

L9: The Chinese Remainder Theorem

Definition 9.1: Direct Product

Let R, S be rings.

The **direct product** of R and S is the ring

$$R \times S := \{(r, s) | r \in R, s \in S\}$$

with ring operations

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$$

$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 \cdot r_2, s_1 \cdot s_2)$$

More generally, if $\{R_\alpha \mid \alpha \in A\}$ is any collection of rings, then the **direct product** of the collection is the ring

$$\prod_{\alpha \in A} R_\alpha := \{(r_\alpha)_{\alpha \in A} \mid r_\alpha \in R_\alpha\}$$

with ring operations

$$(r_\alpha)_{\alpha \in A} + (s_\alpha)_{\alpha \in A} := (r_\alpha + s_\alpha)_{\alpha \in A}$$

$$(r_\alpha)_{\alpha \in A} \cdot (s_\alpha)_{\alpha \in A} := (r_\alpha \cdot s_\alpha)_{\alpha \in A}$$

Definition 9.2: Relatively Prime Integers

Given $a, b \in \mathbb{Z}$, we say they are **relatively prime** if the greatest common divisor is 1. Equivalently (Bezout's Identity), we say a, b are relatively prime if there exists $m, n \in \mathbb{Z}$ such that

$$am + bn = 1$$

Definition 9.3: Comaximal Ideals

In a commutative ring R with $1 \neq 0$, we say two ideals $A, B \subset R$ are **comaximal** (i.e relatively prime) if $A + B = R$. This implies there exists a sum $a + b$ such that $a + b = 1$.

Theorem 9.4: Product of pairwise comaximals is intersection

Let $A_1, \dots, A_k \subset R$ be ideals in a commutative ring with $1 \neq 0$.

If they are pairwise comaximal then

$$A_1 \cdot A_2 \cdot \dots \cdot A_k = A_1 \cap A_2 \cap \dots \cap A_k$$

Proof.

We already know that

$$A_1 \cdot A_2 \cdot \dots \cdot A_k \subset A_1 \cap A_2 \cap \dots \cap A_k$$

It suffices to show

$$A_1 \cap A_2 \cap \dots \cap A_k \subset A_1 \cdot A_2 \cdot \dots \cdot A_k$$

Let's prove this for two ideals and then generalize. First, consider comaximal ideals A, B .

Let $x \in A \cap B$, then we want to show $x \in A \cdot B$

By comaximality,

$$\exists a \in A, b \in B, a + b = 1 \in A + B$$

In particular,

$$x = x \cdot 1 = x \cdot (a + b) = x \cdot a + x \cdot b$$

and so

$$x \in A \cap B \implies \left. \begin{array}{l} x \in A \implies x \cdot b \in A \cdot B \\ x \in B \implies x \cdot a \in A \cdot B \end{array} \right\} \implies x \cdot a + x \cdot b \in A \cdot B$$

Hence $x \in A \cdot B \implies A \cap B \subset A \cdot B$, and we can conclude

$$A \cdot B = A \cap B$$

The general case follows if we can show

$$A = A_1, B = A_2 \cdot A_3 \cdot \dots \cdot A_k$$

are comaximal; we can do this with induction.

By assumption of comaximality A_1, A_i are comaximal for all $i \in \{2, \dots, k\}$ therefore

$$\exists x_2 \in A_1, y_2 \in A_2, \text{ s.t. } 1 = x_2 + y_2$$

$$\exists x_3 \in A_1, y_3 \in A_3, \text{ s.t. } 1 = x_3 + y_3$$

\vdots

$$\exists x_k \in A_1, y_k \in A_k, \text{ s.t. } 1 = x_k + y_k$$

and this implies

$$1 = (x_2 + y_2) \cdot (x_3 + y_3) \cdot \dots \cdot (x_k + y_k) \in A_1 + (A_2 \cdot \dots \cdot A_k)$$

since all x 's are in A_1 and all y 's are in the product of the other ideals, the expanded product will have some mix of x 's and some mixes of the y 's. Hence, we conclude $A_1, A_2 \cdot \dots \cdot A_k$ are comaximal. ■

Theorem 9.5: Chinese Remainder Theorem

Let $A_1, \dots, A_k \subset R$ ideals in a commutative ring with $1 \neq 0$.

The map

$$\begin{aligned} \phi: R &\rightarrow (R/A_1) \times (R/A_2) \times (R/A_3) \times \dots \times (R/A_k) \\ r &\mapsto (r + A_1, r + A_2, r + A_3, \dots, r + A_k) \end{aligned}$$

is a ring homomorphism with $\text{Ker } \phi = A_1 \cap A_2 \cap \dots \cap A_k$.

Moreover, if they are pairwise comaximal, then ϕ is surjective.

Corollary 9.6: Isomorphisms of quotient rings by product of ideals

If $A_1, \dots, A_k \subset R$ are pairwise comaximal ideals in a commutative ring with $1 \neq 0$, then there is an isomorphism of rings (by the First Isomorphism Theorem)

$$R/(A_1 \cdot \dots \cdot A_k) \cong R/(A_1 \cap A_2 \cap \dots \cap A_k) \cong (R/A_1) \times (R/A_2) \times (R/A_3) \times \dots \times (R/A_k)$$

So you can think of your quotient ring over the one ideal or over the separate components of the ideal.

Corollary 9.7: $\mathbb{Z}/n\mathbb{Z}$ isomorphic to quotients by prime factors

Let n be a positive integer with factorization into unique primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

Example 9.1. Here are factorizations of two integer modulo rings:

$$\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$$

$$\mathbb{Z}/168\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$$

Proof of CRT.

We want to see

$$\begin{aligned} \phi: R &\rightarrow (R/A_1) \times (R/A_2) \times (R/A_3) \times \dots \times (R/A_k) \\ r &\mapsto (r + A_1, r + A_2, r + A_3, \dots, r + A_k) \end{aligned}$$

(1) $\text{Ker } \phi = A_1 \cap \dots \cap A_k$

(2) If A_1, \dots, A_k are pairwise comaximal then ϕ is surjective.

We will prove these for $k = 2$ and then generalize:

(1) Let $A, B \subset R$ be ideals and

$$\begin{aligned} \phi: R &\rightarrow (R/A) \times (R/B) \\ r &\mapsto (r + A, r + B) \end{aligned}$$

Let $r \in \text{Ker } \phi$, then

$$\left. \begin{aligned} r + A = 0 + A &\implies r \in A \\ r + B = 0 + B &\implies r \in B \end{aligned} \right\} \implies r \in A \cap B$$

If $r \in A \cap B$ then

$$\left. \begin{aligned} r \in A &\implies r + A = 0 + A \\ r \in B &\implies r + B = 0 + B \end{aligned} \right\} \implies r \in \text{Ker } \phi$$

(2) If A, B are comaximal then there exists $x \in A, y \in B$ such that $1 = x + y$, then

$$1 - x = y \in B \implies 1 + A = y + A$$

$$1 - y = x \in A \implies 1 + B = x + B$$

and hence

$$\phi(x) = (x + A, x + B) = (0 + A, 1 + B)$$

$$\phi(y) = (y + A, y + B) = (1 + A, 0 + B)$$

So if we have any element $(r + A, s + B) \in R/A \times R/B$ then

$$\begin{aligned} (r + A, s + B) &= (r + A, 0 + B) + (0 + A, s + B) \\ &= (r + A, r + B) \cdot (1 + A, 0 + B) + (s + A, s + B) \cdot (0 + A, 1 + B) \\ &= \phi(r) \cdot \phi(y) + \phi(s) \cdot \phi(x) \\ &= \phi(ry + sx) \implies \phi \text{ surjective} \end{aligned}$$

More generally if $A_1, \dots, A_k \subset R$ are ideals.

Let $A = A_1$, $B = A_2 \cdot A_3 \dots \cdot A_k$, then we have a homomorphism

$$\phi_1: R \rightarrow R/A \times R/B, \quad \text{Ker } \phi_1 = A_1 \cap B$$

Now by the Lattice Isomorphism Theorem $A_2/B, A_3/B, \dots, A_k/B \subset R/B$ are ideals.

Take

$$A' = A_2/B, \quad B' = (A_3/B) \cdot (A_4/B) \cdot \dots \cdot (A_k/B) = (A_3 \cdot A_4 \cdot \dots \cdot A_k)/B$$

Then we get a homomorphism

$$\phi_2: R/B \rightarrow (R/B)/A' \times (R/B)/B', \quad \text{Ker } \phi_2 = A' \cap B'$$

By the third isomorphism theorem

$$(R/B)/A' = (R/B)/(A_2/B) \cong R/A_2$$

and similarly,

$$(R/B)/B' = (R/B)/(A_3 \cdot A_4 \cdot \dots \cdot A_k)/B \cong R/(A_3 \cdot A_4 \cdot \dots \cdot A_k)$$

Therefore, we have

$$\hat{\phi}_2 = (\text{Id}, \phi_2) \circ \phi_1: R \rightarrow R/A_1 \times R/A_2 \times R/(A_3 \cdot \dots \cdot A_k)$$

Proceeding inductively on k , we end up with

$$\phi: R \rightarrow R/A_1 \times R/A_2 \times \dots \times R/A_k$$

and the surjectivity when A_1, \dots, A_k are pairwise comaximal follow essentially because A_1, A_2, \dots, A_k are comaximal. ■