Lecture 11: Chinese remainder theorem

24 September 2020
12:36

Recall: $R_1, \dots, R_n$ comm rings with unity then $\underset{R}{\overset{\shortparallel}{R_1 \times \dots \times R_n}}$ with component wise addition & multiplication is also a comm ring with unity. $1_R = (1_{R_1}, \dots, 1_{R_n})$

⊛ Ideals in $R_1 \times \dots \times R_n$ are of the form $I_1 \times \dots \times I_n$ where I_j is an R_j ideal. (Note: this is not true for subgroups of a group or subspaces of a vector space)

⊛ Prime ideals in $R_1 \times R_2 \times \dots \times R_n$ ($= R$ say).

Example: In $\mathbb{Z} \times \mathbb{Z}$, give an example prime ideal. $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}$
$a, b \in \mathbb{Z} \times \mathbb{Z}$ $\quad ab \in \mathbb{Z} \times \{0\}$

$\{0\} \times \{0\} = \{(0,0)\}$ $\qquad \underline{(1,0) \cdot (0,1) = (0,0)}$

⊛ Let $P \subseteq R$ be a prime ideal then $P = I_1 \times I_2 \times \dots \times I_n$ s.t. $I_j = R_j$ for all but one subscript j_0 & I_{j_0} is prime ideal of R_{j_0} and conversely.

Pf: conversely is easy to see, since if $\underline{I} = R_1 \times \dots \times R_{j_0-1} \times P_{j_0} \times R_{j_0+1} \times \dots \times R_n$
the $R/I \cong R_{j_0}/P_{j_0}$ which is an integral domain. (P_{j_0} is prime)
Hence I is a prime ideal of R.

$$\begin{tikzcd} R \arrow[r, two heads, "p_{j_0}"] \arrow[rr, bend right, "\theta"'] & R_{j_0} \arrow[r, two heads, "q"] & R_{j_0}/P_{j_0} \end{tikzcd}$$

$\ker(p_{j_0}) = R_1 \times \dots \times R_{j_0-1} \times \{0\} \times R_{j_0+1} \times \dots \times R_n$; $\ker(\theta) = I$

$\ker(\theta) = p_{j_0}^{-1}(\ker(q)) = p_{j_0}^{-1}(P_{j_0}) = I$

($\Rightarrow$): i.e. $P \subseteq R$ prime then $P = I_1 \times \dots \times I_n$ $\quad I_j$ an R_j-ideal

$$R/P = \frac{R_1 \times R_2 \times \dots \times R_n}{I_1 \times I_2 \times \dots \times I_n} \cong R_1/I_1 \times R_2/I_2 \times \dots \times R_n/I_n$$

$r = (r_1, \dots, r_n) \in R$
$$(r + P) \longmapsto (r_1 + I_1, r_2 + I_2, \dots, r_n + I_n)$$

And $R_1/I_1 \times \dots \times R_n/I_n$ is not an integral domain if $\exists\, 1 \le i, j \le n$ $\; i \ne j$ s.t. $I_i \ne R_i$ & $I_j \ne R_j$

$\Big(\therefore \; \bar{e}_i = (0, 0, \dots, 0, \overset{\substack{i\text{th factor} \\ \downarrow}}{1}, 0, \dots, 0)$, $\bar{e}_j \in R_1/I_1 \times \dots \times R_n/I_n$
$\bar{e}_i \cdot \bar{e}_j = 0$ but $\bar{e}_i, \bar{e}_j \ne 0 \Big)$

Hence $I_j = R_j$ $\forall\, 1 \le j \le n$ except one (say j_0).

Then $R/P \cong R_{j_0}/I_{j_0}$ and this is an int dom iff I_{j_0} is a prime ideal of R_{j_0}. ∎

⊛ Note $R = R_1 \times \dots \times R_n$ then e_j have the property
$e_j^2 = e_j \qquad e_i e_j = 0$ if $i \ne j \qquad (1 - e_j) e_j = 0$

Idempotents: Let R be a ring an element $e \in R$ is called an idempotent if $e^2 = e$.

Eg: 0_R & 1_R are idempotents is every ring with unity.

(*) Let $e \in R$ be an idempotent then $1-e$ is also an idempotent and $R \cong eR \times (1-e)R$
(i.e. eR & $(1-e)R$ are rings & their product is isom to R)

$S \subseteq R$

$1_S = 1_R$

$eR \subseteq R$

$1_{eR} \neq 1_R$

Pf: $(1-e)^2 = 1-e-e+e^2$
$= 1-e \quad (\because e^2 = e)$

So $1-e$ is an idempotent.

Claim: eR is comm ring with unity

eR is an ideal in R & hence closed under addition and multiplication satisfying all the ring axioms

Also $e \in eR$ & $e \cdot x = x \quad \forall x \in eR$

$(\because x \in eR \Rightarrow x = ey$ for some $y \in R$
$\Rightarrow ex = e^2 y = ey = x)$

Hence the claim.

So $(1-e)R$ is also a comm ring with unity $(1-e)$ as $1_{(1-e)R}$.

Also note $e(1-e) = 0$

$e(1-e) = e - e^2 = 0$

$eR \times (1-e)R \xrightarrow{\psi} R$

$(ex, (1-e)y) \longmapsto ex + (1-e)y$

$R \xrightarrow{\varphi} eR \times (1-e)R$

$x \longmapsto (ex, (1-e)x)$

$\varphi \circ \psi(ex, (1-e)y) = \varphi(ex + (1-e)y) = (ex, (1-e)y)$

$\psi \circ \varphi = id_R$ & $\varphi \circ \psi = id_{eR \times (1-e)R}$

$\varphi(x+y) = (e(x+y), (1-e)(x+y)) = (ex, (1-e)x) + (ey, (1-e)y)$
$= \varphi(x) + \varphi(y)$

$|||^{ly}$ $\varphi(xy) = (exy, (1-e)xy)$
$= (exey, (1-e)x(1-e)y)$
$= (ex, (1-e)x) \cdot (ey, (1-e)y)$
$= \varphi(x)\varphi(y)$ ▨

Chinese Remainder Theorem: (Classical version): Let $n_1, n_2, \ldots, n_k$ be pairwise coprime positive integers. Let $0 \le a_i < n_i$, $1 \le i \le k$ be integers then $\exists$ an integer a s.t.

$$a \equiv a_i \pmod{n_i} \quad \forall\ 1 \le i \le k$$

Abstract version: Let R be a comm ring with unity. Let $I_1, I_2, \ldots, I_k$ be R-ideals s.t. they are pairwise comaximal, (i.e. $I_j + I_{j'} = R$ for $j \neq j'$). Then the $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$. Moreover the ring homo $\phi : R \to R/I_1 \times \cdots \times R/I_n$, $r \mapsto (r + I_1, \ldots, r + I_n)$ is surj with $\ker(\phi) = I_1 \cap \cdots \cap I_k$. In part.

$$R/I_1 \cdots I_k = R/I_1 \cap \cdots \cap I_k \cong R/I_1 \times \cdots \times R/I_n.$$

Pf of Abstract version $\Rightarrow$ Classical version

$R = \mathbb{Z}$, $I_j = (n_j)$ n_j's pairwise coprime $\Rightarrow$ I_j's are pairwise comaximal.

$$n \longmapsto ([n]_{n_1}, [n]_{n_2}, \ldots, [n]_{n_k})$$

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_k) \quad (\text{surj})$$

(By Abstract version)

$\Rightarrow$ Classical version of CRT

Pf of Abs version of CRT: Case $k=2$. So $I_1+I_2=R$.

Hence $\exists\ x_1\in I_1$ & $x_2\in I_2$ s.t. $x_1+x_2=1$

Let $x\in I_1\cap I_2$ then $x=1\cdot x=(x_1+x_2)x=\underset{\in I_1I_2}{x_1x}+\underset{\in I_1I_2}{x x_2}$

Hence $I_1\cap I_2\subseteq I_1I_2$

$\Rightarrow I_1I_2=I_1\cap I_2$ ($\because I_1I_2\subseteq I_1\cap I_2$ is always true)

$$\varphi: R\to R/I_1\times R/I_2$$
$$r\mapsto (r+I_1,\ r+I_2)$$

$(\bar a,\bar b)\in R/I_1\times R/I_2$, $\bar a(\bar 1,0)+\bar b(0,\bar 1)$

is surj if

$(\bar 1,0)=(1+I_1,\ I_2)$ & $(I_1,\ 1+I_2)=(0,\bar 1)$ are in the image

$(1+I_1,\ I_2)=\varphi(x_2)=(x_2+I_1,\ x_2+I_2)$, where $x_2+I_1=x_1+x_2+I_1=1+I_1$ and $x_2+I_2=I_2$

$(I_1,\ 1+I_2)=\varphi(x_1)$

Hence φ is surjective.

Now $k\geq 3$

Claim: I_1 & $I_2\cdots I_k$ are comaximal

Claim $\Rightarrow I_1\cdot I_2\cdots I_k=I_1\cap I_2\cdots I_k$ ($k=2$ case)
$=I_1\cap I_2\cap\cdots\cap I_k$.

Pf: $I_1+I_j=R\quad\forall\ j\geq 2$

$\Rightarrow x_j+y_j=1$ for some $x_j\in I_1$ & $y_j\in I_j$ $\forall\ j\geq 2$

$(x_2+y_2)(x_3+y_3)\cdots(x_k+y_k)=1$

$\underset{\in I_1}{\alpha}+\underset{\in I_2\cdots I_k}{\underbrace{y_2y_3\cdots y_k}}=1$

Hence the claim.