5 Chinese Remainder Theorem

We can define direct products of rings, just as we did for groups. If R, S are rings, then $R \times S$ is a ring under componentwise addition and multiplication. This can be done for an arbitrary family $\{R_i \mid i \in I\}$ of rings, in which case the direct product is denoted $\prod_{i \in I} R_i$. It is easy to see that if A_i is an ideal in R_i for each $i \in I$, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.

If $R_1 \times \cdots \times R_n$ is a finite direct product of rings, each of which has identity, then every ideal of $R_1 \times \cdots \times R_n$ is of the form $A_1 \times \cdots \times A_n$, where A_i is an ideal in R_i. (Notice this is quite different from what could happen for subgroups of direct products of groups.)

Definition 5.1. *Two ideals A_1, A_2 of a ring R are called* comaximal *if $A_1 + A_2 = R$.*

Theorem 5.2. Chinese Remainder Theorem *Let $A_1, A_2, \ldots, A_k$ be ideals in a commutative ring R with 1. The map $R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k$ defined by $r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$ is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$, the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so*

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Proof. We prove for $k = 2$. The general case follows by induction if we can show $A = A_1$ and $B = A_2 \cdots A_k$ are comaximal when the A_1's are pairwise comaximal. We show this first. For each $i \in \{2, 3, \ldots, k\}$, there exist elements $x_i \in A_1$ and $y_i \in A_i$ such that $x_i + y_i = 1$. Thus $1 = (x_2 + y_2) \cdots (x_k + y_k) \in A_1 + (A_2 \cdots A_k)$.

To prove the main result for $k = 2$, let $A = A_1, B = A_2$, and let $\phi : R \to R/A \times R/B$ as defined in the statement of the theorem. This is clearly a ring homomorphism. with kernel $A \cap B$. If A, B are comaximal, then $A + B = R$ so there exist $x \in A, y \in B$ such that $x + y = 1$. Then $\phi(x) = (0, 1); \phi(y) = (1, 0)$. Thus for any $r_1, r_2 \in R$, we have $\phi(r_2 x, r_1 y) = (r_1 + A, r_2 + B)$, showing ϕ is surjective. We have $AB \subseteq A \cap B$ always. If A, B are comaximal, then for $c \in A \cap B$, $c = c \cdot 1 = cx + cy \in AB$, so $AB = A \cap B$. □

Corollary 5.3. *If m, n are relatively prime, then $\boldsymbol{Z}/mn\boldsymbol{Z} \cong \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/n\boldsymbol{Z}$ as rings. In particular, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then $\boldsymbol{Z}/n\boldsymbol{Z} \cong \boldsymbol{Z}/p_1^{\alpha_1}\boldsymbol{Z} \times \cdots \times \boldsymbol{Z}/p_k^{\alpha_k}\boldsymbol{Z}$ as rings, so $(\boldsymbol{Z}/n\boldsymbol{Z})^* \cong (\boldsymbol{Z}/p_1^{\alpha_1}\boldsymbol{Z})^* \times \cdots \times (\boldsymbol{Z}/p_k^{\alpha_k}\boldsymbol{Z})^*$*