Lecture 3 Monday Jan 25

7.6 The Chinese Remainder Theorem

DEF 1 Given rings R, S (possibly non com)

$\exists$ ring denoted

$R \times S$ "direct product"

whose elements are the ordered pairs

(r, s) $r \in R,$ $s \in S$

Addition is

$(r, s) + (r', s') = (r+r', s+s')$

The zero is $(0, 0)$

Multiplication is

$(r, s) \times (r', s') = (rr', ss')$

If each of R, S has mult identity 1, then

$R \times S$ has mult identity $(1, 1)$.

Given a ring R

Given a 2-sided ideal I of R

Recall the quotient ring

$$R/I = \text{set of cosets of } I \text{ in } R$$

the map

$$\begin{aligned} R &\longrightarrow R/I \qquad \text{"quotient map"} \\ r &\longrightarrow r+I \qquad \text{"canonical map"} \end{aligned}$$

is a surjective ring homomorphism with kernel I.

Recall the ring of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

Given $n \in \mathbb{Z}$ with $n>0$, consider the ideal

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$$

The ring $\mathbb{Z}/n\mathbb{Z}$ has n elements

$$r + n\mathbb{Z} \qquad 0 \le r \le n-1$$

Abbreviate

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

For notational convenience view

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

with addition, mult performed modulo n.

Given integers $n, m > 1$

Assume n, m have no prime factor in common
"relatively prime"

We will give a ring isomorphism

$$\mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

We start with an example

$$\mathbb{Z}_{15} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$$

We consider this example in detail.

Since 3 divides 15,

$\exists$ ring homomorphism

$$\varphi : \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_3$$

that sends

$$x + 15\mathbb{Z} \longrightarrow x + 3\mathbb{Z} \qquad \forall x \in \mathbb{Z}$$

φ is surjective with kernel $3\mathbb{Z}_{15}$

Similarly, since 5 divides 15

$\exists$ ring homomorphism

$$\phi : \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_5$$

that sends

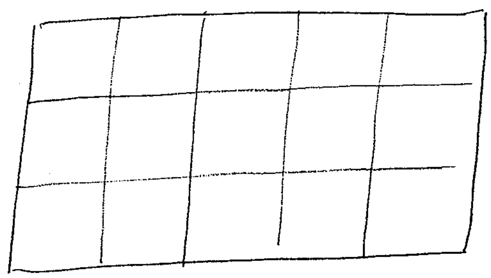
$$x + 15\mathbb{Z} \longrightarrow x + 5\mathbb{Z} \qquad \forall x \in \mathbb{Z}$$

φ is surjective with kernel $5\mathbb{Z}_{15}$

1/25/16
5

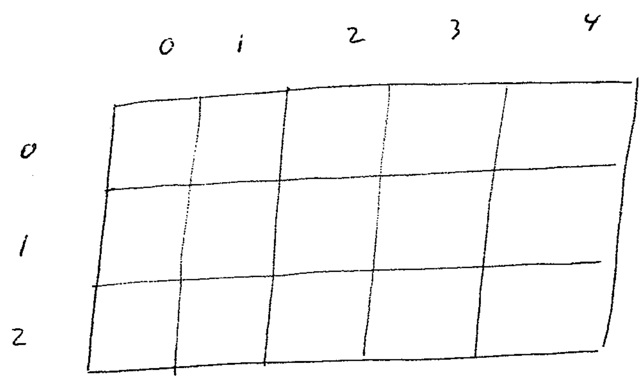
x	$\varphi(x)$	$\phi(x)$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Consider 3×5 "chessboard"



Label rows by $\mathbb{Z}_3$

Label cols by $\mathbb{Z}_5$



View the locations on chess bd as the

elements of $\mathbb{Z}_3 \times \mathbb{Z}_5$

Starting at top-left square, label the squares with $\mathbb{Z}_{15}$ going South-East with "wrap around"

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

For $0 \le x \le 14$,

x is in row a, col b where

$$x \equiv a \quad (3)$$
$$x \equiv b \quad (5)$$

In other words

x is in location $(\varphi(x), \phi(x))$

Each location in the chessbd gets a unique element in $\mathbb{Z}_{15}$.

So the map

$$\varphi \times \phi : \quad \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$x \longrightarrow (\varphi(x), \ \phi(x))$$

is a bijection.

The map $\varphi \times \phi$ is a ring homomorphism, since each of φ, ϕ is a ring homomorphism.

So $\varphi \times \phi$ is a ring isomorphism.

We now give more detail about $\varphi \times \phi$.

the inverse of $\varphi \times \phi$

Define $e, f \in \mathbb{Z}_{15}$ as follows:

$$e = \text{preimage of } (1,0) \text{ under } \varphi \times \phi$$

$$f = \text{preimage of } (0,1) \text{ under } \varphi \times \phi$$

From chessbd,

$$e = 10 + 15\mathbb{Z} \qquad f = 6 + 15\mathbb{Z}$$

By construction

$$\varphi(e) = 1, \qquad \phi(e) = 0$$

$$\varphi(f) = 0, \qquad \phi(f) = 1$$

In $\mathbb{Z}_{15}$,

$$e^2 = e, \qquad f^2 = f$$

"orthogonal idempotents"

$$ef = fe = 0, \qquad e + f = 1$$

Consider the inverse

$$(\varphi \times \phi)^{-1} : \quad \mathbb{Z}_3 \times \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{15}$$

$(\varphi \times \phi)^{-1}$ sends

$(1, 0) \longrightarrow e$
$\shortparallel$
$1+3\mathbb{Z}$

$(0, 1) \longrightarrow f$
$\shortparallel$
$1+5\mathbb{Z}$

So for $a, b \in \mathbb{Z}$, $(\varphi \times \phi)^{-1}$ sends

$$(a+3\mathbb{Z},\ b+5\mathbb{Z}) \longrightarrow ae+bf = 10a+6b+15\mathbb{Z}$$

Some ideals in $\mathbb{Z}_{15}$

Define

$I_1 =$ elements in Col 0 of chessbd

$= \{0, 10, 5\}$

$= \{$ multiples of 5 in $\mathbb{Z}_{15}\}$

$=$ ideal of $\mathbb{Z}_{15}$ gen by 5

$= 5\,\mathbb{Z}_{15}$

$=$ ker of ϕ

Obs

$$I_1 = \{0, \underset{e}{\underset{\shortparallel}{10}}, \underset{2e}{\underset{\shortparallel}{5}}\}$$

$= \{$ multiples of e in $\mathbb{Z}_{15}\}$

$= e\,\mathbb{Z}_{15}$

Define

I_2 = elements in row 0 of chessbd

$= \{ 0, 6, 12, 3, 9 \}$

$= \{$multiples of 3 in $\mathbb{Z}_{15}\}$

= ideal of $\mathbb{Z}_{15}$ gen by 3

$= 3\,\mathbb{Z}_{15}$

= ker of φ

Obs

$$I_2 = \{ 0, \underset{f}{\overset{\shortparallel}{6}}, \underset{2f}{\overset{\shortparallel}{12}}, \underset{3f}{\overset{\shortparallel}{3}}, \underset{4f}{\overset{\shortparallel}{9}} \}$$

$= \{$ multiples of f in $\mathbb{Z}_{15} \}$

$= f\,\mathbb{Z}_{15}$

Obs
$$I_1 \cap I_2 = 0$$

Show
$$I_1 + I_2 = \mathbb{Z}_{15}$$

Labeled chess bd is the addition table for I_1, I_2 in $\mathbb{Z}_{15}$:

+	0	6	12	3	9
0	0	6	12	3	9
10	10	1	7	13	4
5	5	11	2	8	14

For instance
$$10 + 12 \equiv 7 \quad (15)$$

So
$$I_1 + I_2 = \mathbb{Z}_{15}$$

I_1 is a subring of $\mathbb{Z}_{15}$ with identity e

I_2 is a subring of $\mathbb{Z}_{15}$ with identity f

The restriction of φ to I_1 gives a ring iso

$I_1 \longrightarrow \mathbb{Z}_3$ such that

x	0	10	5
$\varphi(x)$	0	1	2

The restriction of ϕ to I_2 gives a ring iso

$I_2 \longrightarrow \mathbb{Z}_5$ such that

x	0	6	12	3	9
$\phi(x)$	0	1	2	3	4

By construction we have ring iso

$$I_1 \times I_2 \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$(a, b) \longrightarrow (\varphi(a), \phi(b))$$

This iso sends

$$(e, 0) \longrightarrow (1, 0)$$

$$(0, f) \longrightarrow (0, 1)$$

Since $I_1 \cap I_2 = 0$ and $I_1 + I_2 = \mathbb{Z}_{15}$

we have ring iso

$$\sigma : \begin{array}{ccc} I_1 \times I_2 & \longrightarrow & \mathbb{Z}_{15} \\ (a, b) & \longrightarrow & a + b \end{array}$$

σ sends

$$(e, 0) \longrightarrow e$$

$$(f, 0) \longrightarrow f$$

$$(e, f) \longrightarrow 1$$

Thm 2 The following diagram commutes:

$$\begin{tikzcd}
 & \mathbb{Z}_{15} \arrow[dr, "\varphi \times \phi"] & \\
I_1 \times I_2 \arrow[ur, "\sigma"] \arrow[rr] & & \mathbb{Z}_3 \times \mathbb{Z}_5
\end{tikzcd}$$

$$(a,b) \longrightarrow (\varphi(a), \phi(b))$$

pf For $(a,b) \in I_1 \times I_2$ chase it around diagram.

$$\begin{tikzcd}
 & a+b \arrow[dr] & \\
(a,b) \arrow[ur] \arrow[r] & & (\varphi(a+b), \phi(a+b))
\end{tikzcd}$$

$$(\varphi(a+b), \phi(a+b)) \overset{?}{=} (\varphi(a), \phi(b))$$

$$\varphi(a+b) \overset{?}{=} \varphi(a)$$
$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(b) = 0 \quad \text{since } b \in I_2 = \ker \varphi$$

$$\phi(a+b) \overset{?}{=} \phi(b)$$
$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(a) = 0 \quad \text{since } a \in I_1 = \ker \phi$$

$\square$