Elementary Number Theory

Thaqib Mo.

November 14, 2020

1 Integral Domains

Definition 1: Integral Domains

Let R be a commutative ring, then $a \in R$ is called the *zero divisor*, if there is some $b \in R$ with $b \neq 0$ for which $ab = 0$.

An *Integral Domain* is a commutative ring R, with $R \neq \{0\}$ such that 0 is the only *zero divisor*. If we have $ab = 0$ then either $a = 0$ or $b = 0$.

We can define Integral Domains in another equivalent way using the "cancellation law".

Theorem 1

A commutative ring $R \neq \{0\}$ is an integral domain if and only if for all $a, b, c \in R$ if $a \neq 0$ and

$$ab = ac$$

Then

$$b = c$$

Proof. Suppose R is an integral domain, and we have $ab = ac$ and $a \neq 0$ then $ab - ac = 0$ and then $a(b - c) = 0$. Since R is an integral domain we must have $b - c = 0$ that implies $b = c$.

Now suppose R is a ring where the commutative property holds. Assume we have $ab = 0$ If $a = 0$ we are done, suppose $a \neq 0$ then

$$ab = a \cdot 0 \rightsquigarrow b = 0$$

□

Example 1. The ring $\mathbb{Z}$ is an integral domain.

Example 2. The commutative rings $\mathbb{Q}, \mathbb{R}$ are an integral domains.

The rings $\mathbb{Q}$ and $\mathbb{R}$ are more than rings. They are also *fields*.

Definition 2: Fields

A ring F is called a *field* if it is commutative, and if every non zero element in F has a multiplicative inverse. That means if $a \in F$ with $a \neq 0$ then we have $b \in F$ such that

$$ab = 1$$

For the fields $\mathbb{Q}, \mathbb{R}$ if we have $r \in \mathbb{Q}$ then we also have $\frac{1}{r} \in \mathbb{Q}$ and $r \cdot \frac{1}{r} = 1$. The same applies for the field $\mathbb{R}$. The ring $\mathbb{Z}$ is not a field since not every element has a multiplicative inverse.

Theorem 2

Every subring of a field is an integral domain. In particular, every field is an integral domain.

Proof. Let F be a field and R be a sub ring. Since $\times$ in R and $\times$ in F is the same, $(R, \times)$ is commutative and R is a commutative ring. Now suppose we have $a, b \in R$ such that $ab = 0$. If $a = 0$ we are done. Assume $a \neq 0$ since this equation also holds in F then there is some $a^{-1} \in F$ such that $aa^{-1} = 1$ then we get

$$ab = 0$$

$$aba^{-1} = 0a^{-1}$$

$$b = 0$$

□

Example 3. If $n \geq 2$ is composite then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain. Since there is a factorization of $n = ab$ then $[a], [b]$ are both non zero elements with $[a][b] = [ab] = [n] = [0]$

Example 4. We define the ring of *Gaussian integers* denoted by $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ where addition is given by

$$a + bi + c + di = (a + b) + (c + d)i$$

and multiplication is given by

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

This is a subring is $\mathbb{C}$ the complex numbers.

1.1 Basic Properties of Integral Domains

Theorem 3

If R is an integral domain then $\mathrm{Char} R = 0$ or $\mathrm{Char} R$ is prime.

Proof. Suppose R is an integral domain and $\mathrm{Char} R \neq 0$ and $\mathrm{Char} R$ is not prime. Then if we have $\mathrm{Char} R = 1$, then R is the zero ring since $1 = 0$, which is not possible due to the definition of integral domain. Now suppose $\mathrm{Char} R = n$ where $n > 1$ is not prime. Then we have $n = ab$ then $a \cdot 1_R$ and $b \cdot 1_R$ are non zero elements but $(a \cdot 1)(b \cdot 1) = ab \cdot 1 = 0$ that contradicts the definition of an integral domain. □

Note that this again shows that $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain

Theorem 4

Every finite integral domain is a field.

Proof. Let R be an integral domain, and suppose $|R| = n$. Let $a \in R$ with $a \neq 0$ consider the multiplication map $\phi_a(r) = ar$ then ϕ is injective since if we have $\phi(r) = \phi(s)$ then $ra = sa$ since R is an integral domain we can use the cancellation property to get $r = s$.

So we have an injective function $\phi : R \to R$. Since R is finite then this implies ϕ is surjective. Given that ϕ is injective we have $|\phi(R)| = n$. Since ϕ is surjective there must be some $b \in R$ such that $\phi(b) = 1$ which means $ab = ba = 1$ thus a has an multiplicative inverse in R. By definition R is a field. $\square$