MA542 Lecture

Timothy Kohl

Boston University

January 29, 2025

Integral Domains

Beyond the distinction between commutative and non-commutative rings, we can subdivide the category of rings into other 'subcategories' or classes, based on particular global characteristics.

Note, there is a notion in mathematics of 'category' which has a formal defintion, but here we will use the term somewhat loosely to distinguish between different types of rings due to properties they share.

We begin with a subcategory of the category of commutative rings, known as integral domains, whose definition has a direct connection with the idea of 'cancellation' we discussed earlier, namely when does $ab = ac$ imply $b = c$?

Consider the following:

In $M_2(\mathbb{R})$ the zero element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and one can show that

$$\begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

i.e. the product of two non-zero elements (matrices) is the zero

A more simple example is in the ring $\mathbb{Z}_6$ where we have $2 \cdot 3 = 0$ since $2 \cdot 3 = 6 \equiv 0 \ (mod\ 6)$ but where $2 \neq 0$ and $3 \neq 0$ of course.

In $\mathbb{Z}$ this can't happen, namely $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$, or, equivalently, $ab = 0$ implies $a = 0$ and/or $b = 0$.

Definition

A non-zero element 'a' of a ring R is a zero divisor if for some other non-zero element $b \in R$ one has $ab = 0$.

Definition

An integral domain (or simply domain) is a commutative ring, with unity, without zero divisors.

There are many examples!

- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}[i]$ (exercise)
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

It is a nice exercise to prove that not only is $\mathbb{Z}[\sqrt{2}]$ a (commutative) ring but that it is a domain.

Note, the quaternions $\mathbb{H}$ have no zero-divisors, but as it's not commutative, we don't call it a domain.

We've seen that $\mathbb{Z}$ is a domain, but that, for example, $\mathbb{Z}_6$ is not.

However, there are some $\mathbb{Z}_n$ which are domains.

We first pause to observe that $1 \in R$ is **never** a zero-divisor.

$\mathbb{Z}_2 = \{0, 1\}$ is domain since $1 \cdot 1 = 1$.(Not terribly exciting of course.)

Also $\mathbb{Z}_3 = \{0, 1, 2\}$ is too since $2 \cdot 2 = 1$.

However in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ we have $2 \cdot 2 = 0$.

So what's the pattern?

Theorem

$\mathbb{Z}_n$ is a domain if and only if n is a prime.

Proof.

If n is not a prime, then $n = r \cdot s$ for two numbers $r, s < n$ so r, s may be regarded as elements of $\mathbb{Z}_n$ and $rs = 0$.
If $n = p$ is prime and if $a, b \in \mathbb{Z}_p$ are non-zero elements, then $a < p$ and $b < p$.
So if $ab = 0$ then p divides ab but that means either p divides a or p divides b, which is impossible. □

Proposition

A field is an integral domain.

Proof.

Recall that a fields is a commutative ring with unity where every non-zero element has a multiplicative inverse.
So suppose $a, b \in F$ are elements of a field F such that $ab = 0$.
If $a \neq 0$ then $a^{-1} \in F$ and so

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

$$\downarrow$$

$$1b = 0$$

$$\downarrow$$

$$b = 0$$

which means that F has no-zero divisors. □

We will explore fields in much more detail later on, but we can pause to give a few other examples of fields besides the 'canoncial' examples $\mathbb{Q}$,$\mathbb{R}$, and $\mathbb{C}$.

There are many interesting examples 'in between' $\mathbb{Q}$ and $\mathbb{C}$.

Define

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

with addition and multiplication defined as in $\mathbb{C}$.

Indeed $\mathbb{Q}(i)$ is a subring of $\mathbb{C}$.

The question is whether this is a field, but this isn't too difficult.

Let $a+bi$ be a non-zero element which means at least one of a or b are non-zero.

$$\begin{aligned}\frac{1}{a+bi} = \frac{1}{a+bi}\frac{a-bi}{a-bi} &= \frac{a-bi}{a^2+b^2} \\ &= \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\end{aligned}$$

In $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$ since a, b are not both zero then $a^2+b^2>0$ so the above element is still in $\mathbb{Q}(i)$, i.e. $\frac{1}{a+bi} \in \mathbb{Q}(i)$.

More Field Examples

Recall $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ which we saw is a field.

Here is a similar example:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

where again, a non-zero element is one of the form $a + b\sqrt{2}$ where a and b are not both zero.

We again look to see whether the reciprocal is also a member of $\mathbb{Q}(\sqrt{2})$.

The argument is similar to the one used above using the 'conjugate radical':

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}} &= \frac{a-b\sqrt{2}}{a^2-2b^2}\\ &= \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}\end{aligned}$$

and we finish by realizing that $\frac{a}{a^2-2b^2},\frac{b}{a^2-2b^2}$ are in $\mathbb{Q}$ in particular that $a^2-2b^2 \neq 0$. Why?

For $a, b \in \mathbb{Q}$ suppose that $a^2 - 2b^2 = 0$ which means $a^2 = 2b^2$

If $a = 0$ then $a^2 = 2b^2$ implies $b = 0$ which is impossible.

If $b = 0$ then $a^2 = 2b^2$ implies $a = 0$ which is also impossible.

If $a \neq 0$ and $b \neq 0$ then $a^2 = 2b^2$ implies $\frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = 2$ but $\frac{a}{b} \in \mathbb{Q}$ which is impossible since $\sqrt{2} \notin \mathbb{Q}$.

Note: If $\sqrt{2} = \frac{a}{b}$ where $gcd(a, b) = 1$ then $2b^2 = a^2$ which means $a = 2c$ so $2b^2 = 4c^2$, so $b^2 = 2c^2$ so $b = 2d$, this means $gcd(a, b) > 1$.
This was the argument used by Euclid to prove $\sqrt{2}$ is irrational.

Now, we already know that for each prime p that $\mathbb{Z}_p$ is a commutative ring with unity, and that since $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\}$ it is a field.

However, there is another nice way to demonstrate this is the case, and also helps us demonstrate that other such finite rings are fields. This is a consequence of the following neat theorem.

Theorem (Wedderburn)

A finite integral domain is a field.

Proof.

Let $D = \{0, d_1, d_2, \ldots, d_n\}$ be a finite domain, and assume that $d_1 = 1$ (the unity element).
Pick any non-zero $d_i \in D$ consider $d_i d_1, d_i d_2, \ldots, d_i d_n$ and suppose $d_i d_j = d_i d_k$ then $d_i(d_j - d_k) = 0$.
But since D is a domain and $d_i \neq 0$ then $(d_j - d_k) = 0$ which means $d_j = d_k$.
Moreover, no $d_i d_j = 0$ (again since D is a domain) and so $d_i d_1, d_i d_2, \ldots, d_i d_n$ is a rearrangement of $d_1, d_2, \ldots, d_n$ which means one of the $d_i d_j = 1$ ergo $d_i^{-1} = d_j$.
As such D must be a field. □

And since we've shown that $\mathbb{Z}_n$ is a domain when n is a prime, we have:

Corollary

For any prime p, $\mathbb{Z}_p$ is a field.