_i\in A, b_i\in B$. Let $n\in\mathbb{N}$. Inductively, we define (1) $A^1=A$, (2) $A^n=AA^{n-1}, n>1$.

- If R is a ring and I is an ideal of R, then the ring $(R/I,+,\cdot)$ is called the **quotient ring of R by I**, where R/I denotes the set of all cosets $x+I=\{x+a : a\in I\}$ for all $x\in R$, and $(x+I)+(y+I)=(x+y)+I$, $(x+I)\cdot(y+I)=xy+I$.

- Let I be an ideal of a ring R. Then (1) I is called a **nil ideal** if each element of I is a nilpotent element, (2) I is called a **nilpotent ideal** if $I^n=\{0\}$ for some positive integer n. From the definition, it follows that every nilpotent ideal is a nil ideal.

Annihilator of an ideal, homomorphism of rings

- Let I be an ideal of a commutative ring R. Define the **annihilator** of I to be the set $\text{ann}(I) = \{r \in R : ra = 0 \text{ for all } a \in I\}$. It easy to prove that $\text{ann}(I)$ is an ideal of R.
- Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be rings, and let f be function from R into R'. Then f is called a **homomorphism** of R into R' if $f(a + b) = f(a) +' f(b)$, $f(a \cdot b) = f(a) \cdot' f(b)$ for all $a, b \in R$.
- A homomorphism f of a ring R into a ring R' is called (i) a **monomorphism** if f is one-one, (2) an **epimorphism** if f is onto R', and (3) an isomorphism if f is one-one and maps R onto R'. An isomorphism of a ring R onto R is called an **automorphism**. Two rings R and R' are said to be **isomorphic** if there exists an isomorphism of R onto R' (In this case, we write $R \simeq R'$).
- Let f be a homomorphism of a ring R into a ring R'. Then the **kernel** of f, written $\ker f$, is defined to be the set $\ker f = \{a \in R : f(a) = 0'\}$, where $0'$ denote the additive identity of R'. It is clear that $\ker f$ is an ideal of R.

The fundamental theorem of a ring homomorphism

- Let R be a ring and I be an ideal of R. Define the mapping $\eta : R \to R/I$ by $\eta(a) = a + I$ for all $a \in R$. Then η is a homomorphism, called the **natural homomorphism**, of R onto R/I. Furthermore, $\ker \eta = I$.
- As in the group theory, we have the following theorems (1) **The fundamental theorem of homomorphisms for rings**: Let f be a homomorphism of a ring R into a ring R'. Then $f(R)$ is an ideal of R' and $R/\ker f \simeq f(R)$, (2) **Correspondence Theorem**: Let f be a homomorphism of a ring R onto a ring R'. Then f induces a one-one inclusion preserving correspondence between the ideals of R containing $\ker f$ and the ideals of R' in such a way that if I is an ideal of R containing $\ker f$, then $f(I)$ is the corresponding ideal of R', and if I' is an ideal of R', then $f^{-1}(I')$ is the corresponding ideal of R.

Embedding and quotient field

- A ring R is said to be **embedded** in a ring S if there exists a monomorphism of R into S. It follows that a ring R can be embedded in a ring S if there exists a subring T of S such that $R \simeq T$. In fact, any ring R can be embedded in a ring S with 1 such that R is an ideal of S. Furthermore, (1) if R is a commutative ring with no zero divisors, then R can be embedded in an integral domain, (2) any integral domain R can be embedded in a field. Let R be an integral domain. A field F is called a **quotient field of R or a field of quotients of R** if there exists a subring R' of F such that $R \simeq R'$ and for all $x \in F$, there exists $a, b \in R'$ with $b \neq 0$ such that $x = ab^{-1}$.