Salahaddin University-Erbil, College of Science,
Department of Mathematics

Lecture

Non-Commutative Algrbra

MSc Level

Prof. Dr. Abdullah M. Abdul-Jabbar

3 units per week

2023-2024

Chapter 1

Rings with some properties

Def. 1.1: (Rings)

Let $R \neq \phi$ and *, o be two operations defined on R. Then, (R, *, o) is a ring if

(1) (R, *) is an abelian group.

(2) (R, o) is a semi-group.

(3) o is distributive over * from both sides.

Remark 1.2: To simplicity we use (R, +, .) instead of (R, *, o), but +, . are not usual addition and multiplication always.

The definition of rings by other way:

Def. 1.3: (Rings)

A ring (R, +, .) is a non empty set of R with two operations +, . such that

(1) $\forall$ a, b $\in$ R, a+b $\in$ R (closure law w.r.to +).

(2) $\forall$ a, b, c $\in$ R,

a+(b+c) = (a+b)+c (associative law w.r.to +).

(3) $\exists$ 0 $\in$ R such that

a+0 = 0+a = a, $\forall$ a $\in$ R,

(0 is the identity element w.r.to +).

(4) $\forall$ a $\in$ R, $\exists$ -a $\in$ R such that

(a)+(-a) = (-a)+(a) = 0,

(-a is the inverse element of a w.r.to +).

(5) $\forall$ a, b $\in$ R, a+b = b+a (abelian or commutative law w.r.to +).

(6) $\forall$ a, b $\in$ R, a.b $\in$ R (closure law w.r.to .).

(7) $\forall$ a, b, c $\in$ R,

a.(b.c) = (a.b).c (associative law w.r.to .).

(8) $\forall$ a, b, c $\in$ R,

a. (b+c) = a.b+a.c (distributive law from the left)

(b+c).a = b.a+c.a. (distributive law from the right).

Def. 1.4: (commutative ring)

A ring (R, +, .) is called commutative if a.b = b.a, $\forall$ a, b $\in$ R.

Def. 1.5: (ring with unity)

A ring (R, +, .) is called a ring with unity (identity) if there exists 1 $\in$ R such that a.1 = 1.a =a, $\forall$ a $\in$ R.

Example 1.6:

(**Z**, +, **.**), the ring of integers.

(**Q**, +, **.**), the ring of rational numbers.

(**R**, +, **.**), the ring of real numbers.

($\mathbf{Z}_n$, $+_n$, $\cdot_n$), the ring of integers modulo n.

Q 1.7 (H.W.): Is ($\mathbf{I}_{rr}$, +, **.**) a ring or not ?

Q 1.8 (H.W.): Let X be a non-empty set,

P(X): A collection of all subsets of X (power set of X)

For each A, B $\in$ P(X). Define the operation Δ as follows:

A Δ B = (A-B) $\cup$ (B-A).

Is (P(X), Δ, $\cap$) a commutative ring with identity ? Explain it.

Q 1.9 (H.W.): Let

$$M_{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \right\}$$

Show that ($M_{2\times 2}$, +, .) is a ring with identity, but not commutative, where **R** is the set of real numbers.

Q 1.10 (H.W.): Let

$$M_{nn} = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} : a_{ij} \in \mathbf{R} \quad \forall\, i = 1, 2, \dots, n \text{ and } \forall\, j = 1, 2, \dots, n \right\}$$

Show that $M_{nn}(\mathbf{R})$, +, .) is a ring with identity, but not commutative, where **R** is the set of real numbers.

Def. 1.11: If R is a ring and $0 \neq a \in R$, then a is called a left (right) zero divisor in R if there exists $0 \neq b \in R$ such that ab = 0 (ba = 0).

A zero divisor is any element of R, that is either a left zero divisor or right zero divisor.

Ex. 1.12: ($\mathbf{Z}_6$, $+_6$, $._6$) has zero divisor since $2 \neq 0$, $3 \neq 0$ implies $2.3 = 0$.

Whence, ($\mathbf{Z}_n$, $+_n$, $._n$) has zero divisor if n is not prime number.

Ex. 1.13: 0 is not a zero divisor.

Def. 1.14: A ring (R, +, .) has no zero divisor if

$a \neq 0$, $a.b = 0 \Rightarrow b = 0$.

Or, $a.b = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

Q 1.15 (H.W.): Give an example of zero divisor for non commutative ring.

Th. 1.16 (H.W.): Let (R, +, .) be a ring without zero divisor **iff** the cancellation law holds for multiplication.

Def. 1.17: If (R, +, .) is a ring, then

na = a+a+…+a, $\forall$ a $\in$ R.

Remark 1.18: (mn)a = m(na)

(n+m)a =na+ma

Def. 1.19: For a, b $\in$ R.

a-b = a+(-b).

Def. 1.20: By an integral domain is meant a commutative ring with identity which has no zero divisors.

Remark 1.21: The best-known example of an integral domain is the ring of integers. By **Th. 1.16** shows that the cancellation laws for multiplication hold in any integral domain.

Def. 1.22: (Sub ring)

Let (R, +, .) be a ring and S $\subseteq$ R a non empty subset of R. If the system (S, +, .) is itself a ring (using the induced operations), then (S, +, .) is said to be a sub ring of (R, +, .). Or,

Def. 1.23: (Sub ring)

The system (S, +, .) forms a sub ring of the ring (R, +, .) **iff**

(1) S $\neq \phi$, S $\subseteq$ R.

(2) $\forall$ a, b $\in$S imply a-b $\in$S (closure under differences).

(3) $\forall$ a, b $\in$S imply a.b $\in$S (closure under multiplication).

Ex. 1.24: Every ring R has two obvious sub rings, namely the set {0} and R itself.

They are called trivial sub rings of R; all other sub rings (if any exist) are called nontrivial.

Ex. 1.25: The set $\mathbf{Z_e}$ of even integers forms a sub ring of $\mathbf{Z}$ since

$2n-2m = 2(n-m) \in \mathbf{Z_e}$.

$(2n)(2m) = 2(2nm) \in \mathbf{Z_e}$.

Remark 1.26: (Z, +, .) is the ring of integers with identity, but ($\mathbf{Z_e}$,+, .) is a sub ring of **Z** does not contain the identity element.

Q 1.27: (H.W.)

Let (**R**, +, .) be the ring of real numbers,

$\mathbf{R} \times \mathbf{R} = \{(a, b): a, b \in \mathbf{R}\}$ and $S = \mathbf{R} \times \{0\}$.

Define $\oplus$, $\otimes$ on $\mathbf{R} \times \mathbf{R}$,

$(a, b) \oplus (c, d) = (a+c, b+d)$.

$(a, b) \otimes (c, d) = (a.c, b.d)$.

(1) Is $(\mathbf{R} \times \mathbf{R}, \oplus, \otimes)$ a ring ? Explain your answer.

(2) Is $S = \mathbf{R} \times \{0\}$ a sub ring of $\mathbf{R} \times \mathbf{R}$? Explain your answer.

Def. 1.28: (Center of a ring)

The center of a ring R, denoted by Cent R, to be the set

Cent R = $\{a \in R: ar = ra, \text{ for all } r \in R\}$, i.e.,

Cent R consists of those elements which commute with every member of R.

Q 1.29 (H.W.):

A ring R is commutative **iff** Cent R = R.

Th. 1.30 (H.W.):

For any ring R, Cent R is a sub ring of R.

Q **1.30′ (H.W.):** Is Cent R an ideal ? Explain your answer.

Def. 1.31: If R is an arbitrary ring and n a positive integer, then the n^{th} power a^n of an element $a \in R$ is defined by the inductive conditions $a^1 = a$ and $a^n = a^{n-1}.a$.

Q. 1.32 (H.W.): From the usual laws of exponents follow:

$a^n a^m = a^{n+m}$,

$(a^n)^m = a^{nm} \quad (n, m \in Z^+)$.

Hint: To prove these rules, fix m and proceed by induction on n.

Q 1.33 (H.W.): If two elements $a, b \in R$ happen to commute, so do all powers of a and b, whence $(ab)^n = a^n b^n$, for each positive integer n.

Def. 1.34: (Negative powers of a)

Let R be a ring with identity element 1 and a^{-1} exists, negative power of a can be defined as: $a^{-n} = (a^{-1})^n$, where $n > 0$.

Def. 1.35: For each positive integer n, define the n^{th} natural multiple na as follows:

$1a = a$ and

$na = (n-1)a+a$, where $n > 1$.

Remark 1.36: If it is also agreed to let $0a = 0$ and $(-n)a = -(na)$, then the definition of na can be extended to all integers.

Q 1.37 (H.W.): In general multiples satisfy several identities which are easy to establish:

(1) $(n+m)a = na+ma$,

(2) $(nm)a = n(ma)$,

(3) $n(a+b) = na + nb$,

for $a, b \in R$ and arbitrary integers n and m.

Q 1.38 (H.W.): Show that

(1) $n(ab) = (na)b = a(nb)$,

(2) $(na)(mb) = (nm)(ab)$,

for all $a, b \in R$ and arbitrary integers n and m.

Def. 1.39: (characteristic of a ring)

Let R be an arbitrary ring. If there exists a positive integer n such that $na = 0$, for all $a \in R$, then the smallest positive integer with this property is called the characteristic of the ring.

If no such positive integer exists (that is, $n = 0$ is the only integer for which $na = 0$ for all $a \in R$), then R is said to be of characteristic zero.

We shall write char R for the characteristic of R.

Ex. 1.40: **Z**, **Q** and **R** are standard examples of system having characteristic zero.

Ex. 1.41: The ring P(X) of subsets of a fixed set X in **Q. 1.8** is of characteristic 2 since

$2A = A \Delta A = (A-A) \cup (A-A) = \phi$, for every subset $A \subseteq X$.

Th. 1.42: If R is any ring with identity 1, then R has characteristic $n > 0$ **iff** n is the least positive integer for which $n1 = 0$.

Proof: H.W.

Def. 1.43: For an element $a \neq 0$ of the group $(R, +)$ to have order m means that $ma = 0$ and $ka \neq 0$ if $0 < k < m$.

Q 1.43′ (H.W.): Give an example of **Def. 1.43**.

Corollary 1.44:

(1) In an integral domain R all the non zero elements have the same additive order; this order is the characteristic of the domain when char R $>$ 0 and (2) infinite when char R = 0.

Proof: (H.W.).

Remark 1.45: When char R = 0. The equation ma = 0 would lead, as before to m1 = 0 or m = 0.

In this case every no zero element $a \in R$ must be of infinite order.

Corollary 1.46: An integral domain R has positive characteristic **iff** na = 0, for some $0 \neq a \in R$ and some integer $n \in \mathbf{Z}^+$.

Proof: (H.W.).

Th. 1.47: The characteristic of an integral domain is either zero or a prime number.

Proof: Let R be positive characteristic n and assume that n is not a prime.

Then, n has a nontrivial factorization $n = n_1n_2$, with $1 < n_1, n_2 < n$.

It follows that,

$0 = n1 = (n_1n_2)1 = (n_1n_2)1^2 = (n_11).(n_21)$.

By supposition, R is without zero divisors, so that either $n_11 = 0$ or $n_21 = 0$.

Since both n_1 and n_2 are less than n, this contradicts the choice of n as the least positive integer for which n1 = 0.

Whence char R must be prime.

Corollary 1.48: If R is a finite integral domain, then char R = p, where p is a prime.

Proof: (H.W.).

Remark 1.49: Let R be any ring with identity and consider the set **Z**1 of integral multiples of the identity; stated symbolically

Z1 = {n1: n $\in$ **Z**}.

From the relations

n1-m1 = (n-m)1,

(n1)(m1) = (nm)1

Q.1.50 (H.W.): Show that **Z**1 form a commutative ring with identity.

Q.1.51 (H.W.): The order of the additive cyclic group (**Z**1, +) is the characteristic of the given ring R.

Q.1.52 (H.W.): If R is an integral domain, then **Z**1 is a subdomain of R (that is, **Z**1 is also an integral domain with respect to the operations in R).

In fact, show that **Z**1 is the smallest subdomain of R, in the sense that it is contained in every other subdomain of R.

Q1.53 (H.W.): If R is a domain of characteristic p, where p is a prime, then show that each non zero element of **Z**1 is invertible.