Lecture 3: Characteristic of a Ring

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Characteristic of a Ring

Definition

Let R be a ring. If there exists a positive integer n such that $na = 0_R$ for all $a \in R$, then the smallest such positive integer is called the **characteristic of** R, and denoted by **Char**(R) . If no such positive integer exists, then R is said to be **characteristic zero**.

Examples:

1. $\text{Char}(\mathbb{Z}) = 0, \text{Char}(\mathbb{Q}) = 0, \text{Char}(\mathbb{R}) = 0, \text{Char}(\mathbb{C}) = 0$

2. $\text{Char}(\mathbb{Z}_n) = n$, since $\forall \overline{x} \in \mathbb{Z}_n$, $n\overline{x} = \overline{0}$.

3. If R is a Boolean ring, then $\text{Char}(R) = 2$. Since $\forall x \in R, x + x = 2x = 0_R$.

Characteristic of a Ring

The following theorem is useful to find the characteristic of a ring when that ring has unity.

Theorem

Let R be a ring with unity.
(i) If $n1_R \neq 0_R$ for all $n \in \mathbb{Z}^+$, then R has characteristic zero.
(ii) If $n1_R = 0_R$ for some $n \in \mathbb{Z}^+$, then the smallest such integer n is the characteristic of R.

That is;
(i) if 1_R has infinite order under addition, then $\text{Char}(R) = 0$
(ii) if 1_R has order n under addition, then $\text{Char}(R) = n$.

Example:

1. $\text{Char}(\mathbb{Z}) = 0$, since we could not find $n \in \mathbb{Z}^+$ such that $n1 = 0$.
2. $\text{Char}(\mathbb{Z}_m \times \mathbb{Z}_n) = \operatorname{lcm}(m, n)$. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ is a ring with unity $(\overline{1}, \overline{1})$, it is enough to check the order of the unity to find the characteristic of $\mathbb{Z}_m \times \mathbb{Z}_n$.
3. $\text{Char}(\mathbb{Z} \times \mathbb{Z}_2) = 0$.

Characteristic of a Ring

Example: Let X be a set and $P(X)$ be its power set. $P(X)$ is a ring with the following operations $+$ and $.$ defined by:

$$\begin{aligned} A + B &:= (A \cup B) \setminus (A \cap B) \\ A.B &:= A \cap B \end{aligned}$$

for $A, B \in P(X)$.

- $(P(X), +, .)$ is a commutative ring with unity.
- The zero element of $P(X)$ is $\emptyset$.
- The unity of $P(X)$ is X.
- $(P(X), +, .)$ is a Boolean ring, since every element of $P(X)$ is idempotent. Hence, $\text{Char}(P(X)) = 2$.

Theorem

The characteristic of an integral domain D is either zero or a prime.

Corollary

The characteristic of a field F is either zero or a prime.

Theorem

The characteristic of a finite ring R divides $|R|$.

Example: Let F be a field of order 2^n. From the result of the Lagrange Theorem, $\text{Char}(F) = 2$.

Characteristic of a Ring

Remark: If $\text{Char}(R) = 0$, then the ring has infinitely many elements. But the converse is not true.

Example: Consider the ring $P(\mathbb{Z})$ which has infinitely many elements, but the $\text{Char}(P(\mathbb{Z})) = 2$.

For the compatibility of this chapter, now we give an important result related to the rings with unity. For details see:
Chapter 5: Ring Homomorphisms and Isomorphisms
Chapter 6: Field of Quotients of an Integral Domain.

Theorem

Let R be a ring with unity.
If $Char(R) = n$, then R contains a subring isomorphic to $\mathbb{Z}_n$.
If $Char(R) = 0$, then R contains a subring isomorphic to $\mathbb{Z}$.

From this theorem, we can consider that the rings $\mathbb{Z}_n$ and $\mathbb{Z}$ are the fundamental building blocks for all rings with unity.

Characteristic of a Ring

Corollary

Let D be an integral domain.
If $Char(D) = p$, then D contains a subring isomorphic to $\mathbb{Z}_p$.
If $Char(D) = 0$, then D contains a subring isomorphic to $\mathbb{Z}$.

Theorem

Every field F contains a subfield isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Q}$.

Thus, the fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are the fundamental building blocks for all fields. (These fields are prime fields).

Remark:

- The smallest subfield of a field F is called the **prime subfield.** In other words; the prime subfield of F is the smallest subfield containing 1_F.
- If F_q is a finite field of characteristic p, then $|F_q| = p^n$ for some positive integer n. Also every subfield of F_q has order p^k, where k is a positive divisor of n. Conversely, if k is a positive divisor of n, then there is exactly one subfield of F_q with p^k elements.
- Let K be a subfield of F. Then Char(K)=Char(F).