1 Characteristic of a Ring

Consider the ring $\mathbb{Z}_3[i]$, with the elements:

$$\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$$

For any element x in this ring, we have:

$$3x = x + x + x = 0$$

For example:

- $2i + 2i + 2i = 6i = 0i = 0$
- $(1+2i) + (1+2i) + (1+2i) = 3 + 6i = 0$
- And so on.

Similarly, in the ring $\{0, 3, 6, 9\} \subset \mathbb{Z}_{12}$, we have, for all x:

$$4x = x + x + x + x = 0$$

1.1 Characteristic of a Ring

Definition 1.1: Characteristic of a Ring

The **characteristic** of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\text{char } R$.

So, for example, the ring of integers $\mathbb{Z}$ has characteristic 0 and $\mathbb{Z}_n$ has characteristic n. For example, consider $\mathbb{Z}_3 = \{0, 1, 2\}$. Then, we know that:

$$3x = x + x + x = 0 \qquad \forall x$$

So the characteristic of $\mathbb{Z}_3$ is $\boxed{3}$. Now, consider $\mathbb{Z}_6$. We know that:

$$6x = x + x + x + x + x + x = 0 \qquad \forall x$$

So, its characteristic is $\boxed{6}$. As a final example, $\{0\}$ has characteristic $\boxed{1}$.

1.2 Characteristic of a Ring with Unity

Occasionally, we might have more complicated rings where the above theorem may be hard to apply.

Theorem 1.1: Characteristic of a Ring with Unity

Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Remark: Here, suppose $(\mathbb{R}, +)$ is a group. Then, we say that $x \in \mathbb{R}$ has an additive order n if $nx = 0$ and n is the smallest positive number with this property.

Proof. Suppose 1 has infinite order. Then, there is no positive integer n such that $n \cdot 1 = 0$, so R must have characteristic 0. Now, let's suppose that 1 does have additive order n. Then, we know that

$n \cdot 1 = 0$ and n is the least positive integer with this property. So, for any $x \in R$, we have:

$$\begin{aligned} n \cdot x &= \overbrace{x + x + \cdots + x}^{n \text{ times}} \\ &= \overbrace{1x + 1x + \cdots + 1x}^{n \text{ times}} \\ &= (\overbrace{1 + 1 + \cdots + 1}^{n \text{ times}})x \\ &= (n \cdot 1)x = 0x = 0 \end{aligned}$$

So, R has characteristic n. □

For example, take $R = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

1. Does this ring have unity? Each member of this direct product ring has 1, so the unity would be $(1, 1, 1) \in R$.
2. What is the characteristic of R? The characteristic order of R is the additive order of $(1, 1, 1) \in R$. Well, we have that:

$$n(1, 1, 1) = (n1, n1, n1)$$

Consider the first element in the pair. When is $n1 \equiv 0 \pmod 6$? This is when $6|n$, or:

$$n \in \{6, 12, 18, 24, \dots\}$$

For the third element in the pair, we need to know when $n1 \equiv 0 \pmod{10}$. This is when $10|n$, or:

$$n \in \{10, 20, 30, \dots\}$$

Here, it's clear that the answer is $\operatorname{lcm}(6, 4, 10) = 60$.

Theorem 1.2: Characteristic of an Integral Domain

The characteristic of an integral domain is 0 or prime.

Proof. It suffices to consider the additive order of 1. Suppose towards a contradiction that 1 has composite order n and $1 < s$ and $t < n$ such that $n = st$. Then, we know that:

$$0 = n1 = (st)1 = s(t1) = (s1)(t1)$$

But, $1 < s$ and $t < n$, so by minimality of n being the order of 1, it must be that $s1, t1 \neq 0$ and are thus zero-divisors. But, this is a contradiction. □

1.2.1 Problem 1: Field

Suppose F is a field of order 3^n. Show that $\operatorname{char} F = 3$.

Proof. We know that $\operatorname{char} F$ has order 1. Well, the order of 1 divides the order of F. The order of F is 3^n, so the order of 1 is potentially $1, 3^1, 3^2, \dots, 3^n$. But, the characteristic of an integral domain is prime, so the answer must be 3. □

1.2.2 Problem 2: Field

Find the characteristic of $\mathbb{Z}/4\mathbb{Z} \oplus 4\mathbb{Z}$.

Proof. We know that $\operatorname{char} 4\mathbb{Z} = 0$, so $\operatorname{char} \mathbb{Z}/4\mathbb{Z} \oplus 4\mathbb{Z} = 0$. If we pick $(1, 4) \in \mathbb{Z}/4\mathbb{Z} \oplus 4\mathbb{Z}$, then for any positive integer n:

$$n(1, 4) = (n, 4n) \neq (0, 0)$$

So, we can't find one. $\square$

1.3 Summary of Rings

Ring	**Characteristic**	**Integral Domain?**
$\mathbb{Z}$	0	Yes
$M_2(\mathbb{Z})$	0	No
$\mathbb{Z} \oplus \mathbb{Z}$	0	No
$\mathbb{F}_p$ $(\mathbb{Z}/p\mathbb{Z})$	p	Yes
$\mathbb{F}_p \oplus \mathbb{F}_p$	p	No
$\mathbb{F}_p[x]$	p	Yes
$\mathbb{Z}/n\mathbb{Z}[i]$	n	$\begin{cases} \text{No} & n \text{ not prime.} \\ \text{Maybe} & n \text{ prime.} \end{cases}$