Lecture 12: Chinese remainder theorem; Euclidean domain and PID

25 September 2020
14:27

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. $\underline{I_j + I_{j'} = R \text{ for } j \neq j'}$). Then the $I_1 \cap \ldots \cap I_k = I_1 \cdots I_k$. Moreover the ring homo $\varphi : R \xrightarrow{r \mapsto (r+I_1, \ldots, r+I_n)} R/I_1 \times \ldots \times R/I_k$ is surj with $\ker(\varphi) = I_1 \cap \ldots \cap I_k$. In part.

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

Pf: So far we saw:
1) $k=2$ case
2) $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$
3) I_1 & $I_2 \cdots I_k$ are comaximal

$j \geq 2$
$x_j \in I_1$ & $y_j \in I_j$
$x_j + y_j = 1$

Like (3) $\boxed{I_j \;\&\; \prod_{\substack{r=1 \\ r \neq j}}^{k} I_r}$ are comaximal.

To show φ is surjective enough to show e_j $1 \leq j \leq k$

$$e_j = (0, \ldots, 0, \overset{j^{th}\text{ spot}}{1}, 0, \ldots, 0) \in R/I_1 \times \ldots \times R/I_k$$

ED

are in the image of φ.

$\exists\, x_j \in I_j$ & $y_j \in \prod_{\substack{r=1 \\ r \neq j}}^{k} I_r$ s.t. $x_j + y_j = 1$

$$\begin{aligned} \text{Then } \varphi(y_j) &= (y_j + I_1, \ldots, y_j + I_k) \\ &= (I_1, \ldots, I_{j-1}, \overset{x_j+}{y_j} + I_j, I_{j+1}, \ldots, I_k) \quad (\because y_j \in I_r \ \forall r \neq j) \\ &= (\bar{0}, \ldots, \bar{0}, \bar{1}, \bar{0}, \ldots, \bar{0}) = e_j \quad \circledast \end{aligned}$$

Let $(\bar{a}_1, \ldots, \bar{a}_k) \in R/I_1 \times \ldots \times R/I_k$ $\quad (a_1 + I_1, \ldots, a_k + I_k)$

$$\begin{aligned} \text{Then } \varphi\Big(\sum_{j=1}^{k} a_j y_j\Big) &= \sum_{j=1}^{k} \varphi(a_j)\varphi(y_j) \\ &= \sum_{j=1}^{k} (\bar{a}_j, \bar{a}_j, \ldots, \bar{a}_j)\, e_j \quad (\text{from } \circledast) \\ &= \sum_{j=1}^{r} (0, \ldots, 0, \overset{j^{th}\text{ spot}}{\bar{a}_j}, 0, \ldots, 0) \\ &= (\bar{a}_1, \ldots, \bar{a}_k) \end{aligned}$$

Note $\ker(\varphi) = I_1 \cap I_2 \cap \ldots \cap I_k$.

$$\begin{aligned} x \in \ker\varphi &\iff x + I_j = I_j \ \forall 1 \leq j \leq k \\ &\iff x \in I_j \ \forall 1 \leq j \leq k \\ &\iff x \in I_1 \cap \cdots \cap I_k \end{aligned}$$

Now use 1st isom thm to conclude $R/I_1 \cap \cdots \cap I_k \cong R/I_1 \times \ldots \times R/I_k$

■

Euclidean domain

Def^n: A Euclidean domain (ED) is an integral domain R s.t. there exist a function $N : R^{\times} \to \mathbb{Z}_{\geq 0}$ satisfying the following conditions.

$R^{\times} = R \setminus \{0\}$

For $a, b \in R^{\times}$ $\exists\, q, r \in R$ s.t.

$$a = bq + r \quad \text{with} \quad N(r) < N(b) \quad \text{or} \quad r = 0.$$

N will be called a Euclidean norm.

Eg: 1) $\mathbb{Z}$, $N : \mathbb{Z}^{\times} \to \mathbb{Z}_{\geq 0}$

$$a \longmapsto |a|$$

$a, b \in \mathbb{Z}^{\times}$, By remainder's thm $\exists\, q \in \mathbb{Z}$ &
$a = bq + r$ $0 \leq r < |b|$
$r \neq 0$ $N(r) = |r| < |b| = N(b)$

2) $\mathbb{Q}[X]$ or $k[X]$, k a field.

$$N : k[X]^{\times} \longrightarrow \mathbb{Z}_{\geq 0}$$
$$f \longmapsto \deg(f)$$

Remainder's thm: $f(X), g(X) \in k[X]$, by Division algo. $\exists\, q(x)$ & $r(X)$ s.t.

$$f(X) = q(X)\, g(X) + r(X) \quad \text{where}$$

$$\deg(r(X)) < \deg(g(X)) \quad \text{or} \quad r(X) = 0$$

$\Longrightarrow$ N is a euclidean norm & $k[X]$ is ED.

3) Valuation rings with valuations as Euclidean norm. (HW)

Principal ideal domain (PID)

Defⁿ: An integral domain R is called PID if every R-ideal is principal, i.e. every R-ideal is generated by one element.

Ex: Fields, $\mathbb{Z}$, $\mathbb{Q}[x]$, $k[x]$

⊛ Let R be an int domain. An element $x \in R$ is called irreducible if x is a nonzero nonunit and if $x = yz$ for some $y, z \in R$ then either y is a unit or z is a unit.

An element $x \in R$ is called a prime element if whenever $x \mid ab \Rightarrow x \mid a$ or $x \mid b$ for $a, b \in R$.

⊛ x is prime iff (x) is a prime ideal.

Pf: $(x) \neq R \iff x$ is a nonunit

$ab \in (x) \iff x \mid ab$

x is prime $\iff x$ is a nonunit & "$x \mid ab \Rightarrow x \mid a$ or $x \mid b$" for $\forall a, b \in R$

$\iff (x) \neq R$ & "$ab \in (x) \Rightarrow a \in (x)$ or $b \in (x)$ $\forall a, b \in R$"

$\iff (x)$ is a prime ideal

⊛ Let R be an int domain & $x \in R$ be a prime element then x is irred.

Pf: Let $x = yz$ for some $y, z \in R$

$\Rightarrow x \mid yz \Rightarrow x \mid y$ or $x \mid z$

$x \mid y \Rightarrow \exists a \in R$ s.t. $y = ax$

$\Rightarrow x = axz$

($\because x \neq 0$ & R int domain)

$\Rightarrow 1 = az \Rightarrow z$ is a unit

$|||^{ly}$ $x \mid z \Rightarrow y$ is a unit. $\boxtimes$

Hence x is irred.

Example: 1) In $\mathbb{Z}$, the prime elements are precisely the prime numbers. Also $\{\text{irreducibles}\} = \{\text{primes}\}$

2) In $\mathbb{Q}$ v no irred or primes.
(or any field)

3) In $k[X]$, k a field. A poly is irreducible if it is an irreducible element of $k[X]$
Also irreducible polynomials are prime elements.

In fact we will see the following:

Thm: Let R be a PID then every irred element of R is a prime element.

Pf: Let $a \in R$ be an irred. element. Then (a) is a proper R-ideal. Let $m \subseteq R$ be a maximal ideal containing (a). Since R is a PID, $m = (b)$ for some $b \in R$.
$a \in m = (b) \Rightarrow a = bc$ for some $c \in R$
But a is irred & b is not a unit
$\Rightarrow c$ is a unit $\Rightarrow b = c^{-1}a \Rightarrow m = (b) = (a)$. Hence
(a) is a prime ideal $\Rightarrow a$ is a prime element. ∎

Cor: (of the proof) In a PID every nonzero prime ideal is maximal ideal.

Thm: Every Euclidean domain is a PID.

Pf: Let R be a ED & let
$N : R^{\times} \longrightarrow \mathbb{Z}_{\geq 0}$ be a Euclidean norm.

Let $I \subseteq R$ be a nonzero ideal.
Let $a \in I$ be such that $N(a)$ is the smallest.

Claim: $(a) = I$.

$(a) \subseteq I$. ✓

Let $b \in I$, so axiom of Euclidean norm
$\exists q, r \in R$ s.t.
$b = qa + r$ with $r = 0$ or $\boxed{N(r) < N(a)}$
Not possible
$(\because r = b - qa \in I \Rightarrow N(r) \geq N(a))$

$\Rightarrow b = qa$
$\Rightarrow b \in (a)$

Hence claim and hence every ideal in R is principal. ∎