

Lecture 05: Integral domains

Monday, April 9, 2018 11:05 PM

We were proving:

Proposition. Let A be a unital commutative ring. Then A is an integral domain if and only if it has the cancellation property;

that means $ab=ac$ and $a \neq 0 \Rightarrow b=c$.

Pf. We have already proved (\Rightarrow) .

(\Leftarrow) Suppose to the contrary that A has a zero-divisor.

So $a \cdot b = 0$ for some $a \neq 0$ and $b \neq 0$. Then $a \cdot b = a \cdot 0$

Hence by the cancellation property $b=0$, which is a contradiction. ■

Lemma. A field F is an integral domain.

Pf. Suppose $a \cdot b = 0$ and $a \neq 0$. Then $a^{-1} \in F$, $a^{-1} \cdot (a \cdot b) = 0$

$\Rightarrow 1_F \cdot b = 0 \Rightarrow b = 0$. And so F has no zero-divisor. ■

Ex. \mathbb{Z} is an integral domain which is not a field.

Next result shows that in finite case converse holds.

Lecture 05: Integral domains and fields

Monday, April 9, 2018 11:27 AM

Theorem. Suppose D is a finite integral domain. Then D is a field.

Pf. For $a \in D \setminus \{0\}$, let $f_a: D \rightarrow D$, $f_a(x) = ax$.

Claim f_a is injective.

Pf of claim. $f_a(x_1) = f_a(x_2) \Rightarrow ax_1 = ax_2$

by the cancellation property $\Rightarrow x_1 = x_2$

Claim. f_a is surjective.

Pf of claim. Since D is finite and $f_a: D \rightarrow D$ is injective,

f_a is surjective. If not and $|D| = n$, then f_a sends n

"pigeons" to at most $n-1$ "pigeonholes"; and so by the

the pigeonhole principle, two "pigeons" are sent to the same

"pigeonholes" which contradicts injectivity of f_a .

Finishing proof. Since f_a is surjective, $\exists a' \in D$ s.t. $f_a(a') = 1$.

which means $\exists a' \in D$, $aa' = 1$. And so a has a multiplicative

Lecture 05: Integral domains and fields

Monday, April 9, 2018 11:38 AM

inverse. Hence D is a field. (as it is also a non-zero unital commutative ring). ■

Proposition. (1) \mathbb{Z}_n is not an integral domain if n is composite.

(2) \mathbb{Z}_p is a field if p is prime.

Pf. (1) $n=ab$ and $1 < a, b < n$. Then $a \circ b = 0$ in \mathbb{Z}_n and $a \neq 0, b \neq 0$ in \mathbb{Z}_n . So \mathbb{Z}_n has zero-divisors.

(2) It is enough to show \mathbb{Z}_p is an integral domain as it is finite.

Suppose $a \circ b = 0$ in \mathbb{Z}_p . That means $p \mid ab$.

Since p is prime, $p \mid a$ or $p \mid b$ (from 109). And so either $a = 0$ or $b = 0$ in \mathbb{Z}_p . Therefore \mathbb{Z}_p does not have a zero-divisor; and claim follows. ■

Proposition. Suppose A is an integral domain. Then $\text{char}(A)$ is either 0 or prime.

Pf. If not, $\text{char}(A) = ab$ for some $a, b > 1$. Then

Lecture 05: Integral domains and field of fractions

Wednesday, April 11, 2018 11:04 AM

$$(a1_A)(b1_A) = (\underbrace{1_A + \dots + 1_A}_a) (\underbrace{1_A + \dots + 1_A}_b) = \underbrace{1_A \cdot 1_A + \dots + 1_A \cdot 1_A}_{ab} \\ = ab 1_A = 0 ; \text{ and}$$

$a1_A \neq 0$ and $b1_A \neq 0$ as $\text{char}(A) = \text{ord}(1_A) = ab$ and $a, b < ab$.

An integral domain is not necessarily a field; but for any integral domain D , there is a "smallest" field which contains D . Similar to \mathbb{Q} containing \mathbb{Z} .

Theorem. Suppose D is an integral domain. Then there is a field $Q(D)$ and a ring homomorphism $\theta: D \rightarrow Q(D)$ such that (1) θ is an embedding.

(2) Any element of $Q(D)$ is of the form $\theta(a)\theta(b)^{-1}$ for $a \in D, b \in D \setminus \{0\}$.

(3) If F is a field and $\varphi: D \hookrightarrow F$ is an injective ring homomorphism, then $\exists \tilde{\varphi}: Q(D) \hookrightarrow F$ s.t. $\tilde{\varphi}|_{Q(D)} = \varphi$.

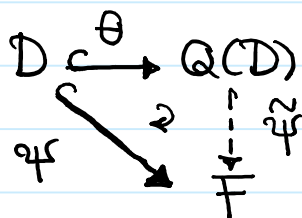
(4) There is a unique field $Q(D)$ with these properties (up to

Lecture 05: Field of fractions

Wednesday, April 11, 2018 11:16 AM

an isomorphism), and it is called the field of fractions of D .

(We often describe part (3) using the following diagram:



(we say it is a commuting diagram.))

We will prove this statement next time.