Lecture 04: Characteristic

Friday, January 18, 2019 8:52 AM

In the previous lecture we proved that $\operatorname{char} A = \underset{a\in A}{\mathrm{l.c.m.}}\ o(a)$.

Next we get a much better result for a unital ring:

<u>Proposition</u>. Suppose A is a unital ring. If $o(1_A) < \infty$, then $\operatorname{char} A = o(1_A)$; if $o(1_A) = \infty$, then $\operatorname{char} A = 0$.

<u>Pf</u>. If $o(1_A) = \infty$, then $\nexists n \in \mathbb{Z}^+$, $n 1_A = 0$; and so $C_A = \emptyset$.

Therefore $\operatorname{char} A = 0$.

. Let $n := o(1_A)$. We will show that $n = \underset{a\in A}{\mathrm{l.c.m}}\ o(a)$.

$n 1_A = 0 \Rightarrow \forall a \in A, (n 1_A) a = 0 \Rightarrow n a = 0$

$\Rightarrow o(a) \mid n$.

Hence n is a common multiple of $o(a)$'s; thus

$$\underset{a\in A}{\mathrm{l.c.m.}}\ o(a) \le n. \qquad (\mathrm{I})$$

On the other hand $\underset{a\in A}{\mathrm{l.c.m.}}\ o(a)$ is a (positive) multiple of $o(1_A)$; and so $\underset{a\in A}{\mathrm{l.c.m.}}\ o(a) \ge o(1_A) = n$ (II)

(I) and (II) imply $o(1_A) = \underset{a\in A}{\mathrm{l.c.m.}}\ o(a)$. And by the result proved in the previous lecture claim follows. ∎

Lecture 04: Characteristic

Friday, January 18, 2019 9:03 AM

<u>Ex.</u> Find $\mathrm{char}(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k})$.

<u>Solution</u>. Since $\mathbb{Z}_{n_i}$'s are unital rings, so is their direct product (as you showed it in your HW assignment). Hence

$$\mathrm{char}(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}) = o(\text{the identity})$$

$$= o(1_{\mathbb{Z}_{n_1}}, \ldots, 1_{\mathbb{Z}_{n_k}}) \qquad \text{(the same HW)}$$

Let $m := o(1_{\mathbb{Z}_{n_1}}, \ldots, 1_{\mathbb{Z}_{n_k}})$. So m is the smallest positive integer s.t. $m(1_{\mathbb{Z}_{n_1}}, \ldots, 1_{\mathbb{Z}_{n_k}}) = (0, \ldots, 0)$. Notice

$$m(1_{\mathbb{Z}_{n_1}}, \ldots, 1_{\mathbb{Z}_{n_k}}) = (0, \ldots, 0) \Leftrightarrow (m 1_{\mathbb{Z}_{n_1}}, \ldots, m 1_{\mathbb{Z}_{n_k}}) = (0, \ldots, 0)$$

$$\Leftrightarrow m 1_{\mathbb{Z}_{n_1}} = 0, \ldots, m 1_{\mathbb{Z}_{n_k}} = 0$$

$$\Leftrightarrow o(1_{\mathbb{Z}_{n_1}}) \mid m, \ldots, o(1_{\mathbb{Z}_{n_k}}) \mid m$$

$$\Leftrightarrow n_1 \mid m, \ldots, n_k \mid m$$

$$\Leftrightarrow m \text{ is a common multiple of } n_1, \ldots, n_k.$$

Hence smallest positive integer with this property is $\mathrm{l.c.m.}(n_1, \ldots, n_k)$. So overall $\mathrm{char}(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}) = \mathrm{l.c.m.}(n_1, \ldots, n_k)$. ∎

Lecture 04: Integral domain

Friday, January 18, 2019 9:18 AM

Def. A unital commutative ring D is called an integral domain if $0 \neq 1$ and D has no zero-divisor.

Ex. $\mathbb{Z}_4$ is not an integral domain as $2 \neq 0$ and $2 \times 2 = 0$.

- $\mathbb{Z}$, $\underbrace{\mathbb{Q}, \mathbb{R}, \text{ and } \mathbb{C}}_{\substack{\text{more special;} \\ \text{these are fields.}}}$ are integral domains.

Proposition In a unital ring A, $D(A) \cap A^\times = \emptyset$ where $D(A)$ is the set of all zero-divisors of A. In particular a field F is an integral domain.

Pf. Suppose to the contrary that $a \in D(A) \cap A^\times$. So

$$\underbrace{a \neq 0 \text{ and } \exists\, a' \in A \setminus \{0\},\ a a' = 0}_{a \in D(A)} \text{ and } \underbrace{\exists\, a'' \in A,\ a'' a = 1}_{a \in A^\times}.$$

$$\Rightarrow \left.\begin{array}{l} a''(a a') = a'' \cdot 0 = 0 \\ \quad \parallel \\ (a'' a) a' = 1 \cdot a' = a' \end{array}\right\} \Rightarrow a' = 0 \text{ which is a contradiction.}$$

- Since F is a field, it is a unital commutative ring and $0 \neq 1$. Therefore to show F is an integral domain, it is enough to show $D(F)=\emptyset$. By the first part of this proposition $D(F)\cap F^{\times}=\emptyset$; and so $D(F)\subseteq$ complement of $F^{\times}$. As $F^{\times}=F\setminus\{0\}$, we deduce that $D(F)\subseteq\{0\}$. Since 0 is not a zero-divisor, $D(F)=\emptyset$; and claim follows. ∎

Notice that $\mathbb{Z}$ is an integral domain which is not a field; and so the converse of the above statement is not true in general. Next we see that when a ring is finite then the converse holds as well.

Theorem. A finite integral domain D is a field.

Pf. Since D is an integral domain, it is a unital commutative ring and $0\neq 1$. So to show it is a field, it is enough to prove any non-zero element is a unit; that means we have to show $\forall a\in D\setminus\{0\}, \exists a'\in D, aa'=1$. (Similar to the proof of Cayley's theorem in group theory we make use of $\ell_a: D\to D$, $\ell_a(x):=ax$.) Let $\ell_a: D\to D$, $\ell_a(x)=ax$.

Lecture 04: Integral domain

Friday, January 18, 2019 9:39 AM

We have to show that $\exists a' \in D$ s.t. $aa' = 1$ which is equivalent to saying $\in 1$ Image of l_a. So it is enough to show l_a is surjective. We will prove that is l_a injective, and then using pigeonhole and the assumption that D is finite, we deduce that l_a is surjective and claim would follow.

<u>Injectivity of l_a</u>. $l_a(x_1) = l_a(x_2) \Rightarrow a x_1 = a x_2$

now we have to show that we can cancel out a.

$$a x_1 = a x_2 \Rightarrow a x_1 - a x_2 = 0 \Rightarrow a(x_1 - x_2) = 0$$

$\Rightarrow$ either $a = 0$ or $x_1 - x_2 = 0$ as D has no zero-divisor

$\underset{(\text{as } a \neq 0)}{\Rightarrow}$ $x_1 - x_2 = 0 \Rightarrow x_1 = x_2$

(we showed the cancellation law.)

Since $|D| < \infty$ and $l_a : D \to D$ is injective, l_a is surjective.

Hence $1 \in$ Image of l_a, which means $\exists a' \in D$, $l_a(a') = 1$, and so $aa' = 1$; and claim follows. ∎

Lecture 04: Recall an application of pigeonhole principle

Friday, January 18, 2019 9:49 AM

<u>Recall</u>. Suppose X and Y are two finite sets and $|X|=|Y|$.

Suppose $f: X \to Y$ is a function. Then the following are equivalent: (a) f is injective; (b) f is surjective;

(c) f is bijective;

(a) $\Rightarrow$ (b) Suppose f is not surjective. Think about elements of X as "pigeons", elements of Y as "pigeonholes", and f as a way of assigning pigeonholes to pigeons. Since f is not surjective, we have at least one less pigeonhole to assign to pigeons. So by the pigeonhole principle at least two pigeons should be assigned to the same pigeonholes; but this means f is not injective which is a contradiction.

(b) $\Rightarrow$ (c) We have to show f is injective. If not, let's say the 1^{st} and the 2^{nd} pigeons are sharing a pigeonhole. So only $n-2$ pigeons remain; and they cannot cover the $n-1$ remaining pigeonholes. This contradicts surjectivity of f.

(c) $\Rightarrow$ (a) is clear. ∎

Lecture 04: Integral domain

Friday, January 18, 2019 10:07 AM

<u>Theorem</u>. Suppose $n \in \mathbb{Z}^+$. Then the following statements are equivalent:

(a) $\mathbb{Z}_n$ is a field, (b) $\mathbb{Z}_n$ is an integral domain, (c) n is prime

<u>Pf</u>. (a) $\Rightarrow$ (b) A field is an integral domain.

(b) $\Rightarrow$ (c) If not, n is either 1 or ab for some $0<a,b<n$

- In $\mathbb{Z}_1$, $0=1$; and so it is not an integral domain which is a contradiction.

- If $n=ab$ for some $0<a,b<n$, then

  $a,b \in \mathbb{Z}_n \setminus \{0\}$ and $ab=0$ in $\mathbb{Z}_n$; and so a and b are zero-divisors in $\mathbb{Z}_n$, which implies $\mathbb{Z}_n$ is not an integral domain. This is a contradiction.

(c) $\Rightarrow$ (a) We proved this in the previous lecture. ∎

As we have seen, an integral domain is not necessarily a field, e.g. $\mathbb{Z}$. Any integral domain, however, can be embedded in a field and there is the <u>smallest</u> such field, e.g. $\mathbb{Z} \subseteq \mathbb{Q}$.

Lecture 04: Field of fractions

Friday, January 18, 2019 12:45 PM

For instance in the case of $\mathbb{Z}$, if a field F contains $\mathbb{Z}$ as a subring, then $\forall\, m \in \mathbb{Z}\setminus\{0\}$, $\frac{1}{m}$ exists in F, and so for any $n \in \mathbb{Z}$, $m \in \mathbb{Z}\setminus\{0\}$, $\frac{n}{m}$ exists in F, which means there is a copy of $\mathbb{Q}$ in F.

Our goal is to show for any integral domain D there is the smallest field $Q(D)$ that contains a copy of D; $Q(D)$ is called the field of fractions of D.

We will use $\mathbb{Q}$ as a guide for the construction of $Q(D)$. That means we will make sense of fractions $\frac{a}{b}$ for $a \in D$ and $b \in D\setminus\{0\}$. One might be tempted to consider $D \times (D\setminus\{0\})$ to be the set for $Q(D)$; viewing first component as the numerator and the 2^{nd} component as the denominator. The problem with this naïve approach is that $\frac{ar}{br} = \frac{a}{b}$ for any $r \in D\setminus\{0\}$. So we need to treat (a,b) and (ar,br) as equal. And in general we need to treat (a_1,b_1) and (a_2,b_2)

Lecture 04: Field of fractions

Friday, January 18, 2019 12:56 PM

as equal if $a_1 b_2 = a_2 b_1$ $\left(\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftarrow a_1 b_2 = a_2 b_1\right)$.

That is why we collect all such pairs in a subset and consider the collection of these subsets. Intuitively each subset consists of pairs that represent the same fraction; let

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

<u>Theorem</u>. $\{[(a,b)] \mid (a,b) \in D \times (D \setminus \{0\})\}$ is a partition of $D \times (D \setminus \{0\})$.

We will prove this in a several steps:

<u>Step 1</u>. $(c,d) \in [(a,b)] \Rightarrow (a,b) \in [(c,d)]$

<u>Pf</u>. $(c,d) \in [(a,b)] \Rightarrow cb = ad \Rightarrow (a,b) \in [(c,d)]$.

<u>Step 2</u>. $\left.\begin{array}{l}(c,d) \in [(a,b)] \\ (e,f) \in [(c,d)]\end{array}\right\} \Rightarrow (e,f) \in [(a,b)]$.

<u>Pf.</u> $\left.\begin{array}{l}(c,d) \in [(a,b)] \Rightarrow cb = ad \Rightarrow ecb = ead \\ (e,f) \in [(c,d)] \Rightarrow ed = fc \Rightarrow aed = afc\end{array}\right\} \Rightarrow$

$ceb - caf = c(eb - af) = 0 \Rightarrow$ either $c = 0$ or $eb = af$. In latter case $(e,f) \in [(a,b)]$. If $c = 0$, then

Lecture 04: Field of fractions

Friday, January 18, 2019 1:05 PM

$$\left.\begin{array}{l} 0=cb=ad \Rightarrow \left.\underset{d\neq 0}{a=0 \text{ or } d=0}\right\} \Rightarrow a=0 \\ 0=cf=ed \Rightarrow \left.\underset{d\neq 0}{e=0 \text{ or } d=0}\right\} \Rightarrow e=0 \end{array}\right\} \Rightarrow af=be$$

And so again $(e,f)\in[(a,b)]$.

<u>Step 3.</u> $(c,d)\in[(a,b)] \Rightarrow [(a,b)]=[(c,d)]$.

<u>Pf.</u> $(c,d)\in[(a,b)] \Rightarrow [(c,d)]\subseteq[(a,b)]$ (I) by step 2.

$(c,d)\in[(a,b)] \Rightarrow (a,b)\in[(c,d)]$ by step 1

$\Rightarrow [(a,b)]\subseteq[(c,d)]$ (II) by step 2.

(I) and (II) imply $[(a,b)]=[(c,d)]$.

<u>Step 4.</u> $[(a,b)]\cap[(a',b')]\neq\emptyset \Rightarrow [(a,b)]=[(a',b')]$.

<u>Pf.</u> $(c,d)\in[(a,b)]\cap[(a',b')] \Rightarrow$

$$\left\{\begin{array}{l} (c,d)\in[(a,b)] \xrightarrow{\text{Step3}} [(c,d)]=[(a,b)] \\ (c,d)\in[(a',b')] \xrightarrow[\text{Step3}]{} [(c,d)]=[(a',b')] \end{array}\right\} \Rightarrow [(a,b)]=[(a',b')].$$

<u>Step 5.</u> $\displaystyle\bigcup_{(a,b)\in D\times(D\setminus\{0\})} [(a,b)] = D\times(D\setminus\{0\})$

<u>Pf.</u> $ab-ab=0 \Rightarrow (a,b)\in[(a,b)]$. ∎

Steps 1–5 imply the mentioned theorem. We will treat $[(a,b)]$ as a/b.