# Class 18

April 3, 2024

## Integral Domains

In a commutative ring $R$ we call a non-zero element $a \in R$ a zero-divisor if $\exists b \in R$ such that $b \neq 0$ and $ab = 0$.

### Ex

Consider the ring of $2 \times 2$ real matrices $M_2(\mathbb{R})$. Then $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor as $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is not a zero divisor as for any matrix $A \in M_2(\mathbb{R})$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} A = 0$$

$$A = 0$$

so there cannot exist a nonzero $A$ such that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} A = 0$.

### Def

An integral domain (ID) is a commutative ring with unity and no zero-divisors.

### Ex 1

$\mathbb{Z}$ is an integral domain under the usual definition of multiplication and addition. We know the integers are commutative and that 1 is an integer. If we consider two integers, $a, b$ such that

$$ab = 0$$

we know

$$a = 0 \text{ or } b = 0$$

by the properties of the integers.

### Ex 2

Consider the Gaussian integers $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. First, let's show $R$ is a ring under the usual definition of multiplication and addition. We have previously shown the complex numbers form a group under addition, so we will use the first subgroup test to show $R$ is a subgroup of $\mathbb{C}$ under addition. Let $a + bi, c + di \in R$. Then

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

As $(a - c), (b - d) \in \mathbb{Z}$, then $(a + bi) - (c + di) \in R$. As the Gaussian integers are a subset of the complex numbers, we know they will obey associativity and the distributive laws. We need to show they remain closed under multiplication. Let $a + bi, c + di \in R$. Then using foil:

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

as $(ac-bd),(bc+ad) \in \mathbb{Z}$, then $(a+bi)(c+di) \in R$, thus $R$ is a ring. Now, we will show $R$ is a commutative ring with unity. As the Gaussian integers are a subset of $\mathbb{C}$ and the complex numbers are commutative, then $R$ is commutative. Finally, consider $1+0i \in R$. For any $a+bi \in R$,

$$(1+0i)(a+bi) = 1(a+bi) = a+bi$$

thus 1 is a unity in $R$, so $R$ is a ring with unity. Now, we show that $R$ is an integral domain. Let $a+bi, c+di \in R$ both be non-zero such that

$$(a+bi)(c+di) = 0$$

Then

$$(ac-bd) + (bc+ad)\,i = 0+0i$$

We can match the real and imaginary parts to yield

$$(ac-bd) = 0$$

$$(bc+ad) = 0$$

Suppose WLOG $a \neq 0$. As the integers are a subset of the real numbers, then we can rearrange the first equation to yield (even though $\frac{1}{a}$ is not an integer)

$$ac = bd$$

$$c = \frac{bd}{a}$$

Substitute back into the second equation to yield

$$b\left(\frac{bd}{a}\right) + ad = 0$$

$$\frac{b^2 d}{a} + ad = 0$$

multiply both sides by $a$ to yield

$$b^2 d + a^2 d = 0$$

Factor out a $d$ to yield

$$\left(b^2+a^2\right) d = 0$$

As $a \neq 0$, then $\left(b^2+a^2\right) > 0$ thus $d = 0$. If $d = 0$, then we can plug into the equation for $c$

$$c = \frac{bd}{a} = 0$$

thus $c, d = 0$ and $c+di = 0$ a contradiction! Thus $R$ cannot contain any zero divisors and as such $R$ is an integral domain.

## Ex 3

Consider $\mathbb{Z}_p$ such that $p$ is prime. I claim $\mathbb{Z}_p$ is a commutative ring with unity (it would be good practice to prove this). Let's show $\mathbb{Z}_p$ contains no zero divisors. Let $a, b \in \mathbb{Z}_p$ such that $1 \leq a, b < p$. Then

$$ab \neq_p 0$$

To show this, first suppose WLOG $a = 1$. Then $ab =_p b \neq_p 0$ as $1 \leq b < p$. Now suppose $a, b \neq 1$. Then $a, b$ cannot be factors of $p$ as $p$ is prime and can only have factors of 1 or $p$. As such, the product $a, b$ cannot be divisible by $p$, so $ab \neq_p 0$. Thus $\mathbb{Z}_p$ cannot be an integral domain.

### Non Ex 4

Consider $\mathbb{Z}_n$ such that $n$ is not prime. Suppose $n = ab$ for $a, b \in \mathbb{Z}_n$ such that $a, b \neq 1, n$. Then $a, b$ are zero divisors as

$$ab = n =_p 0$$

### Ex 5

Consider $I = \mathbb{Z}\left[x\right]$, the set of all polynomials with integer coefficients. This example was given in class without a full proof. First, note $I$ is a ring. We will show $I$ is commutative, has a unity, and has no zero divisors. Let $p\left(x\right), q\left(x\right) \in I$ with $p\left(x\right) = \sum_{i=0}^{n} c_i x^i$ and $q\left(x\right) = \sum_{j=0}^{m} d_j x^j$. Then

$$p\left(x\right) q\left(x\right) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} c_j d_{i-j}\right) x^i = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} d_j c_{i-j}\right) x^i = q\left(x\right) p\left(x\right)$$

as each $c_i, d_j$ is an integer and the product of integers is commutative. The unity will be the polynomial 1, as 1 is an integer, thus $1 \in \mathbb{Z}\left[x\right]$. To show there are no zero divisors, consider any two $p\left(x\right), q\left(x\right) \in \mathbb{Z}\left[x\right]$ with the same rules as above. Then if $p\left(x\right) q\left(x\right) = 0$ then $\sum_{j=0}^{i} d_j c_{i-j} = 0$ for all $0 \leq i \leq n+m$. But if we take the highest order term in both $p\left(x\right), q\left(x\right)$, then we have

$$\sum_{j=0}^{n+m} d_j c_{i-j} = c_n d_m$$

as these are the only terms in the polynomial that will contribute to the $x^{n+m}$ term of the product. As $c_n, d_m \neq 0$ and $c_n, d_m$ are both integers,then $c_n d_m \neq 0$, thus $p\left(x\right) q\left(x\right) \neq 0$. This means $I$ has no zero divisors and when combined with the other results implies $I$ is an integral domain.

### Thm

If $I$ is an integral domain and $a, b, c \in I$ such that $a \neq 0$ if $ab = ac$ then $b = c$ (and as $I$ is commutative, if $ba = ca$ then $b = c$)

### Pf

$$ab = ac$$

$$ab - ac = 0$$

$$a\left(b - c\right) = 0$$

as $I$ is an integral domain, then $a = 0$ or $b - c = 0$ but we already are assuming $a \neq 0$, thus

$$b - c = 0$$

$$b = c$$

## Fields

A field $F$ is a commutative ring with unity such that every non-zero element is a unit. This is analogous to stating $F \backslash \{0\}$ is an abelian group under multiplication (Can you see why?).

### Non-Ex 1

$R_1 = \mathbb{Z}$ is not a field under the usual definition of addition and multiplication. Consider $a = 2$. Then

$$ab = 1$$

$$2b = 1$$

is only possible for

$$b = \frac{1}{2} \notin R_1$$

Thus 2 is not a unit and $R_1$ is not a field.

## Ex 2

$R_2 = \mathbb{Q}$ under the usual definition of addition and multiplication. The rational numbers are a commutative ring with unity 1. Let's show each element is a unit. Let $\frac{a}{b} \in R_2$ such that $a, b \neq 0$. Then

$$\frac{a}{b} * \frac{b}{a} = 1$$

As $a, b \neq 0$, then $\frac{b}{a} \in \mathbb{Q}$ and every non-zero rational number is a unit.

## Ex 3

$R_3 = \mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} | a, b \in \mathbb{Q}\right\}$ under the usual addition and multiplication of real numbers. First, let's show this is a ring. As $\mathbb{R}$ is a ring, we can use the subring test to show this. Let $a + b\sqrt{2}, c + d\sqrt{2} \in R_3$.Then

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) = (a - c) + (b - d)\sqrt{2}$$

as $a - c, b - d \in \mathbb{Q}$, then

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) \in R_3$$

Now, to show closure under multiplication:

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$

$$= (ac + 2bd) + (ad + bc)\sqrt{2}$$

as $(ac + 2bd), (ad + bc) \in \mathbb{Q}$, then $\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) \in R_3$. As the real numbers are commutative, then $R_3 \subseteq \mathbb{R}$ must also be commutative. As $1 = 1 + 0\sqrt{2} \in R_3$, $R_3$ is a ring with unity. Now, let's show that $R_3$ is a field. To do so, we will show each non-zero element in $R_3$ has a multiplicative inverse. Let $a + b\sqrt{2} \in R_3$. We want to show the following holds for $c + d\sqrt{2} \neq 0$

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = 1$$

Let's show $\frac{1}{c+d\sqrt{2}} \in R_3$. We will multiply the numerator and denominator by the conjugate of the denominator.

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} * \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}$$

As long as $c^2 - 2d^2 \neq 0$, then $\frac{ac-2bd}{c^2-2d^2}, \frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$. Let's show $c^2 - 2d^2 \neq 0$. If we try solving the equation we get

$$c^2 = 2d^2$$

$$c = 0$$

or

$$c = \pm\sqrt{2d^2} = \pm d\sqrt{2}$$

but if $d$ is rational, then $c$ must be irrational, as $\sqrt{2}$ is irrational. This is a contradiction, as we assume $c$ is rational, thus $c^2 - 2d^2 \neq 0$ and $\frac{ac-2bd}{c^2-2d^2}, \frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$, so for $a + b\sqrt{2} \in R_3$, $\exists \frac{1}{c+d\sqrt{2}} \in R_3$ such that

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = 1$$

so $R_3$ is a field.

## Thm

Every finite integral domain is a field.

## Pf

Let $I$ be a finite integral domain. Then for each $a \in R$, there exist $i, j \in \mathbb{Z}$ such that $i \neq j$ and $a^i = a^j$. Thus

$$a^i = a^j$$

Suppose WLOG $i > j$

$$a^{i-j}a^j = 1a^j$$

By our previous theorem for integral domains implies

$$a^{i-j} = 1$$

Thus

$$aa^{i-j-1} = 1$$

As $i > j$, then $i - j - 1 \geq 0$, so $a^{i-j-1} \in R$ and $a$ is a unit.

## Ex

As $\mathbb{Z}_p$ is a finite integral domain for prime $p$, then $\mathbb{Z}_p$ is a field.

## Thm

Every field is an integral domain.

## Pf

Let $F$ be a field. Suppose $\exists a, b \in F$ such that $a, b$ are zero divisors. Then

$$ab = 0$$

As $F$ is a field, there exists $a^{-1} \in F$, thus

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

$$1b = b = 0$$

but $b \neq 0$ as $b$ is a zero-divisor! Thus to avoid contradiction, there cannot be any zero divisors in a field. This means $F$ is an integral domain.