Lecture 4 Wednesday Jan 27

[Chinese Remainder thm, cont]

We found a ring iso

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

More generally, for rel prime integers $n, m > 1$,

we will give a ring iso

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

More generally still, let

R = any commutative ring with $1 \neq 0$

(for rest of lecture)

Let A, B denote ideals of R such that

$$A + B = R \qquad \text{"comaximal"}$$

We will give a ring iso

$$R/AB \longrightarrow R/A \times R/B$$

Recall

$$AB = \left\{ a_1 b_1 + a_2 b_2 + \cdots + a_r b_r \;\middle|\; 0 \le r < \infty \quad a_i \in A \quad b_i \in B \ (1 \le i \le r) \right\}$$

LEM 3 Given comaximal ideals A, B of R. Then

$$AB = A \cap B$$

pf $\subseteq$: Since A, B are ideals of R

$\supseteq$: Write

$$1 = a + b \qquad a \in A \qquad b \in B$$

Given $r \in A \cap B$ show $r \in AB$:

$$\begin{aligned} r &= r1 \\ &= r(a+b) \\ &= \underbrace{\overset{\overset{B}{\Psi}}{r}\,a}_{\overset{\Uparrow}{AB}} + \underbrace{\overset{\overset{A}{\Psi}}{r}\,b}_{\overset{\Uparrow}{AB}} \end{aligned}$$

$\in AB$

$\square$

Given ideals A, B of R

Recall quotient maps

$$\varphi: \begin{array}{ccc} R & \longrightarrow & R/A \\ r & \longrightarrow & r+A \end{array} \qquad \text{surj with ker } A$$

$$\phi: \begin{array}{ccc} R & \longrightarrow & R/B \\ r & \longrightarrow & r+B \end{array} \qquad \text{surj with ker } B$$

φ, ϕ are ring homomorphisms

<u>Observe</u> the map

$$\varphi \times \phi: \begin{array}{ccc} R & \longrightarrow & R/A \times R/B \\ r & \longrightarrow & (\varphi(r), \phi(r)) \end{array}$$

is a ring hom with kernel $A \cap B$

LEM 4 For A, B, φ, ϕ above TFAE:

(i) $A + B = R$,

(ii) $\varphi \times \phi$ is surjective.

pf (i) $\to$ (ii) Given

$x \in R/A$, $y \in R/B$

Display $r \in R$ such that

$\varphi(r) = x$, $\phi(r) = y$

- Show $\exists\, a \in A$ st $\phi(a) = y$:

$\exists\, r_1 \in R$ st $\phi(r_1$

$\exists\, a \in A$ st $r_1 - a \in B$

$$\phi(a) = \phi(r_1 + \underset{\in B}{a - r_1}) = \underset{\substack{\| \\ y}}{\phi(r_1)} + \underbrace{\phi(a - r_1)}_{\substack{\| \\ 0}}$$

$= y$ ✓

- Show $\exists\, b \in B$ st $\varphi(b) = x$: ✓

Similar arg

Define

$$r = a + b$$

Observe

$$\begin{aligned} \varphi(r) &= \varphi(a+b) \\ &= \underset{\substack{\parallel \\ 0}}{\varphi(a)} + \underset{\substack{\parallel \\ x}}{\varphi(b)} \\ &= x \end{aligned}$$

$$\begin{aligned} \phi(r) &= \phi(a+b) \\ &= \underset{\substack{\parallel \\ y}}{\phi(a)} + \underset{\substack{\parallel \\ 0}}{\phi(b)} \\ &= y \end{aligned}$$

(ii) $\rightarrow$ (i) Given $r \in R$

Display $a \in A$ and $b \in B$ s.t. $a+b=r$

Consider

$$(\varphi(r), \phi(r)) \in R/A \times R/B$$

$$\|$$

$$(\varphi(r), 0) + (0, \varphi(r))$$

Since $\varphi \times \phi$ is surj $\exists\, a \in R$ s.t

$\varphi \times \phi$ sends

$$a \longrightarrow (0, \phi(r))$$

So $\varphi(a) = 0$, $\phi(a) = \phi(r)$

$a \in A$

Define $b = r - a$ so $a+b=r$

We have

$$\begin{aligned}\phi(b) &= \phi(r-a)\\ &= \phi(r) - \phi(a)\\ &= 0\end{aligned}$$

So $b \in B$ $\square$

Thm 5 (CH REM) Given commutative ring R with $1 \neq 0$. Given comaximal ideals A, B of R.

Then $\exists$ ring isomorphism

$$\begin{aligned} R/AB &\longrightarrow R/A \times R/B \\ r + AB &\longrightarrow (r+A,\ r+B) \end{aligned}$$

pf Consider ring hom

$$\varphi \times \phi : \begin{aligned} R &\longrightarrow R/A \times R/B \\ r &\longrightarrow (\varphi(r),\ \phi(r)) \end{aligned}$$

By LEM 3,
$\varphi \times \phi$ has kernel $A \cap B = AB$

By LEM 4,
$\varphi \times \phi$ is surjective.

So $\varphi \times \phi$ induces a ring iso

$$\begin{aligned} R/AB &\longrightarrow R/A \times R/B \\ r + AB &\longrightarrow (\varphi(r),\ \phi(r)) \end{aligned}$$

Result follows. $\square$

COR 6 Given relatively prime integers $n, m > 1$

$\exists$ ring isomorphism

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$r + nm\mathbb{Z} \longrightarrow (r + n\mathbb{Z},\ r + m\mathbb{Z})$$

pf Apply thm 5 with

$R = \mathbb{Z}$ $\qquad A = n\mathbb{Z}$ $\qquad B = m\mathbb{Z}$

Check $A + B = R$:

Since n, m rel prime, $\exists$ $r, s \in \mathbb{Z}$ st

$$rn + sm = 1$$

So $\underbrace{1 = \underset{A}{\underset{\cap}{rn}} + \underset{B}{\underset{\cap}{sm}}} \in A + B$

Now $R = R1 \subseteq A + B$

So $R = A + B$

$\square$

Extensions

LEM 7 Given ideals A, B, C of R such that

$$A + C = R, \qquad B + C = R$$

Then

$$AB + C = R.$$

pf $\exists$ $a \in A$ and $c \in C$ st

$$a + c = 1$$

$\exists$ $b \in B$ and $c' \in C$ st

$$b + c' = 1$$

So

$$1 = (a+c)(b+c')$$

$$= \underset{\substack{\cap \\ AB}}{ab} + \underset{\substack{\cap \\ C}}{\underbrace{cb + ac' + cc'}}$$

So

$$1 \in AB + C$$

Result follows. $\square$

COR 8 Given commutative ring R with $1 \neq 0$

Given integer $k \geq 1$

Given ideals $A_1, A_2, \ldots, A_k$ of R st

$$A_i + A_j = R \qquad (1 \leq i < j \leq k)$$

Then $\exists$ ring isomorphism

$$R/A_1A_2\cdots A_k \longrightarrow R/A_1 \times R/A_2 \times \cdots \times R/A_k$$

$$r + A_1A_2\cdots A_k \longrightarrow (r+A_1,\ r+A_2,\ \ldots,\ r+A_k)$$

pf Apply induction on k, using Thm 5 and LEM 7 $\square$

Notation

Given ring S with $1 \neq 0$ (not nec com)

Define $S^\times$ = set of units in S

We have

- $1 \in S^\times$
- $\forall a, b \in S^\times$, $ab \in S^\times$
- $\forall a \in S^\times$ $a^{-1} \in S^\times$

$S^\times$ becomes a group

<u>Note</u> Given rings S_1, S_2 with $1 \neq 0$

$$(S_1 \times S_2)^\times = S_1^\times \times S_2^\times$$

COR 9 Referring to COR 8,

we have a group isomorphism

$$\left(R / A_1 A_2 \cdots A_k \right)^{\times} \simeq \left(R/A_1 \right)^{\times} \times \left(R/A_2 \right)^{\times} \times \cdots \times \left(R/A_k \right)^{\times}$$

pf By Cor 8 and above note. $\square$

Given integer $N > 1$

Factor N:

$$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

$p_1, p_2, \ldots, p_k$ mutually distinct primes

$e_1, e_2, \ldots, e_k$ pos integers

COR 10 With above notation: $\exists$ ring iso

$$\mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$$

$$r + N\mathbb{Z} \longrightarrow \left(r + p_1^{e_1}\mathbb{Z},\ r + p_2^{e_2}\mathbb{Z},\ \ldots,\ r + p_k^{e_k}\mathbb{Z} \right)$$

pf Apply COR 8 with

$R = \mathbb{Z}$

$A_i = p_i^{e_i}\mathbb{Z} \qquad 1 \le i \le k$

$\square$

COR 11 Referring to COR 10, $\exists$ group iso

$$\left(\mathbb{Z}/N\mathbb{Z}\right)^{\times} \simeq \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^{\times} \times \left(\mathbb{Z}/p_2^{e_2}\mathbb{Z}\right)^{\times} \times \cdots \times \left(\mathbb{Z}/p_k^{e_k}\mathbb{Z}\right)^{\times}$$

pf By Cor 9, Cor 10 $\square$

Given integer $N \geq 1$

Recall Euler φ- function

$\varphi(N) =$ number of integers among $1, 2, \ldots, N$
that are rel prime to N

ex $N = 6$

$$1 \quad \cancel{2} \quad \cancel{3} \quad \cancel{4} \quad 5 \quad \cancel{6}$$

$$\varphi(6) = 2$$

Ex For a prime p:

$$\varphi(p) = p-1$$

$$\varphi(p^2) = p^2 - p$$

$$\varphi(p^3) = p^3 - p^2$$

$$\ldots$$

For $N \geq 1$,

$\varphi(N) =$ cardinality of the group of units for $\mathbb{Z}/N\mathbb{Z}$:

$$\varphi(N) = \left| \left(\mathbb{Z}/N\mathbb{Z} \right)^{\times} \right|$$

So, referring to COR 10, COR 11,

$$\varphi(N) = \varphi\left(p_1^{e_1}\right) \varphi\left(p_2^{e_2}\right) \cdots \varphi\left(p_k^{e_k}\right)$$

Consequently, for rel prime integers $n, m \geq 1$,

$$\varphi(nm) = \varphi(n)\, \varphi(m)$$