Lecture 03: Homomorphisms between Zn and Zm

Tuesday, January 15, 2019 11:40 AM

In the previous lecture we were proving

Theorem. Suppose $m, n \in \mathbb{Z}^+$, $m|n$. Let $c_{n,m}: \mathbb{Z}_n \to \mathbb{Z}_m$,

$c_{n,m}(a) :=$ the remainder of a divided by m. Then

$c_{n,m}(c_n(b)) = c_m(b)$ for any $b \in \mathbb{Z}$; alternatively we say

the following diagram commutes

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, "c_n"'] \arrow[dr, "c_m"] \arrow[d, phantom, "\circlearrowright"] & \\ \mathbb{Z}_n \arrow[rr, "c_{n,m}"'] & & \mathbb{Z}_m \end{tikzcd}.$$

And $c_{n,m}$ is a ring homomorphism.

Pf. (Cont.) We have already proved that the above diagram commutes. Next we show why $c_{n,m}$ is a ring homomorphism

$$c_{n,m}(\underbrace{a+a'}_{\text{in } \mathbb{Z}_n}) = c_{n,m}(c_n(\overbrace{a+a'}^{\text{in } \mathbb{Z}})) = c_m(\overbrace{a+a'}^{\text{in } \mathbb{Z}}) \quad \text{(because of the above diagram)}$$

$$= \underbrace{c_m(a) + c_m(a')}_{\text{in } \mathbb{Z}_m} \quad (c_m \text{ is a ring hom.})$$

$$= \underbrace{c_{n,m}(a) + c_{n,m}(a')}_{\text{in } \mathbb{Z}_m}$$

Notice that $c_{n,m}\big|_{\mathbb{Z}_n} = c_m$ and that is why the last equality holds.

Similarly $c_{n,m}(\underbrace{a \cdot a'}_{\text{in } \mathbb{Z}_n}) = c_{n,m}(c_n(\underbrace{a \cdot a'}_{\text{in } \mathbb{Z}})) = c_m(\underbrace{a \cdot a'}_{\text{in } \mathbb{Z}})$

$$= c_m(a) \cdot c_m(a') \quad (c_m \text{ is a ring hom})$$

$$= c_{n,m}(a) \cdot c_{n,m}(a'). \quad \blacksquare$$

Lecture 03: Chinese remainder theorem

Tuesday, January 15, 2019 11:51 AM

Notice that $c_{n,m} = c_m|_{\mathbb{Z}_n}$ is true for any pair (n,m) of positive integers, c_m is always a ring hom; but $c_{n,m}$ is a ring hom exactly when $m|n$. The main reason is that $\mathbb{Z}_n$ is NOT a subring of $\mathbb{Z}$; and so c_m being a ring hom does not tell us much about $c_{n,m}$.

<u>Theorem</u> (Chinese Remainder Theorem)

Suppose $n, m \in \mathbb{Z}^+$ and $\gcd(n,m) = 1$. Then

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n .$$

<u>Pf.</u> Let $f : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f(a) := (c_{mn,m}(a), c_{mn,n}(a))$

Since $m | mn$ and $n | mn$, $c_{mn,m}$ and $c_{mn,n}$ are ring hom.

So
$$\begin{aligned}
f(a+a') &= (c_{mn,m}(a+a'), c_{mn,n}(a+a')) \\
&= (c_{mn,m}(a) + c_{mn,m}(a'),\ c_{mn,n}(a) + c_{mn,n}(a')) \\
&= (c_{mn,m}(a), c_{mn,n}(a)) + (c_{mn,n}(a), c_{mn,n}(a')) \\
&= f(a) + f(a');
\end{aligned}$$

Similarly one can check that $f(aa') = f(a)f(a')$.

Lecture 03: Proof of CRT

Tuesday, January 15, 2019 12:03 PM

So f is a ring homomorphism.

<u>Injectivity</u>. From group theory we know that a group homomorphism is injective if and only if $\ker f = 0$;

<u>Proposition from group theory</u> Suppose $\phi: G_1 \to G_2$ is a group homomorphism, and G_1 and G_2 are two (abelian) groups.

Then ϕ is injective $\Leftrightarrow$ $\ker \phi := \{g_1 \in G_1 \mid \phi(g_1) = 0\}$
$= \{0\}$.

<u>Pf of Prop</u>. $(\Rightarrow)$ $g_1 \in \ker \phi \Rightarrow \phi(g_1) = 0 = \phi(0)$
$\Rightarrow g_1 = 0$ as ϕ is injective.

$(\Leftarrow)$ $\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_1) - \phi(g_2) = 0 \Rightarrow \phi(g_1 - g_2) = 0$
$\Rightarrow g_1 - g_2 \in \ker \phi = \{0\} \Rightarrow g_1 - g_2 = 0 \Rightarrow g_1 = g_2$. ∎

$a \in \ker f \Leftrightarrow f(a) = (0, 0)$

$\Leftrightarrow c_{mn,m}(a) = 0$ and $c_{mn,n}(a) = 0$

$\Leftrightarrow m \mid a$ and $n \mid a$

$\gcd(m,n) = 1$

$\Leftrightarrow mn \mid a \Leftrightarrow a = 0$.

(see next page) $0 \le a < mn$

Lecture 03: Proof of CRT

Thursday, January 17, 2019 2:35 PM

<u>Recall</u>. For any two integers m, n, $\exists\, r, s \in \mathbb{Z}$, $\gcd(m,n) = mr + ns$

In particular, $\gcd(m,n) = 1$ implies $\exists\, r, s \in \mathbb{Z}$, $mr + ns = 1$. $(*)$

Suppose $m \mid a$ and $n \mid a$. Then

$$\left.\begin{array}{l} m \mid a \Rightarrow mn \mid an \\ n \mid a \Rightarrow mn \mid am \end{array}\right\} \Rightarrow mn \mid amr + ans$$

and so by $(*)$ $mn \mid a$.

This is what we have used.

<u>Surjectivity</u> Since f is injective and $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$,

by pigeonhole principle f is surjective. $\blacksquare$

<u>Proposition</u>. $\mathbb{Z}_n^\times = \{ a \in \mathbb{Z} \mid 0 \le a < n,\ \gcd(a,n) = 1 \}$.

<u>Pf</u>. Suppose $a \in \mathbb{Z}_n^\times$. Then $\exists\, a' \in \mathbb{Z}_n$, $a \cdot a' = 1$ in $\mathbb{Z}_n$; and

so $a a' \equiv 1 \pmod n$, which implies $\exists\, b \in \mathbb{Z}$ s.t.

$aa' - 1 = nb$. Suppose $d = \gcd(a,n)$. Then

$d \mid aa' - nb$ which implies $d \mid 1$; and so $\gcd(a,n) = 1$.

If $\gcd(a,n) = 1$, then $\exists\, r, s \in \mathbb{Z}$, $ra + sn = 1$; and

so $ra \equiv 1 \pmod n$. Let a' be the remainder of r

Lecture 03: Euler's phi function

Friday, January 18, 2019 2:18 AM

$a'a = 1$ in $\mathbb{Z}_n$; and so $a \in \mathbb{Z}_n^\times$. ∎

<u>Corollary</u>. Suppose p is prime. Then $\mathbb{Z}_p$ is a field.

<u>Pf.</u> $\mathbb{Z}_p$ is a unital commutative ring and $0 \neq 1$. So it is enough to show $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$. By the previous theorem

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid \gcd(a,p) = 1\} \underset{\boxed{p \text{ is prime}}}{=} \{a \in \mathbb{Z}_p \mid 0 < a < p\}$$

$$= \mathbb{Z}_p \setminus \{0\}.$$ ∎

<u>Def.</u> (Euler's phi function) $\forall n \in \mathbb{Z}^+$, $\phi(n) := |\mathbb{Z}_n^\times|$;

alternatively $\phi(n) := |\{a \in \mathbb{Z} \mid 0 < a \leq n, \gcd(a,n) = 1\}|$.

<u>Ex.</u> Suppose p is prime; then $\phi(p) = p - 1$.

<u>Ex.</u> Suppose p is prime and $k \in \mathbb{Z}^+$; then $\gcd(a, p^k) = 1$ exactly when $p \nmid a$. Therefore

$$\phi(p^k) = p^k - \underbrace{|\{a \in [1, p^k] \mid p \mid a\}|}_{\parallel}$$

$$|\{p, 2p, 3p, \dots, p^k\}| = p^k / p = p^{k-1}$$

$$\Rightarrow \phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

<u>Theorem</u>. Suppose $m, n \in \mathbb{Z}^+$, $\gcd(m,n) = 1$; then $\phi(mn) = \phi(m)\phi(n)$.

Lecture 03: Euler's phi function; characteristic

Friday, January 18, 2019 2:30 AM

Pf. By CRT, $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$; and so

$$|\mathbb{Z}_{mn}^{\times}| = |(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times}| \underset{\uparrow}{=} |\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}|,$$ which implies

$\boxed{\text{HW assignment}}$

$$\phi(mn) = \phi(m)\,\phi(n). \quad \blacksquare$$

Def. Suppose A is a ring. Let $C_A := \{n \in \mathbb{Z}^+ \mid \forall a \in A, na = 0\}$.

If $C_A = \emptyset$, we say characteristic of A is zero and write

$\mathrm{char}(A) = 0$. If $C_A \neq \emptyset$, we say

$$\mathrm{char}(A) = \min C_A.$$

. So in either case we have $\mathrm{char}(A)\, a = 0 \quad \forall a \in A$.

Recall. Order of an element g in an abelian group G is the smallest positive integer d such that $dg = 0$. If there is no such positive integer, we say g is of infinite order. We denote order of g by $o(g)$. Here is the main property of order of an element:

$$ng = 0 \iff o(g) \mid n.$$

Pf. ($\Leftarrow$) $o(g) \mid n \Rightarrow n = k\, o(g) \Rightarrow ng = (k\, o(g))\, g = k\,(o(g)\, g)$
$= k \cdot 0 = 0.$

Lecture 03: Characteristic

Friday, January 18, 2019 8:36 AM

($\Rightarrow$) Let r be the remainder of n divided by $o(g)$. Then

$n = q \cdot o(g) + r$ for some $q \in \mathbb{Z}$ and $0 \le r < o(g)$.

So $ng = (q\, o(g) + r)\, g = (q\, o(g))\, g + rg = q\,(o(g)\, g) + rg = rg$

$\Rightarrow rg = 0$; since $o(g)$ is the smallest positive integer s.t. $o(g)\, g = 0$, $r < o(g)$, and $rg = 0$, we deduce that r is not positive. As $0 \le r$, we deduce that $r = 0$, which means $o(g) \mid n$.

<u>Proposition</u>. Suppose char $A \neq 0$. Then

$$\operatorname{Char} A = \underset{a \in A}{\text{l.c.m.}}\ o(a).$$

<u>Pf.</u> Let $n := \operatorname{char} A$. Then, for any $a \in A$, $na = 0$. By the above discussed property of groups, $o(a) \mid n$. Hence n is a common multiple of $o(a)$'s for $a \in A$. Therefore

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

In particular, $m := \underset{a \in A}{\text{l.c.m}}\ o(a) < \infty$. For any $a \in A$, $o(a) \mid m$;

and so again by the above discussed property of groups, $ma=0$ for any $a\in A$. Thus $m\in \mathcal{C}_A$, which implies

$$\text{char } A = \min \mathcal{C}_A \leq m. \quad \text{(II)}$$

(I) and (II) imply $\text{char } A = \underset{a\in A}{\text{l.c.m}}\ o(a)$. ∎