Modern Algebra I

Lecture 17

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

Chapter III: Rings

Section III.2: Ideals

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i \in I} R_i$ be the direct product of the additive abelian groups R_i.

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i \in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i \in I} R_i$ is a ring with multiplication defined by

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$,

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$,

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$ is an epimorphism of rings.

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$ is an epimorphism of rings.
- For every $k \in I$,

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$ is an epimorphism of rings.
- For every $k \in I$, the canonical injection $\iota_k : R_k \to \prod_{i\in I} R_i$

Direct Products

Theorem (2.22). Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$ is an epimorphism of rings.
- For every $k \in I$, the canonical injection $\iota_k : R_k \to \prod_{i\in I} R_i$ with $a_k \mapsto (a_i)_{i\in I}$, where $a_i = 0\ \forall i \neq k$,

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).
- For every $k \in I$, the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ with $(a_i)_{i\in I} \mapsto a_k$ is an epimorphism of rings.
- For every $k \in I$, the canonical injection $\iota_k : R_k \to \prod_{i\in I} R_i$ with $a_k \mapsto (a_i)_{i\in I}$, where $a_i = 0\ \forall i \neq k$, is a monomorphism of rings.

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the

Direct Products

Theorem (2.22)**.** Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the (external) direct product of the family of rings $\{R_i \mid i \in I\}$.

Direct Products

Theorem (2.22). Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the (external) direct product of the family of rings $\{R_i \mid i \in I\}$. If the index set is finite,

Direct Products

Theorem (2.22). Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the (external) direct product of the family of rings $\{R_i \mid i \in I\}$. If the index set is finite, say $I = \{1, 2, \ldots, n\}$,

Direct Products

Theorem (2.22). Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the (external) direct product of the family of rings $\{R_i \mid i \in I\}$. If the index set is finite, say $I = \{1, 2, \ldots, n\}$, then we sometimes write $R_1 \times R_2 \times \cdots \times R_n$, instead of $\prod_{i=1}^{n} R_i$.

Direct Products

Theorem (2.22). Let $\{R_i \mid i \in I\}$ be a nonempty family of rings and let $\prod_{i\in I} R_i$ be the direct product of the additive abelian groups R_i.

- $\prod_{i\in I} R_i$ is a ring with multiplication defined by
$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}.$$
- If R_i has an identity 1_{R_i} (resp. is commutative) for all $i \in I$, then $\prod_{i\in I} R_i$ has an identity $(1_{R_i})_{i\in I}$ (resp. is commutative).

Definition. The ring $\prod_{i\in I} R_i$ is called the (external) direct product of the family of rings $\{R_i \mid i \in I\}$. If the index set is finite, say $I = \{1, 2, \ldots, n\}$, then we sometimes write $R_1 \times R_2 \times \cdots \times R_n$, instead of $\prod_{i=1}^{n} R_i$.

Ideals in Direct Products

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i \in I} R_i$ is of the form

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i \in I} R_i$ is of the form $\prod_{i \in I} A_i$ with A_i an ideal in R_i.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.

Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^n R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.

Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i\in I} A_i$ is an ideal in $\prod_{i\in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i\in I} R_i$ is of the form $\prod_{i\in I} A_i$ with A_i an ideal in R_i.

Proof. The first statement can be checked easily. We only show the second statement here.

Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^n R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.

Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that
$(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n)$

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$,

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) \in \mathcal{A}$.

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) \in \mathcal{A}$.
Hence $A_1 \times A_2 \times \cdots \times A_n \subseteq \mathcal{A}$,

Ideals in Direct Products

Proof. Let $\mathcal{A}$ be an ideal in $R_1 \times R_2 \times \cdots \times R_n$. For each $k = 1, 2, \ldots, n$, let $A_k = \pi_k(\mathcal{A})$, where $\pi_k : \prod_{i=1}^{n} R_i \to R_k$ is the canonical epimorphism. Since π_k is an epimorphism, A_k is an ideal of R_k. We claim that $\mathcal{A} = A_1 \times A_2 \times \cdots \times A_n$.
Note that if $\alpha = (a_1, \ldots, a_n) \in \mathcal{A}$, $a_k = \pi_k(\alpha) \in \pi_k(\mathcal{A}) = A_k$ for each $k = 1, 2, \ldots, n$. Hence, $\mathcal{A} \subseteq A_1 \times A_2 \times \cdots \times A_n$.

Conversely, let $a_1 \in A_1$. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha = (a_1, a_2, \ldots, a_n)$. Note that $(a_1, 0, \ldots, 0) = (1_{R_1}, 0, \ldots, 0)(a_1, a_2, \ldots, a_n) \in \mathcal{A}$. Similarly, we can show for each k that if $a_k \in A_k$ then $(0, \ldots, 0, a_k, 0, \ldots 0) \in \mathcal{A}$. Therefore, if $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, a_n) \in \mathcal{A}$.
Hence $A_1 \times A_2 \times \cdots \times A_n \subseteq \mathcal{A}$, and this completes the proof.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity,

Ideals in Direct Products

Remark. Let $\{R_i \mid i \in I\}$ be a family of rings.

- If for each $i \in I$, A_i is an ideal in R_i, then $\prod_{i \in I} A_i$ is an ideal in $\prod_{i \in I} R_i$.
- Conversely, if $|I| < \infty$ and every R_i has an identity, then every ideal in $\prod_{i \in I} R_i$ is of the form $\prod_{i \in I} A_i$ with A_i an ideal in R_i.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings,

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings,

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property. In other words,

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i \in I} R_i$ is a product in the category of rings.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i \in I} R_i$ such that $\pi_i \varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i \in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i \in I} R_i$ is a product in the category of rings.

Proof.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism,

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism, such that $\pi_i\varphi = \varphi_i \; \forall i \in I$.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism, such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Recall that $\varphi(a) = \big(\varphi_i(a)\big)_{i\in I}$ for all $a \in S$.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism, such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Recall that $\varphi(a) = \big(\varphi_i(a)\big)_{i\in I}$ for all $a \in S$. It is easy to check that φ is indeed a ring homomorphism.

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism, such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Recall that $\varphi(a) = \big(\varphi_i(a)\big)_{i\in I}$ for all $a \in S$. It is easy to check that φ is indeed a ring homomorphism. Thus $\prod_{i\in I} R_i$ is a product in the category of rings

Theorem (2.23)

Let $\{R_i \mid i \in I\}$ be a nonempty family of rings. If S is a ring, and if $\{\varphi_i : S \to R_i \mid i \in I\}$ a family of homomorphisms of rings, then there is a unique homomorphism of rings $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Moreover, the ring $\prod_{i\in I} R_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} R_i$ is a product in the category of rings.

Proof. By Theorem (I.8.2), $\exists!\varphi : S \to \prod_{i\in I} R_i$, a group homomorphism, such that $\pi_i\varphi = \varphi_i \; \forall i \in I$. Recall that $\varphi(a) = \big(\varphi_i(a)\big)_{i\in I}$ for all $a \in S$. It is easy to check that φ is indeed a ring homomorphism. Thus $\prod_{i\in I} R_i$ is a product in the category of rings and therefore determined uniquely up to isomorphism by Theorem (I.7.3).

Review

Corollary (I.8.7)**.** If $N_1, N_2, \ldots, N_r$ are normal subgroups of a group G such that

- $G = N_1 N_2 \cdots N_r$, and
- $N_k \cap (N_1 \cdots N_{k-1} N_{k+1} \cdots N_r) = \langle e \rangle$, $\forall k = 1, \ldots, r$,

then $G \simeq N_1 \times N_2 \times \cdots \times N_r$.

Review

Corollary (I.8.7). If $N_1, N_2, \ldots, N_r$ are normal subgroups of a group G such that

- $G = N_1 N_2 \cdots N_r$, and
- $N_k \cap (N_1 \cdots N_{k-1} N_{k+1} \cdots N_r) = \langle e \rangle$, $\forall k = 1, \ldots, r$,

then $G \simeq N_1 \times N_2 \times \cdots \times N_r$.

In the proof of this corollary, we proved that the map

$$\begin{array}{rccc} \varphi & : & N_1 \times N_2 \times \cdots \times N_r & \longrightarrow & G \\ & & (a_1, a_2, \ldots, a_r) & \longmapsto & a_1 a_2 \cdots a_r \end{array}$$

is a group isomorphism.

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups.

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{ccccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n)$

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j$

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j$

Note that $\forall i \neq j$,

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j$

Note that $\forall i \neq j$, $a_i b_j \in A_i \cap A_j$

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j$

Note that $\forall i \neq j$, $a_i b_j \in A_i \cap A_j = 0$,

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$$\begin{aligned}(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \\ &= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.\end{aligned}$$

Note that $\forall i \neq j$, $a_i b_j \in A_i \cap A_j = 0$, so we have

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$$\begin{aligned}(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \\ &= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.\end{aligned}$$

Note that $\forall i \neq j$, $a_i b_j \in A_i \cap A_j = 0$, so we have

Therefore, φ is also a ring homomorphism

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0, \forall k = 1, \ldots, n.$

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Proof. We have shown that the map

$$\begin{array}{rccc} \varphi & : & A_1 \times A_2 \times \cdots \times A_n & \longrightarrow & R \\ & & (a_1, a_2, \ldots, a_n) & \longmapsto & a_1 + a_2 + \cdots + a_n \end{array}$$

is an isomorphism of groups. Moreover,

$$\begin{aligned}(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \\ &= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.\end{aligned}$$

Note that $\forall i \neq j$, $a_i b_j \in A_i \cap A_j = 0$, so we have

Therefore, φ is also a ring homomorphism and hence is a ring isomorphism.

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24),

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24), then R is said to be the (internal) direct product of the ideals A_i.

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24), then R is said to be the (internal) direct product of the ideals A_i.

Notation. We write $R = \prod_{i=1}^{n} A_i$

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24), then R is said to be the (internal) direct product of the ideals A_i.

Notation. We write $R = \prod_{i=1}^{n} A_i$ or $R = A_1 \times A_2 \times \cdots \times A_n$

Internal Direct Products

Theorem (2.24)**.** Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24), then R is said to be the (internal) direct product of the ideals A_i.

Notation. We write $R = \prod_{i=1}^{n} A_i$ or $R = A_1 \times A_2 \times \cdots \times A_n$ to indicate that

Internal Direct Products

Theorem (2.24). Let $A_1, \ldots, A_n$ be ideals in a ring R such that

- $A_1 + A_2 + \cdots + A_n = R$ and
- $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = 0$, $\forall k = 1, \ldots, n$.

Then $R \simeq A_1 \times A_2 \times \cdots \times A_n$ as rings.

Definition. If R is a ring and $A_1, \ldots, A_n$ are ideals in R that satisfy the hypothesis of Theorem (2.24), then R is said to be the (internal) direct product of the ideals A_i.

Notation. We write $R = \prod_{i=1}^{n} A_i$ or $R = A_1 \times A_2 \times \cdots \times A_n$ to indicate that the ring R is the internal direct product of its ideals $A_1, \ldots, A_n$.

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R.

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$,

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$,

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A,

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A}$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A}$$
$$\implies a_1 + A = a_2 + A \text{ and } b_1 + A = b_2 + A \text{ in } R/A$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$\begin{aligned} & a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A} \\ \Longrightarrow\ & a_1 + A = a_2 + A \text{ and } b_1 + A = b_2 + A \text{ in } R/A \\ \Longrightarrow\ & (a_1 + b_1) + A = (a_2 + b_2) + A \end{aligned}$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$\begin{aligned} & a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A} \\ \Longrightarrow\ & a_1 + A = a_2 + A \text{ and } b_1 + A = b_2 + A \text{ in } R/A \\ \Longrightarrow\ & (a_1 + b_1) + A = (a_2 + b_2) + A \text{ and } a_1 b_1 + A = a_2 b_2 + A \end{aligned}$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$\begin{aligned} & a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A} \\ \Longrightarrow\ & a_1 + A = a_2 + A \text{ and } b_1 + A = b_2 + A \text{ in } R/A \\ \Longrightarrow\ & (a_1 + b_1) + A = (a_2 + b_2) + A \text{ and } a_1 b_1 + A = a_2 b_2 + A \\ \Longrightarrow\ & a_1 + b_1 \equiv a_2 + b_2 \pmod{A} \end{aligned}$$

Congruence Modulo an Ideal

Definition. Let A be an ideal in a ring R. For $a, b \in R$, if $a - b \in A$, we say that a is congruent to b modulo A, denoted $a \equiv b \pmod{A}$.

Remark. Note that

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

Hence, we have

$$\begin{aligned} & a_1 \equiv a_2 \pmod{A} \text{ and } b_1 \equiv b_2 \pmod{A} \\ \Longrightarrow\ & a_1 + A = a_2 + A \text{ and } b_1 + A = b_2 + A \text{ in } R/A \\ \Longrightarrow\ & (a_1 + b_1) + A = (a_2 + b_2) + A \text{ and } a_1 b_1 + A = a_2 b_2 + A \\ \Longrightarrow\ & a_1 + b_1 \equiv a_2 + b_2 \pmod{A} \text{ and } a_1 b_1 \equiv a_2 b_2 \pmod{A}. \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R$, $\forall i = 1, 2, \ldots, n$,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R,$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Remark. If R has an identity,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Remark. If R has an identity, then $R^2 = R$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Remark. If R has an identity, then $R^2 = R$ and hence $R^2 + A = R$ for every ideal A of R.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}$ $\forall i = 1, \ldots, n.$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}$ $\forall i = 1, \ldots, n$. Then

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}\ \forall i = 1, \ldots, n$. Then

$$b \equiv c \pmod{A_i} \quad \forall i$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}\ \forall i = 1, \ldots, n$. Then

$$b \equiv c \pmod{A_i} \quad \forall i \implies b - c \in A_i \quad \forall i$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}\ \forall i = 1, \ldots, n$. Then

$$b \equiv c \pmod{A_i} \quad \forall i \implies b - c \in A_i \quad \forall i$$

$$\implies \quad b - c \in \bigcap_{i=1}^{n} A_i$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. We first show the uniqueness. Suppose $c \in R$ also satisfies that $c \equiv b_i \pmod{A_i}\ \forall i = 1, \ldots, n$. Then

$$b \equiv c \pmod{A_i} \quad \forall i \implies b - c \in A_i \quad \forall i$$

$$\implies \quad b - c \in \bigcap_{i=1}^{n} A_i \implies b \equiv c \pmod{\bigcap_{i=1}^{n} A_i}.$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n,$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Take $b = r_1 + r_2 + \cdots + r_n$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Take $b = r_1 + r_2 + \cdots + r_n$.

Then $b \equiv b_1 \pmod{A_1}$,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Take $b = r_1 + r_2 + \cdots + r_n$.

Then $b \equiv b_2 \pmod{A_2}$,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Take $b = r_1 + r_2 + \cdots + r_n$.

Then $b \equiv b_k \pmod{A_k}, \forall k = 1, \ldots, n.$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Then for any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Proof. If we show that $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n,$ then we have $\forall k = 1, \ldots, n$, $b_k = a_k + r_k$ for some $a_k \in A_k$ and $r_k \in \bigcap_{i \neq k} A_i$. Note that

$$r_k \equiv b_k \pmod{A_k} \quad \text{and} \quad r_k \equiv 0 \pmod{A_i} \; \forall i \neq k.$$

Hence it remains to show $R = A_k + \left(\bigcap_{i \neq k} A_i\right), \forall k = 1, \ldots, n.$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R,$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.
Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,
R^2

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3)$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1 A_3$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover, since $R^2 + A_1 = R$,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover, since $R^2 + A_1 = R$,

$$R = R^2 + A_1$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover, since $R^2 + A_1 = R$,

$$R = R^2 + A_1 \subseteq A_1 + (A_2 \cap A_3)$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover, since $R^2 + A_1 = R$,

$$R = R^2 + A_1 \subseteq A_1 + (A_2 \cap A_3) \subseteq R$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \\ &\subseteq A_1 + (A_2 \cap A_3). \end{aligned}$$

Moreover, since $R^2 + A_1 = R$,

$$R = R^2 + A_1 \subseteq A_1 + (A_2 \cap A_3) \subseteq R$$

$$\Longrightarrow \quad R = A_1 + (A_2 \cap A_3).$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$R^2$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$R^2 = \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big)$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \end{aligned}$$

$$\Longrightarrow \quad R = R^2 + A_1$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \\ \Longrightarrow \quad R = R^2 + A_1 &\subseteq A_1 + (A_2 \cap \cdots \cap A_k) \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \\ \Longrightarrow \quad R = R^2 + A_1 &\subseteq A_1 + (A_2 \cap \cdots \cap A_k) \subseteq R \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \\ \Longrightarrow \quad R = R^2 + A_1 &\subseteq A_1 + (A_2 \cap \cdots \cap A_k) \subseteq R \\ \Longrightarrow \quad R &= A_1 + (A_2 \cap \cdots \cap A_k), \end{aligned}$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \\ \Longrightarrow \quad R = R^2 + A_1 &\subseteq A_1 + (A_2 \cap \cdots \cap A_k) \subseteq R \\ \Longrightarrow \quad R &= A_1 + (A_2 \cap \cdots \cap A_k), \end{aligned}$$

and the induction step is proved.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Assume inductively that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= \big(A_1 + (A_2 \cap \cdots \cap A_{k-1})\big)\big(A_1 + A_k\big) \\ &\subseteq A_1 + (A_2 \cap \cdots \cap A_{k-1} \cap A_k) \\ \Longrightarrow \quad R = R^2 + A_1 &\subseteq A_1 + (A_2 \cap \cdots \cap A_k) \subseteq R \\ \Longrightarrow \quad R &= A_1 + (A_2 \cap \cdots \cap A_k), \end{aligned}$$

and the induction step is proved. Hence we can prove inductively that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

The proofs of $R = A_k + \bigcap_{i \neq k}^{n} A_i$ for $k = 2, \ldots, n$ are practically the same,

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.
The proofs of $R = A_k + \bigcap_{i \neq k}^{n} A_i$ for $k = 2, \ldots, n$ are practically the same, simply by exchanging the roles of A_1 and A_k in our proof above.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

Proof. We first show that $R = A_1 + (A_2 \cap \cdots \cap A_n)$.
The proofs of $R = A_k + \bigcap_{i \neq k}^{n} A_i$ for $k = 2, \ldots, n$ are practically the same, simply by exchanging the roles of A_1 and A_k in our proof above. This completes the proof of CRT.

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

For any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Chinese Remainder Theorem

Theorem (2.25, Chinese Remainder Theorem)**.**

Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

- $R^2 + A_i = R, \forall i = 1, 2, \ldots, n,$
- $A_i + A_j = R, \forall i \neq j.$

For any $b_1, b_2, \ldots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \quad \forall i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$.

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$,

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Proof.

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Proof. For each $i = 1, \ldots, n$,

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Proof. For each $i = 1, \ldots, n$, consider the ideals $A_i = (m_i)$ in the ring $\mathbb{Z}$.

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Proof. For each $i = 1, \ldots, n$, consider the ideals $A_i = (m_i)$ in the ring $\mathbb{Z}$. Since $A_i + A_j = \mathbb{Z} \; \forall i \neq j$,

CRT in Number Theory

Corollary (2.26)**.** Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1 \; \forall i \neq j$. For any $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, the system of congruences

$$\begin{cases} X \equiv b_1 & (\text{mod } m_1) \\ X \equiv b_2 & (\text{mod } m_2) \\ \quad \vdots & \\ X \equiv b_n & (\text{mod } m_n) \end{cases}$$

has an integral solution that is uniquely determined modulo $m = m_1 m_2 \cdots m_n$.

Proof. For each $i = 1, \ldots, n$, consider the ideals $A_i = (m_i)$ in the ring $\mathbb{Z}$. Since $A_i + A_j = \mathbb{Z} \; \forall i \neq j$, we can apply Theorem 2.25 to finish the proof.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Remark.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Remark.

- We also refer to Corollary (2.27) as the Chinese Remainder Theorem.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Remark.

- We also refer to Corollary (2.27) as the Chinese Remainder Theorem.
- Theorem (2.25) and Corollary (2.27) are practically the same.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Remark.

- We also refer to Corollary (2.27) as the Chinese Remainder Theorem.
- Theorem (2.25) and Corollary (2.27) are practically the same. They are just stated in different “languages”.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. By Theorem (2.23), the canonical epimorphisms $\pi_k : R \to R/A_k$, $k = 1, 2, \ldots, n$,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. By Theorem (2.23), the canonical epimorphisms $\pi_k : R \to R/A_k$, $k = 1, 2, \ldots, n$, induce a ring homomorphism

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. By Theorem (2.23), the canonical epimorphisms $\pi_k : R \to R/A_k$, $k = 1, 2, \ldots, n$, induce a ring homomorphism

$$\begin{array}{rcccc} \theta_1 & : & R & \longrightarrow & R/A_1 \times R/A_2 \times \cdots \times R/A_n \\ & & r & \longmapsto & (r + A_1, r + A_2, \ldots, r + A_n) \end{array}$$

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. By Theorem (2.23), the canonical epimorphisms $\pi_k : R \to R/A_k$, $k = 1, 2, \ldots, n$, induce a ring homomorphism

$$\begin{array}{rcccc} \theta_1 & : & R & \longrightarrow & R/A_1 \times R/A_2 \times \cdots \times R/A_n \\ & & r & \longmapsto & (r + A_1, r + A_2, \ldots, r + A_n) \end{array}$$

Clearly, $\operatorname{Ker} \theta_1 = A_1 \cap A_2 \cap \cdots \cap A_n$.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. By Theorem (2.23), the canonical epimorphisms $\pi_k : R \to R/A_k$, $k = 1, 2, \ldots, n$, induce a ring homomorphism

$$\begin{array}{rcccc} \theta_1 & : & R & \longrightarrow & R/A_1 \times R/A_2 \times \cdots \times R/A_n \\ & & r & \longmapsto & (r + A_1, r + A_2, \ldots, r + A_n) \end{array}$$

Clearly, $\operatorname{Ker} \theta_1 = A_1 \cap A_2 \cap \cdots \cap A_n$. Therefore, θ_1 induces a monomorphism of rings, i.e., θ above.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n,$

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i.

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Hence for any $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R, \forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Hence for any $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$ $\exists b \in R$ such that $b_i + A_i = b + A_i$ for all i,

Chinese Remainder Theorem

Corollary (2.27)**.** If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R$, $\forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Hence for any $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$ $\exists b \in R$ such that $b_i + A_i = b + A_i$ for all i, i.e., $\theta\big(b + (A_1 \cap \cdots \cap A_n)\big) = (b_1 + A_1, \ldots, b_n + A_n)$.

Chinese Remainder Theorem

Corollary (2.27). If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R$, $\forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Hence for any $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$ $\exists b \in R$ such that $b_i + A_i = b + A_i$ for all i, i.e., $\theta\big(b + (A_1 \cap \cdots \cap A_n)\big) = (b_1 + A_1, \ldots, b_n + A_n)$. Therefore θ is surjective,

Chinese Remainder Theorem

Corollary (2.27). If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then

$$\begin{array}{rcccc} \theta & : & R/(A_1 \cap \cdots \cap A_n) & \longrightarrow & R/A_1 \times \cdots \times R/A_n \\ & & a + (A_1 \cap \cdots \cap A_n) & \longmapsto & (a + A_1, \ldots, a + A_n) \end{array}$$

is a monomorphism of rings. If $R^2 + A_i = R \; \forall i = 1, 2, \ldots, n$ and $A_i + A_j = R \; \forall i \neq j$, then θ is an isomorphism of rings.

Proof. Moreover, if $R^2 + A_i = R$, $\forall i = 1, \ldots, n$, and if $A_i + A_j = R \; \forall i \neq j$, Theorem (2.25) tells us that for any $b_1, b_2, \ldots, b_n \in R$, $\exists b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Hence for any $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$ $\exists b \in R$ such that $b_i + A_i = b + A_i$ for all i, i.e., $\theta\big(b + (A_1 \cap \cdots \cap A_n)\big) = (b_1 + A_1, \ldots, b_n + A_n)$. Therefore θ is surjective, and so θ is an isomorphism of rings.

Exercise for Section III.2

1, 2, 3, 10, 11, 13, 16, 18.