

Recall, R is an integral domain provided:

- R is a commutative ring
- If $ab = 0$ in R , then either $a = 0$ or $b = 0$.

Examples:

- \mathbb{Z}
- \mathbb{Q}, \mathbb{R}
- Polynomials over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- The Gaussian Integers: $\mathbb{Z}[i] := \{a + bi : a, b \text{ in } \mathbb{Z}\}$
- Quadratic rings: $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \text{ in } \mathbb{Z}\}$, where $|d|$ is a fixed non-square

Sets under Δ and \cap is not an integral domain, since the zero is \emptyset , and $A \cap B = \emptyset$ does not imply $A = \emptyset$ or $B = \emptyset$.

Which \mathbb{Z}_n are integral domains?

Note: n composite $\Rightarrow \mathbb{Z}_n$ is not an integral domain.

Why? Write $n = ab$ where $1 < a, b < n$, $a, b \in \mathbb{Z}$. Then $ab = 0$ in \mathbb{Z}_n but $a \neq 0$ and $b \neq 0$.

Note n is prime

$\Rightarrow ab = 0$ in \mathbb{Z}_p

$\iff p|ab$

$\iff p|a$ or $p|b$

$\iff a = 0$ or $b = 0$ in \mathbb{Z}_p .

So when p is a prime \mathbb{Z}_p is an integral domain.

Characteristic

Given a commutative ring and integer n , we can define $n \cdot 1$ to be the sum of n 1's.

Two things can happen: either for every positive integer $n \cdot 1$ is nonzero or there is a positive integer n such that $n \cdot 1 = 0$.

In former case, R contains $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ which is a copy of the integers. (Example: $R[x]$). We say R has characteristic 0.

In the latter, by WOP there is a smallest positive integer n with $n \cdot 1 = 0$. We call the smallest such n the characteristic of R .

Examples.

If characteristic is not 0, then it is prime!

Why? Suppose n is not prime. Write $n = ab$ where a and b are positive integers less than n .

Then $(a \cdot 1)(b \cdot 1) = (ab) \cdot 1 = 0$.

Since integral domain, either $a \cdot 1 = 0$ or $b \cdot 1 = 0$.

But this is impossible, since n is the smallest positive integer n with $n \cdot 1 = 0$.

A **field** is a commutative ring in which each nonzero element has a multiplicative inverse.

Examples:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

\mathbb{Z}_p, p prime

(Why? Take a nonzero in \mathbb{Z}_p . The map that sends b to ab is $1 - 1$, and hence onto.

This means there is a b with $ab = 1$ in \mathbb{Z}_p .

Field of quotients

Every integral domain can be made into a field; just like we can build the rationals from the reals.

Let R be an integral domain

We consider all pairs (a, b) where $a, b, \in R$ and $b \neq 0$.
(Think of (a, b) as a/b).

We say (a, b) is equivalent to (c, d) provided $ad = bc$

Can show

- (a, b) is equivalent to (a, b)
- If (a, b) is equivalent to (c, d) , then (c, d) is equivalent to (c, d) .
- If (a, b) is equivalent to (c, d) and (c, d) is equivalent to (e, f) , then (a, b) is equivalent to (e, f) .

Define $(a, b) + (e, f) = (ae + bf, bf)$ and
 $(a, b)(e, f) = (ae, bf)$.

Can show $+$ and $*$ are well-defined and give us a field.

The elements of the form $(a, 1)$ behave like the elements of
 R

The additive identity is $(0, 1)$.

The multiplicative identity is $(1, 1)$ (or anything equivalent to
it)

If $a \neq 0$, then multiplicative inverse of (a, b) is (b, a) .

Examples:

Field of quotients of \mathbb{Z} is isomorphic to \mathbb{Q}

Field of quotients of $\mathbb{R}[x]$ is isomorphic to the rational functions.

Field of quotient of Gaussian integers is all $\frac{a+bi}{c+di}$ where $a, b, c, d \in \mathbb{Z}$, and $cd \neq 0$.

Let's look at the Gaussian integers more.

Elements $a + bi$, $a, b \in \mathbb{Z}$.

Additive identity: $0 + 0i$.

Multiplicative identity: $1 + 0i$.

Which $a + bi$ have a multiplicative identity? (I.e. what are the units in the Gaussian integers)

Over the complexes, the inverse of $a + bi$ is

$$\frac{a - bi}{a^2 + b^2}$$

When will this be a Gaussian integer? Need $a + bi$ to be one of $1, -1, i, -i$.

In a ring R an **irreducible** is a non-unit r such that whenever $r = ab$ either a or b is a unit.

Examples:

Irreducibles in \mathbb{Z} are $\pm p$, p prime

No irreducibles in \mathbb{Z}

$2x^2 + 2$ is an irreducible in $\mathbb{Q}[x]$, since it can be factored into linear factors

2 is not an irreducible in the Gaussian integers, since $2 = (1 + i)(1 - i)$.

Gauss introduced $\mathbb{Z}[i]$ to try find patterns among the primes.

He came up with some spectacular pictures like the following that shows the irreducibles in the Gaussian integers of the form $a + bi$ where a and b are between -1000 and 1000 .

And to prove number theoretic results such as:

There are no positive integers x and y with $x^2 + 1 = y^3$.

Useful unary function for the Gaussian integers:

$$N(a + bi) = a^2 + b^2$$

Can show that $N((a + bi)(c + di)) = N(a + bi)N(c + di)$.
 $N(a + bi) = 1$ iff $a, b \in \{1, -1, i, -i\}$, i.e. iff $a + bi$ is a unit.

5 is irreducible in the Gaussian integers:

If x and y are Gaussian integers with $xy = 5$, then

$$N(x)N(y) = N(5) = 25.$$

Note there are no integers a and b with $a^2 + b^2 = 5$.

So $N(x) \neq 5$. We conclude $N(x) = 1$ or $N(y) = 1$.

So either x or y is a unit, and 5 is irreducible.

Each Gaussian integer is either 0, a unit, irreducible, or the product of irreducibles.

Proof. Assume the Gaussian integer z is neither 0, a unit, nor irreducible.

Then $z = ab$ for some non-units a and b .

Now $N(z) = N(a)N(b)$. Since a and b aren't units $N(a), N(b) < N(z)$

We've reduced to a smaller case. Now express a and b as products of irreducibles, and concatenate them to get z as a product of irreducibles. ■

