Lecture 03: Homomorphisms between $\mathbb{Z}_n$ and $\mathbb{Z}_m$

Tuesday, January 15, 2019 11:40 AM

In the previous lecture we were proving

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

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

$$\sigma_{n,m}(\sigma_{n,m}(b)) = \sigma_{m}(b) \text{ for any } b \in \mathbb{Z}; \text{ alternatively we say the following diagram commutes}$$

$$\begin{array}{c}
\mathbb{Z} \\
\sigma_{n,m}
\end{array} \quad \begin{array}{c}
\sigma_{m}
\end{array}
$$

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

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

$$\begin{array}{c}
\mathbb{Z}_n \\
\sigma_{n,m}
\end{array} \quad \begin{array}{c}
\sigma_{n,m}
\end{array}
$$

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

Similarly

$$\begin{array}{c}
\mathbb{Z}_n \\
\sigma_{n,m}
\end{array} \quad \begin{array}{c}
\sigma_{n,m}
\end{array}
$$

$$= \sigma_{m}(a) \cdot \sigma_{m}(a') \text{ (Cm is a ring hom)}$$

$$= \sigma_{n,m}(a) \cdot \sigma_{n,m}(a'). \quad \blacksquare$$
Notice that \( c_{n,m} = c_m \mid Z_n \) 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 \( m \mid n \). The main reason is that \( Z_n \) is NOT a subring of \( Z \); and so \( c_m \) being a ring hom does not tell us much about \( c_{n,m} \).

**Theorem** (Chinese Remainder Theorem)

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

\[
\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.
\]

**Pf.** Let \( f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, f(a) := (c_{mn,m}(a), c_{mn,n}(a)) \)

Since \( m \mid mn \) and \( n \mid mn \), \( c_{mn,m} \) and \( c_{mn,n} \) are ring hom.

So \( f(a+a') = (c_{mn,m}(a+a'), c_{mn,n}(a+a')) \)

\[
= (c_{mn,m}(a) + c_{mn,m}(a'), c_{mn,n}(a) + c_{mn,n}(a'))
\]

\[
= (c_{mn,m}(a), c_{mn,n}(a)) + (c_{mn,n}(a), c_{mn,n}(a))
\]

\[
= f(a) + f(a');
\]

Similarly one can check that \( f(aa') = f(a) f(a') \).
So $f$ is a ring homomorphism.

**Injectivity.** From group theory we know that a group homomorphism is injective if and only if $\ker f = \{0\}$.

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

Then $\phi$ is injective $\iff \ker \phi = \{0\}$.

**Proof of Prop.** ($\implies$) $g \in \ker \phi \Rightarrow \phi(g) = 0 = \phi(e)$

$\implies g = e$ as $\phi$ is injective.

($\impliedby$) $\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_1 - g_2) = 0 \Rightarrow \phi(g_1 - g_2) = 0$

$\Rightarrow g_1 - g_2 \in \ker \phi = \{0\}$

$\Rightarrow g_1 - g_2 = 0 \Rightarrow g_1 = g_2$. 

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

$\iff C_{mn, m}(a) = 0$ and $C_{mn, n}(a) = 0$

$\iff m \mid a$ and $n \mid a$

$\iff \gcd(m, n) = 1$

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

*(See next page)*
Recall. 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

\[
\begin{align*}
\frac{a}{m} & = \frac{a}{mn} \quad \text{implies} \quad \frac{a}{mn} \mid amr + ans, \\
\frac{a}{n} & = \frac{a}{mn} \quad \text{implies} \quad \frac{a}{mn} \mid am, \quad \text{and so by} \quad \frac{a}{mn} \mid a.
\end{align*}
\]

This is the cohort we have used.

**Surjectivity** Since \( f \) is injective and \( |\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| \), by pigeonhole principle \( f \) is surjective.

**Proposition.** \( \mathbb{Z}_n^x = \{ a \in \mathbb{Z} \mid 0 \leq a < n, \gcd(a, n) = 1 \} \).

**Pf.** Suppose \( a \in \mathbb{Z}_n^x \). Then \( \exists a' \in \mathbb{Z}_n \), \( a.a' = 1 \) in \( \mathbb{Z}_n \); and so \( a.a' = 1 \pmod{n} \), 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 \( ra = 1 \pmod{n} \). Let \( a' \) be the remainder of \( r \).
Lecture 03: Euler's phi function

Friday, January 18, 2019  2:18 AM

\[ a' a = 1 \text{ in } \mathbb{Z}_n; \text{ and so } a \in \mathbb{Z}_n^\times. \square \]

**Corollary.** Suppose \( p \) is prime. Then \( \mathbb{Z}_p \) is a field.

**Proof.** \( \mathbb{Z}_p \) 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

\[ \mathbb{Z}_p^\times = \{ a \in \mathbb{Z}_p \mid \gcd(a, p) = 1 \} = \{ a \in \mathbb{Z}_p \mid \alpha < a < p \} \]

\[ = \mathbb{Z}_p \setminus \{0\}. \]

\( \square \)

**Def. (Euler's phi function)** \( \forall n \in \mathbb{Z}^+, \phi(m) := |\mathbb{Z}_n^\times|; \)

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

**Ex.** Suppose \( p \) is prime; then \( \phi(p) = p - 1. \)

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

\[ \phi(p^k) = p^k - |\{ a \in [1, p^k] \mid p \nmid a \}| \]

\[ = p^k - (1, p, 2p, \ldots, p^{k-1}) = p^k / p = p^{k-1}(p-1). \]

**Theorem.** Suppose \( m, n \in \mathbb{Z}^+, \gcd(m, n) = 1; \) then \( \phi(mn) = \phi(m) \phi(n). \)
pf. By CRT, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$; and so

$$|\mathbb{Z}_{mn}^x| = |(\mathbb{Z}_m \times \mathbb{Z}_n)^x| = |\mathbb{Z}_m^x \times \mathbb{Z}_n^x|,$$

which implies

$$\phi(mn) = \phi(m) \phi(n).$$

Def. Suppose $A$ is a ring. Let $C_A := \{n \in \mathbb{Z}^+ | \forall a \in A, na = 0\}$. If $C_A = \emptyset$, we say characteristic of $A$ is zero and write $\text{char}(A) = 0$. If $C_A \neq \emptyset$, we say $\text{char}(A) = \min C_A$.

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

Recall. Order of an element $g$ in an abelian group $G$ is the smallest positive integer $d$ such that $d g = 0$. 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:

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

pf. $(\Rightarrow)$ $o(g) | n \Rightarrow n = k o(g) \Rightarrow ng = (k o(g)) g = k (o(g) g) = k \cdot 0 = 0$. 


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

\[
n = q \cdot o(g) + r \quad \text{for some } q \in \mathbb{Z} \text{ and } 0 \leq r < o(g).
\]

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

\[ \Rightarrow rg = 0; \quad \text{since } o(g) \text{ is the smallest positive integer s.t.}
\]

\( o(g) g = o, \quad r < o(g), \text{ and } rg = 0, \) we deduce that \( r \) is

not positive. As \( 0 \leq r \), we deduce that \( r = 0 \), which means

\( o(g) | n \).

\[ \text{Proposition. Suppose } \text{char } A \neq 0. \text{ Then} \]

\[ \text{Char } A = \text{l.c.m. } o(a). \]

\[ a \in A \]

\[ \text{Pf. Let } n := \text{char } A. \text{ Then, for any } a \in A, \text{ } na = 0. \text{ By the} \]

above discussed property of groups, \( o(a) | n \). Hence \( n \) is

a common multiple of \( o(a) \)'s for \( a \in A \). Therefore

\[ \text{l.c.m. } o(a) \leq n. \quad (I) \]

\[ \text{a} \in A \]

In particular, \( m := \text{l.c.m. } o(a) < \infty. \text{ For any } a \in A, o(a) | m; \)
and so again by the above discussed property of groups, \( ma = 0 \)
for any \( a \in A \). Thus \( m e C_A \), which implies

\[
\text{char } A = \min C_A \leq m. \quad (\text{II})
\]

(I) and (II) imply \( \text{char } A = \text{l.c.m. } 0(a). \)