Integral domain

Monday, August 7, 2017 11:07 PM

As we saw in the previous lecture, in a ring we do not necessarily have the cancellation law.

<u>Def.</u> Let R be a ring. A non-zero element a of R is called a <u>zero divisor</u> if $\exists\ b \in R\setminus\{0\}$ such that either $ab=0$ or $ba=0$.

<u>Lemma.</u> The cancellation laws hold in R if and only if R does NOT have a zero divisor.

<u>Pf.</u> $(\Rightarrow)$ $ab = 0 = a\cdot 0 \Rightarrow b=0$

$\boxed{\text{by the cancellation law}}$

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

$(\Leftarrow)$ $ax_1 = ax_2 \Rightarrow \left.\begin{array}{l} 0 = a(x_1-x_2) \\ a\neq 0 \\ \text{no zero divisor}\end{array}\right\} \Rightarrow x_1-x_2=0 \Rightarrow x_1=x_2.$

$y_1 a = y_2 a \Rightarrow \left.\begin{array}{l} 0 = (y_1-y_2)a \\ a\neq 0 \\ \text{no zero divisor}\end{array}\right\} \Rightarrow y_1-y_2=0 \Rightarrow y_1=y_2.$ ■

<u>Def.</u> A commutative unital ring D, with $1\neq 0$ and no zero divisor is called an integral domain.

Finite integral domains

Monday, August 7, 2017 11:25 PM

<u>Ex.</u> If F is a field, then F is an integral domain.

<u>Pf.</u> $\left.\begin{array}{l} ab=0 \\ a\neq 0 \Rightarrow \exists\, a^{-1}\in F \end{array}\right\} \Rightarrow a^{-1}(ab)=a^{-1}\,0=0$

$\Rightarrow b=0.$

So F has no zero-divisor.

Since F is a field, it is a commutative unital ring and $1\neq 0$. ∎

<u>Ex.</u> $\mathbb{Z}$ is an integral domain; and it is not a field.

<u>Proposition.</u> Suppose D is a finite integral domain. Then D is a field.

<u>Pf.</u> For $a\in D\setminus\{0\}$, let $\ell_a: D\to D$ be

$$\ell_a(x)=ax.$$

Since D has the cancellation law, ℓ_a is one-to-one.

Since D is finite, ℓ_a is a bijection. So $\exists\, a'\in D$ such that $\ell_a(a')=1$ (D is unital.). So $aa'=1$. Since D commutative, $aa'=a'a=1$. Thus $a\in U(D)$. Therefore D is a field (as D is a unital commutative ring and $U(D)=D\setminus\{0\}$.) ∎

Integral domains among Zn's

Monday, August 7, 2017 11:35 PM

Ex. $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

($\Rightarrow$)

Pf. Suppose to the contrary that n is composite and $\mathbb{Z}_n$ is an integral domain. Then

$n = ab$ for some $1 < a, b < n$. So

$a \odot_n b = 0$ as the remainder of $ab = n$ divided by n is 0, which implies $\mathbb{Z}_n$ has a zero divisor.

And that gives us a contradiction.

($\Leftarrow$) $U(\mathbb{Z}_p) = \{a \in \mathbb{Z}_p \mid \gcd(a,p) = 1\}$

$$= \{1, 2, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}.$$

So $\mathbb{Z}_p$ is a field, and therefore it is an integral domain. ∎

Corollary. If D is an integral domain, then $\mathrm{char}(D)$ is either 0 or prime. (why?)

The field of fractions of an integral domain

Wednesday, August 9, 2017 12:07 PM

We have seen that any field is an integral domain, but the converse is not true in general. But we will see that any integral domain can be embedded into a field; think about $\mathbb{Z}$ and $\mathbb{Q}$.

Starting with an integral domain D, we would like to construct its field of fractions (also known as field of quotients).

So elements of the field $Q(D)$ of fractions of D are informally of the form numerator / denom. and the denomi. cannot be zero. But a/b should be equal to ar/br. So we start with $D \times (D \setminus \{0\})$ and then partition it in a way that, if (a_1, b_1) and (a_2, b_2) are in the same subset, then "$a_1/b_1 = a_2/b_2$". But what do we expect from $a_1/b_1 = a_2/b_2$? This should imply $a_1 b_2 = a_2 b_1$ (remember that D is a commutative ring.) So for any $(a,b) \in D \times (D \setminus \{0\})$, let

$$[a,b] := \{(a', b') \in D \times (D \setminus \{0\}) \mid ab' = a'b\}.$$

The field of fractions

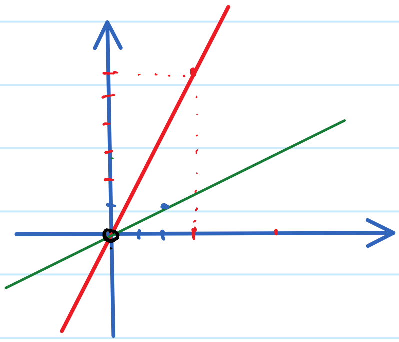
Wednesday, August 9, 2017 12:23 PM

Lemma. $\{[(a,b)] \mid (a,b) \in D \times (D \setminus \{0\})\}$ is a partition of

$D \times (D \setminus \{0\})$.

[Before we get to the proof, let's try to visualize these sets

for $D = \mathbb{Z}$.



So we have to remove the y-axis

$[(2,1)]$
$= \{(x,y) \mid x = \frac{2}{1} y\}$

$[(3,5)]$
$= \{(x,y) \mid x = \frac{3}{5} y\}$

and consider the lines which pass through the origin (excluding the origin). It is clear that we are getting a partition.]

Pf. For any $(a,b) \in D \times (D \setminus \{0\})$, we have

$ab = ab$ so $(a,b) \in [(a,b)]$. And so the union of

these sets $[(a,b)]$ cover $D \times (D \setminus \{0\})$.

- Next we have to show,

$$[(a_1,b_1)] \cap [(a_2,b_2)] \neq \emptyset \Rightarrow [(a_1,b_1)] = [(a_2,b_2)].$$

Suppose $(c,d) \in [(a_1,b_1)] \cap [(a_2,b_2)]$. Then

$c b_1 = d a_1$ and $c b_2 = d a_2$.

Partitioning DxD\{0}

Wednesday, August 9, 2017 1:04 PM

So $\left.\begin{array}{l} cb_1b_2 = (cb_1)b_2 = da_1b_2 \\ \quad\ \ \| \\ cb_2b_1 = (cb_2)b_1 = da_2b_1 \end{array}\right\} \Rightarrow$ by the cancellation law, $a_1b_2 = a_2b_1$, as $d \neq 0$.

Suppose $(a', b') \in [(a_1, b_1)]$. Then $a'b_1 = b'a_1$.

$$\left.\begin{array}{l} a'b_1b_2 = b'a_1b_2 = b'a_2b_1 \\ b_1 \neq 0 \end{array}\right\} \Rightarrow \text{by the cancellation law } a'b_2 = b'a_2.$$

$$\Rightarrow (a', b') \in [(a_2, b_2)].$$

So $[(a_1, b_1)] \subseteq [(a_2, b_2)]$. Similarly we have

$$[(a_2, b_2)] \subseteq [(a_1, b_1)].$$

And so $[(a_1, b_1)] = [(a_2, b_2)]$. ∎

A close look at the above proof shows that

Lemma $[(a_1, b_1)] = [(a_2, b_2)]$ if and only if $a_1b_2 = b_1a_2$

(Exercise) (Hint. ($\Rightarrow$) is easier:

$$\left.\begin{array}{l} [(a_1, b_1)] = [(a_2, b_2)] \\ (a_1, b_1) \in [(a_1, b_1)] \end{array}\right\} \Rightarrow (a_1, b_1) \in [(a_2, b_2)] \Rightarrow a_1b_2 = b_1a_2.$$

.)

Defining the operations on the defined partition

Wednesday, August 9, 2017 1:18 PM

Next we will make $Q(D) := \{[(a,b)] \mid (a,b) \in D \times (D \setminus \{0\})\}$ into a field.

<u>Lemma</u>. The following are well-defined binary operators on $Q(D)$:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$

and

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)].$$

[The above definition is inspired by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ in $\mathbb{Q}$.]

<u>Pf</u>. Let's try to understand what the statement claims:

If the defined $+$ is an operation, then we should have

$$\left.\begin{array}{l}[(a_1,b_1)] = [(a_2,b_2)] \\ [(c_1,d_1)] = [(c_2,d_2)]\end{array}\right\} \Rightarrow [(a_1,b_1)] + [(c_1,d_1)] = [(a_2,b_2)] + [(c_2,d_2)],$$

which means we have to show

$$\left.\begin{array}{l}[(a_1,b_1)] = [(a_2,b_2)] \\ [(c_1,d_1)] = [(c_2,d_2)]\end{array}\right\} \overset{?}{\Rightarrow} [(a_1d_1+b_1c_1, b_1d_1)] = [(a_2d_2+b_2c_2, b_2d_2)]$$

So using the previous lemma, we have to show

$$\left.\begin{array}{l}a_1b_2 = b_1a_2 \\ c_1d_2 = d_1c_2\end{array}\right\} \overset{?}{\Rightarrow} (a_1d_1+b_1c_1)\, b_2d_2 = (a_2d_2+b_2c_2)\, b_1d_1.$$

$$(a_1d_1 + b_1c_1)\, b_2d_2 = \underbrace{a_1b_2}\, d_1d_2 + b_1b_2\, \underbrace{c_1d_2} = b_1a_2\, d_1d_2 + b_1b_2\, d_1c_2$$
$$= (a_2d_2+b_2c_2)\, b_1d_1; \quad \text{as we wished.}$$

Q(D) is a ring

Wednesday, August 9, 2017 1:32 PM

The other part is similar. Exercise finish the proof. ∎

Lemma. $(Q(D),+)$ is an additive group.

Pf. Associativity:

$$\Big(\underbrace{[(a_1,b_1)]+[(a_2,b_2)]}_{[(a_1b_2+b_1a_2,\ b_1b_2)]}\Big)+[(a_3,b_3)] \overset{?}{=} [(a_1,b_1)]+\Big(\underbrace{[(a_2,b_2)]+[(a_3,b_3)]}_{[(a_2b_3+b_2a_3,\ b_2b_3)]}\Big)$$

$$[((a_1b_2+b_1a_2)b_3+(b_1b_2)a_3,\ b_1b_2b_3)] \overset{?}{=} [(a_1(b_2b_3)+b_1(a_2b_3+b_2a_3),\ b_1b_2b_3)]$$

$$(a_1b_2+b_1a_2)b_3+(b_1b_2)a_3 = a_1b_2b_3+a_2b_1b_3+a_3b_1b_2$$

$$\parallel$$

$$a_1(b_2b_3)+b_1(a_2b_3+b_2a_3) = a_1b_2b_3+a_2b_1b_3+a_3b_1b_2 \quad ✓$$

Abelian: $\underbrace{[(a,b)]+[(c,d)]}_{[(ad+bc,\ bd)]} \overset{?}{=} \underbrace{[(c,d)]+[(a,b)]}_{[(cb+da,\ db)]}$

And D is commutative.

Nuetral element: $[(a,b)]+[(0,1)] = [(a\cdot 1+b\cdot 0,\ b\cdot 1)]$
$= [(a,b)]$

Negative of an element: $[(a,b)]+[(-a,b)] = [(ab+b(-a),\ b^2)]$
$= [(0,b^2)] \underset{\boxed{0\times 1 = b^2\times 0}}{=} [(0,1)]$ ∎

Q(D) is a unital commutative ring

Wednesday, August 9, 2017 1:50 PM

Lemma. $(Q(D),+,\cdot)$ is a unital commutative ring.

Pf. We have already proved that $(Q(D),+)$ is an abelian group.

Next we show $\cdot$ is associative.

$$\underbrace{\underbrace{\big([(a_1,b_1)]\cdot[(a_2,b_2)]\big)}_{[(a_1a_2,\,b_1b_2)]}\cdot[(a_3,b_3)]}_{[((a_1a_2)a_3,\ (b_1b_2)b_3)]} \overset{?}{=} [(a_1,b_1)]\cdot\underbrace{\big([(a_2,b_2)]\cdot[(a_3,b_3)]\big)}_{[(a_2a_3,\,b_2b_3)]}$$

$$[(a_1(a_2a_3),\ b_1(b_2b_3))]$$

And we get the equality as D is a ring.

Commutative. $$\underbrace{[(a_1,b_1)]\cdot[(a_2,b_2)]}_{[(a_1a_2,\,b_1b_2)]} \overset{?}{=} \underbrace{[(a_2,b_2)]\cdot[(a_1,b_1)]}_{[(a_2a_1,\,b_2b_1)]}$$

we get the equality as D is commutative.

Distribution.

$$\underbrace{[(a_1,b_1)]\cdot\big(\underbrace{[(a_2,b_2)]+[(a_3,b_3)]}_{[(a_2b_3+b_2a_3,\ b_2b_3)]}\big)} = \underbrace{\underbrace{[(a_1,b_1)]\cdot[(a_2,b_2)]}_{[(a_1a_2,\,b_1b_2)]}+\underbrace{[(a_1,b_1)]\cdot[(a_3,b_3)]}_{[(a_1a_3,\,b_1b_3)]}}$$

$$[(\underbrace{a_1(a_2b_3+b_2a_3)}_{r},\ \underbrace{b_1(b_2b_3)}_{s})] \qquad [(\underbrace{(a_1a_2)(b_1b_3)+(b_1b_2)(a_1a_3)}_{\underbrace{b_1a_1(a_2b_3+b_2a_3)}_{b_1r}},\ \underbrace{(b_1b_2)(b_1b_3)}_{\underbrace{b_1b_1b_2b_3}_{b_1s}})]$$

Since $r(b_1s)=s(b_1r)$, we have $[(r,s)]=[(b_1r,b_1s)]$ which proves the equality.