Lecture 04: Characteristic of a ring

Monday, April 9, 2018 8:27 AM

Def. For a ring A consider

$$C_A = \{n \in \mathbb{Z}^+ \mid \forall x \in A,\ nx = 0\}.$$

If $C_A = \emptyset$, we say the characteristic of A is zero.

If $C_A \neq \emptyset$, then by the well-ordering principle it has a minimum. And the characteristic of A is $\min(C_A)$.

Recall from group theory in a group $(G,+)$, $ng = 0$ if and only if $|g| \mid n$ where $|g|$ is the order of g.

Lemma. For a ring A, let $\ell = \operatorname{l.c.m.}_{a \in A} |a|$. If $\ell < \infty$, then $\operatorname{char}(A) = \ell$. If $\ell = \infty$, then $\operatorname{char}(A) = 0$.

Pf. Let $C_A = \{n \in \mathbb{Z}^+ \mid \forall x \in A,\ nx = 0\}$. Then

$$n \in C_A \Leftrightarrow \forall x \in A,\ nx = 0 \Leftrightarrow \forall x \in A,\ |x| \mid n$$

$$\Leftrightarrow \operatorname{l.c.m}_{x \in A} |x| \leq n \text{ and } \operatorname{l.c.m.}_{x \in A} |x| \in C_A \text{ if finite}.$$

So, if $\operatorname{l.c.m}_{x \in A} |x| < \infty$, then $C_A \neq \emptyset$ and $\min(C_A) = \operatorname{l.c.m}_{x \in A} |x|$.

if $\operatorname{l.c.m}_{x \in A} |x| = \infty$, then $C_A = \emptyset$; and so $\operatorname{char}(A) = 0$. ∎

Lemma. Suppose A is a unital ring. Then $\operatorname{char}(A) = 0$ if 1_A is of infinite (additive) order and otherwise $\operatorname{char}(A) = |1_A|$.

Lecture 04: Characteristic of a ring

Monday, April 9, 2018 8:44 AM

<u>Pf.</u> . If $|1_A| = \infty$, then there is no $n \in \mathbb{Z}^+$ s.t. $n 1_A = 0$. And so $\mathrm{char}(A) = 0$.

. If $|1_A| = n$, then, for any $x \in A$,

$$nx = n(1_A \cdot x) = \underbrace{1_A \cdot x + 1_A \cdot x + \cdots + 1_A \cdot x}_{n \text{ times}} = (\underbrace{1_A + \cdots + 1_A}_{n \text{ times}}) \cdot x$$

$$= (n 1_A) \cdot x = 0 \cdot x = 0.$$

And so, for any $x \in A$, $nx = 0$.

Since $|1_A| = n$, for $m < n$, $m 1_A \neq 0$. Therefore

$n = \min\{k \in \mathbb{Z}^+ \mid \forall x \in A,\ kx = 0\}$; and so $\mathrm{char}(A) = n$. ∎

<u>Ex.</u> $\mathrm{Char}(\mathbb{Z}_n) = n$.

<u>Pf.</u> $\mathrm{ord}(1_{\mathbb{Z}_n}) = n$. ∎

<u>Ex.</u> $\mathrm{Char}(\mathbb{Z} \times \mathbb{Z}_n) = 0$.

<u>Pf.</u> Since $(1,1)$ is the unity of this ring, we need to find its order. So we need to find $m \in \mathbb{Z}^+$ s.t. $m(1,1) = (0,0)$. Which means $(m, m 1_{\mathbb{Z}_n}) = (0,0)$; and so there is no such m. ∎

Lecture 04: Characteristic of a ring

Tuesday, April 10, 2018 12:39 AM

Ex. Let $\bigoplus_{n=2}^{\infty} \mathbb{Z}_n = \{(a_m)_{m=2}^{\infty} \mid a_m \in \mathbb{Z}_m$ and except for finitely many m, a_m's are $0\}$.

Notice that if, for $m \geq M$, $a_m = 0$ and, for $m \geq M'$, $b_m = 0$, then $a_m + b_m = 0$ and $a_m b_m = 0$ for $m \geq \max(M, M')$.

And so $\bigoplus_{n=2}^{\infty} \mathbb{Z}_n$ is a ring. Show that $\mathrm{Char}(\bigoplus_{n=2}^{\infty} \mathbb{Z}_n) = 0$, but order of any element is finite.

Solution. For any $x = (a_2, a_3, \dots) \in \bigoplus_{n=2}^{\infty} \mathbb{Z}_n$, there is M s.t. $a_m = 0$ if $m \geq M$. Hence $x = (a_2, a_3, \dots, a_{M-1}, 0, 0, \dots)$.

Notice that, since $a_m \in \mathbb{Z}_m$, $m a_m = 0$. And so

$$(M-1)!\, x = ((M-1)!\, a_2, (M-1)!\, a_3, \dots, (M-1)!\, a_{M-1}, 0, 0, \dots)$$
$$= (0, 0, \dots).$$ Therefore $\mathrm{ord}(x) < \infty$.

Let $e_n = (0, 0, \dots, 0, 1_{\mathbb{Z}_n}, 0, \dots)$. Then $\mathrm{ord}(e_n) = n$. Thus

$$\operatorname*{lcm}_{x \in \bigoplus_{n=2}^{\infty} \mathbb{Z}_n} \mathrm{ord}(x) \geq \operatorname*{lcm}_{n \geq 2} \mathrm{ord}(e_n) = \operatorname*{lcm}_{n \geq 2} n = \infty;$$ and so

$$\mathrm{char}(\bigoplus_{n=2}^{\infty} \mathbb{Z}_n) = 0. \blacksquare$$

Remark. $\mathrm{Char}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}) = \mathrm{l.c.m.}(n_1, n_2, \dots, n_k)$.

Lecture 04: Integral domains and fields

Monday, April 9, 2018 11:18 AM

Def. . A unital commutative ring is called an integral domain if it does not have a zero-divisor. (and $1 \neq 0$).

. A unital commutative ring is called a field if any non-zero element has an inverse. (and $1 \neq 0$).

Proposition. Suppose A is a non-zero unital commutative ring. Then A is an integral domain if and only if it has cancellation property; that means $ab = ac$ and $a \neq 0 \Rightarrow b = c$.

Pf. $(\Rightarrow)$ $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$

as $a \neq 0$, either $b - c = 0$ or $b-c$ is a zero-divisor.

Since A does not have a zero-divisor, $b = c$.

We will continue next time.

. We also went over the proof of the following result from 103A:

$nx = 0 \Leftrightarrow \operatorname{ord}(x) \mid n$. $\boxed{\text{Pf}}$ Suppose r is the remainder of n divided by $\operatorname{ord}(x)$. Then $n = q \operatorname{ord}(x) + r$. And so $0 = nx = q \operatorname{ord}(x)\, x + rx = rx$. Since $0 \leq r < \operatorname{ord}(x)$, we deduce $r = 0$.