The Characteristics of Integral Domains

Aye Aye Khaing

Lecturer, Department of Mathematics, Meiktila University

Abstract

In this paper some special class of ring are introduced. Especially, integral domain and field are mentioned. And then, the characteristics of integral domain and field are discussed. Finally, we express a finite integral domain has finite characteristics and an infinite integral domain may have finite or zero characteristic.

Key words: ring, integral domain, field, characteristic.

Introduction

In modern algebra, a ring is a system with a nonempty set and two binary compositions also the set of integers under usual addition and multiplication being an example. It does have certain specific properties satisfied with respect to multiplication as well. An integral domain is a commutative ring with unit and a finite integral domain is a field. An integral domain is said to be of characteristic zero and finite characteristic.

Some Definitions of Ring

Definition (1)

A nonempty set *R* is said to be a *ring* if in *R* there are two operations $+$ and $\cdot$ such that:

(i) $a, b \in R$ implies that $a+b \in R$.

(ii) $a+b=b+a$ for $a, b \in R$.

(iii) $(a+b)+c=a+(b+c)$ for $a, b, c \in R$.

(iv) There exists an element $0 \in R$ such that $a+0=a$ for every $a \in R$.

(v) Given $a \in R$, there exists an element $b \in R$ such that $a+b=0$.
(We shall write b as $-a$).

(vi) $a, b \in R$ implies that $a.b \in R$.

(vii) $a \cdot (b \cdot c)=(a \cdot b) \cdot c$ for $a, b, c \in R$.

(viii) $a \cdot (b+c)=a \cdot b+a \cdot c$ and $(b+c) \cdot a=b \cdot a+c \cdot a$, for $a, b, c \in R$.

Lecturer, Department of Mathematics, University of Meiktila

Axioms (i) through (v) merely state that *R* is an *abelian group* under the operation $+,$ which we call addition.

Definition (2)

A ring *R* is called a *commutative ring* if $a \cdot b = b \cdot a$ for all $a, b \in R.$

Definition (3)

If there exists an element 1 in ring *R* such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R,$ then *R* is a *ring with unit element*.

Definition (4)

If R is a commutative ring, then $a \neq 0 \in R$ is said to be a *zero divisor* if there exists $b \in R, b \neq 0$ such that $ab = 0.$

Definition (5)

A ring R with unit is said to be a *division ring* if for every $a \neq 0$ in R there is an element $b \in R$ (usually written as a^{-1}) such that $a \bullet a^{-1} = a^{-1} \bullet a = 1.$

Definition (6)

If *R* is a ring, then a subring of *R* is a subset *S* of *R* which is a ring if the operations ab and $a + b$ are just the operations of *R* applied to the elements $a, b \in S.$

For *S* to be a subring, it is necessary and sufficient that *S* be nonempty and that $a \pm b \in S$ for all $a, b \in S.$

If R is a ring, then $\{0\}$ and R are always subrings of R, called *trivial subrings* of R. Any other subring is called a *non-trivial subring*.

Integral Domains and Fields

Definition (7)

Let R be a commutative ring with unit. R is called an *integral domain* if it has the property that whenever $ab = 0$ for some elements $a, b \in R,$ either $a = 0$ or $b = 0,$ or, if it has no zero-divisors.

Definition (8)

A commutative ring R is called a *field* if every nonzero element in R is a unit of R. A field is a commutative division ring.

Example (1)

The ring of integers is an integral domain as the product of two integers is zero if and only if one or both of the factors is zero. But it is not a field since the only integers that are units are ± 1.

Example (2)

The ring of rational numbers is both an integral domain and a field since every nonzero rational number is a unit.

Example (3)

The ring Z_6 of integers modulo 6 is a commutative ring with identity but is neither an integral domain nor a field: it is not an integral domain since $[2][3]=[0]$, but $[3]\neq[0]$ and $[2]\neq[0]$; and it is not a field since $[2]$ is not a unit of Z_6.

Remark (1)

Every subring of an integral domain is an integral domain. A subring of a field that is itself a field is called a subfield of the field.

Proposition (1)

Every field is an integral domain.

Proof:

Let F be a field.

Let a and b be elements in F such that $ab=0$.

Suppose that $a\neq 0$. Then a is a unit of F.

Therefore $b=1b=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$.

Thus, either a or b is zero.

Therefore F is an integral domain.

Proposition (2)

Every finite integral domain is a field.

Proof:

Let $R = \{r_1, ..., r_n\}$ be a finite integral domain.

Let $r \neq 0$ be a typical nonzero element in R.

Consider the set $rR = \{rr_1, ..., rr_n\}$ consisting of all multiples of r by elements in R.

Clearly, $rR \subseteq R$.

On the other hand, if $rr_i = rr_j$ for some $i \neq j$, then $r(r_i - r_j) = 0$, which is a contradiction since R is an integral domain and $r \neq 0$ and $r_i - r_j \neq 0$.

Thus the products $rr_1, ..., rr_n$ are n distinct elements of R and therefore $rR = R$.

Since $1 \in R$, it now follows that $1 = rb$ for some element $b \in R$ and hence r is a unit of R, as required.

Thus, R is a field.

Lemma (1)

If D is an integral domain and d is a nonzero element of D, then for any integer n, $n1 = 0$ if and only if $nd = 0$.

Proof:

By the distributive laws of a ring R, we have $m(ab) = (ma)b = a(mb)$ for any integer m and for all $a, b \in R$.

If the ring R has 1, $1a = a$ for all $a \in R$.

We write $1+1+...+1$ as $n1$.

Thus $nd = n(1d) = (1d + 1d + ... + 1d)$

$= (n1)d.$

Therefore $n1 = 0$ implies $nd = 0$.

Conversely, suppose that D is an integral domain and $d \neq 0$ in D.

Then $nd = 0$ implies $(n1)d = 0$ and $n1 = 0$.

Lemma (2)

A finite nonzero commutative ring without zero divisors is a field.

Proof :

See [2].

Corollary (1)

If p is a prime number, then Z_p is a field.

Proof :

See [2].

Some Characteristics of Integral Domains and Fields

Definition (9)

An integral domain D is said to be of *characteristic zero* if the relation $ma = 0$, where $a \neq 0$ is in D, and where m is an integer, can hold only if $m = 0$.

Definition (10)

An integral domain D is said to be of *finite characteristic* if there exists a positive integral m such that $ma = 0$ for all $a \in D$. In this case, we define the characteristic of D to be the smallest positive integer p such that $pa = 0$ for all $a \in D$.

A field of characteristic zero is necessarily infinite, but a field with finite characteristic may be finite or infinite.

Example (4)

The ring of integers Z is an integral domain where 1 is the ordinary integer 1. Since $+$ is the ordinary addition, $n1 = 1+1+...+1 = 0$ implies $n = 0.$

Thus, $a \neq 0$ is in Z and $ma = 0$ implies $m1 = 0$ and $m = 0.$

Hence the ring Z has characteristic zero. Other familiar rings of characteristic zero are $2Z,\ R,\ Q,\ C.$

Example (5)

The ring Z_p is a field if p is prime.

So Z_p is an integral domain.

Let $a \in Z_p$ and $a \neq 0.$ Z_p contains p elements.

We have $a + a + ... + a =$ identity of the additive group.

That is, $pa = 0$ for all $a \in Z_p.$

If $0 < r < p,$ then $ra = 0$ for all $a \in Z_p$ implies $r1 = 0.$

Then $r = 0,$ giving a contradiction.

Thus p is the smallest such integer.

Hence Z_p has characteristic p.

Example (6)

A field which has only a finiter number of elements is called a finite field or a Galois field. The above example (5) provides a finite field of characteristic p.

Z_2 is the Galois field with characteristic 2.

Let $D = \{0, 1, a, b\}$ with $+$ and $\bullet$ defined by the following tables:

$+$	0	1	a	b
0	0	1	a	b

$\bullet$	0	1	a	b
0	0	0	0	0

1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

This is a field with four elements and with characteristic 2.

Although the characteristic of a finite field is always finite, the number of elements in the field may not be the same as its characteristic.

Theorem (1)

If D is an integral domain, then characteristic of D is either zero or a prime number.

Proof:

If characteristic of D is zero, we have nothing to prove. Suppose D has finite characteristic then there exist a positive integer integral m such that $ma = 0$ for all $a \in D$.

Let k be such least positive integer then characteristic of D is equal to k, we will show that k is a prime.

Suppose k is not a prime, then we can write $k = rs,\ 1 < r,\ s < k$.

Now $ka = 0$ for all $a \in D$ implies $(rs)a^2 = 0$ for all $a \in D$

$$a^2 + a^2 + ... + a^2 = 0 \text{ (rs times)}$$

$$(a + a + ... + a)(a + a + ... + a) = 0 \text{ for all } a \in D$$

$$(ra)(sa) = 0 \text{ for all } a \in D$$

$$ra = 0 \text{ or } sa = 0 \text{ for all } a \in D,$$

since D is an integral domain.

In either case it will be a contradiction as $r,\ s < k$, but k is the least positive integer such that $ka = 0$.

Hence k is a prime.

Example (7)

If D is an integral domain and if $na = 0$ for some $0 \neq a \in D$ and some integer $n = 0,$ then we will show that the characteristic of D is finite.

Since $na = 0$

$(na)x = 0$ for all $x \in D$

$(a + a + ... + a)x = 0$

$ax + ax + ... + ax = 0$

$a(x + x + ... + x) = 0$ for all $x \in D$

$x + x + ... + x = 0$ for all $x \in D$ as $a \neq 0$

$nx = 0$ for all $x \in D,\ n \neq 0.$

Therefore characteristic of D is finite.

Example (8)

If D is an integral domain and D is of finite characteristic, then we will prove that the characteristic of D is a prime number.

Consider the multiplicative identity 1 of D.

Let the finite characteristic of D be n. Then n is the smallest positive integer such that $n \cdot 1 = 0.$

Since $1 \cdot 1 \neq 0,\ n > 1.$

If possible, let $n = r \cdot s,$ where $1 < r < n$ and $1 < s < n.$

So $(rs)1 = 0.$

But $(1 + ... + 1) + ... + (1 + ... + 1) = 0,$ by distributive law.

Thus $(r1)(s1) = 0.$

Since there exists no zero divisor, this implies $r1 = 1$ or $r1 = 0.$

Contradiction to the choice of n.

Hence n must be a prime number.

Conclusion

This research paper is limited to integral domain and field. Some theorems on the characteristic of integral domain and field are presented and considered with examples. We continue to study the ring of polynomials over a ring R, R[x], is also infinite integral domain. Although R[x] is infinite, it is of finite characteristic. To sum up, the characteristics of integral domain can be applied for the characteristics of R[x].

Acknowledgements

We would like to be deeply indebted to Rector Dr Ba Han, Meiktila University, for his kindly accepted this research and Pro Rector Dr Tin Tun Aung, Meiktila University, for his continuous encouragement. We also thank to Dr Aung Kyaw Min, Head and Professor and Dr Khin Myat Myat Aung, Professor, Department of Mathematics, Meiktila University for their invaluable suggestions.

References

Herstein, I. N., (1975), *Topics in Algebra*, 2nd Edition, United State of America, John Wiley & Sons, Inc., New York.

Herstein, I. N., (1986), *Abstract Algebra*, 2nd Edition, Macmillan Publishing Company, a division of Macmillan, Inc., New York.

K . Dennis (1991), "*Abstract Algebra*", United State of America, Harcourt Brace Jovanovich, Inc., New York.

Vijay, K. K. & S. K. Bhambri., (1993), *A Course In Abstract Algebra*, 2nd revised Edition, UBS Publisher's Distributors Ltd., New Delhi.