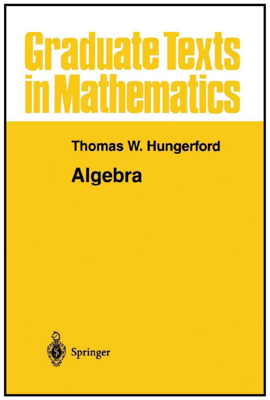
Modern Algebra

Chapter III. Rings

III.2. Ideals—Proofs of Theorems



Theorem III.2.2

Theorem II.2.2. A nonempty subset I of a ring R is a left (respectively, right) ideal if and only if for all $a, b \in I$ and $r \in R$:

(i) $a, b \in I$ implies $a - b \in I$, and

(ii) $a \in I$, $r \in R$ implies $ra \in I$ (respectively, $ar \in I$).

Proof. Suppose I is a left ideal. Then, by definition, (ii) holds. Since an ideal is a subring then (i) holds.

Suppose (i) and (ii) hold for set I. Then I is a group under addition from (i) by Theorem I.2.5. By (ii), I is closed under multiplication. So I is a subring of R. By (ii) R is a left ideal. Similarly for "right ideals." □

Theorem III.2.5

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(i) The principal ideal (a) consists of all elements of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i$$

where $r, s, r_i, s_i \in R$, $m \in \mathbb{N} \cup \{0\}$, and $n \in \mathbb{Z}$.

(ii) If R has an identity ("unity") then

$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \in \mathbb{N} \right\}.$$

(iii) If a is in the center of R, $C(R) = \{c \in R \mid cr = rc \text{ for all } r \in R\}$, then $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$.

Theorem III.2.5 (continued)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(iv) $Ra = \{ra \mid r \in R\}$ (respectively, $aR = \{ar \mid r \in R\}$), is a left (respectively, right) ideal in R (which may not contain a). If R has an identity, then $a \in Ra$ and $a \in aR$.

(v) If R has an identity and a is in the center of R, then $Ra = (a) = aR$.

(vi) If R has an identity and X is the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ where $n \in \mathbb{N} \cup \{0\}$, $r_i \in R$, and $a_i \in X$.

Theorem III.2.5(i)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(i) The principal ideal (a) consists of all elements of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i$$

where $r, s, r_i, s_i \in R$, $m \in \mathbb{N} \cup \{0\}$, and $n \in \mathbb{Z}$.

Proof. (i) Let $r' \in R$ and $a' \in I$ where I consists of the elements of the given form. Then

$$\begin{aligned} r'a' &= r'\left(ra + as + na + \sum_{i=1}^{m} r_i a s_i\right) \\ &= (r'r + nr')a + \sum_{i=1}^{m+1} r_i' a s_i \text{ where } r_i' = r' r_i,\ r_{m+1} = r', \text{ and } s_{m+1} = s \\ &\in I \text{ since } r'r + nr' \in R. \end{aligned}$$

Theorem III.2.5(i) continued

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(i) The principal ideal (a) consists of all elements of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i$$

where $r, s, r_i, s_i \in R$, $m \in \mathbb{N} \cup \{0\}$, and $n \in \mathbb{Z}$.

Proof. (i) (continued) So I is a left ideal and, similarly, a right ideal. With $r = s = 0$, $n = 1$, $m = 1$, $r_1 = 0$ we see that $a \in I$.

Now let I' be any ideal containing a. Then $ra \in I'$ and $r_i a \in I'$ since I' is a left ideal. So as and $r_i a s_i \in I'$ since I' is a right ideal. Next, $na \in I'$ since I' is a subring of R (and so is closed under addition). So $ra + as + na + \sum_{i=1}^{m} r_i a s_i \in I'$ and $I \subseteq I'$. That is, I is a subset of any ideal containing a, so $I = (a)$. □

Theorem III.2.5(ii)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(ii) If R has an identity ("unity") then

$$(a) = \left\{\sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \in \mathbb{N}\right\}.$$

Proof. (ii) If R has identity 1_R, then we write $ra = ra1_R = r_{m+1} a s_{m+1}$, $as = 1_R as = r_{m+2} a s_{m+2}$, and $na = n(1_R a) = (n1_R)a1_R = r_{m+3} a s_{m+3}$ and so any element of (a) is of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i = \sum_{i=1}^{m+3} r_i a s_i.$$

Theorem III.2.5(iii)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(iii) If a is in the center of R,
$C(R) = \{c \in R \mid cr = rc \text{ for all } r \in R\}$, then
$(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$.

Proof. (iii) If a is in the center of R then any element of (a) is of the form

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i = ra + sa + na + \sum_{i=1}^{m} r_i s_i a$$

$$= \left(r + s + \sum_{i=1}^{m} r_i s_i\right) a + na = r'a + na$$

where $r' = r + s + \sum_{i=1}^{m} r_i s_i$. □

Theorem III.2.5(iv, v)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(iv) $Ra = \{ra \mid r \in R\}$ (respectively, $aR = \{ar \mid r \in R\}$), is a left (respectively, right) ideal in R (which may not contain a). If R has an identity, then $a \in Ra$ and $a \in aR$.

(v) If R has an identity and a is in the center of R, then $Ra = (a) = aR$.

Proof. **(iv)** This is almost trivial given Note III.2.A.

(v) By (iii),

$$(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\} = \{ra + (n1_R)a \mid r \in R, n \in \mathbb{Z}\}$$

$$= \{(r + n1_R)a \mid r \in R, n \in \mathbb{Z}\} = \{r'a \mid r' \in R\} = Ra.$$

With a in the center of R, $r'a = ar'$ and so $(a) = aR$ as well. □

Theorem III.2.5(vi)

Theorem III.2.5. Let R be a ring $a \in R$ and $X \subset R$.

(vi) If R has an identity and X is the center of R, then the ideal (X) consists of all finite sums $r_1a_1 + r_2a_2 + \cdots + r_na_n$ where $n \in \mathbb{N} \cup \{0\}$, $r_i \in R$, and $a_i \in X$.

Proof. **(vi)** Let R have identity and let X be in the center of R. Let I be an ideal containing X and let $a_i \in X$. Since I is an ideal containing a_i, then I must contain (a_i) (the "smallest" ideal containing a_i) and by (v) contains $Ra_i = \{ra_i \mid r \in R\}$. Since I is an ideal, then it is a subring of R and so contains all $r_1a_1 + r_2a_2 + \cdots + r_na_n$. Let $I' = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R, a_i \in X\}$, so $I' \subseteq I$. For $r \in R$ and $r_1a_1 + r_2a_2 + \cdots + r_na_n \in I'$ we have $r(r_1a_1 + r_2a_2 + \cdots r_na_n) = (rr_1)a_1 + (rr_2)a_2 + \cdots + (rr_n)a_n \in I'$ so I' is a left (and since each a_i is in the center of R, also a right) ideal of R. We have now that I' is an ideal of R which is a subset of any ideal containing X. Therefore, $I' = (X)$. □

Theorem III.2.6

Theorem III.2.6. Let $A_1, A_2, \ldots, A_n, B, C$ be left (respectively, right) ideals in a ring R.

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1A_2 \cdots A_n$ are left (respectively, right) ideals.

(ii) $(A + B) + C = A + (B + C)$.

(iii) $(AB)C = ABC = A(BC)$.

(iv) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$ and $(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots A_nC$.

Proof. **(i)** Let $a_1 + a_2 + \cdots + a_n, a_1' + a_2' + \cdots + a_n' \in A_1 + A_2 + \cdots A_n$. Then

$$(a_1+a_2+\cdots+a_n)-(a_1'+a_2'+\cdots+a_n') = a_1+a_2+\cdots+a_n-a_1'-a_2'-\cdots-a_n'$$

$$= (a_1 - a_1') + (a_2 - a_2') + \cdots + (a_n - a_n') \in A_1 + A_2 + \cdots A_n$$

since each A_i being an ideal, is a subring. Let $r \in R$. Then $r(a_1 + a_2 + \cdots + a_n) = (ra_1) + (ra_2) + \cdots + (ra_n) \in A_1 + A_2 + \cdots + A_n$ since each A_i is an ideal. By Theorem III.2.2, $A_1 + A_2 + \cdots A_n$ is an ideal.

Theorem III.2.6(i)

Theorem III.2.6. Let $A_1, A_2, \ldots, A_n, B, C$ be left (respectively, right) ideals in a ring R.

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1A_2 \cdots A_n$ are left (respectively, right) ideals.

Proof. **(i) (continued)** Let $a_1^1a_2^1 \cdots a_n^1 + a_1^2a_2^2 \cdots a_n^2 + \cdots a_1^\ell a_2^\ell + \cdots a_n^\ell, b_1^1b_2^1 \cdots b_n^1 + b_1^2b_2^2 \cdots b_n^2 + \cdots b_1^mb_2^m + \cdots + b_n^m \in A_1A_2 \cdots A_n$. Then

$$a_1^1a_2^1 \cdots a_n^1 + a_1^2a_2^2 \cdots a_n^2 + \cdots a_1^\ell a_2^\ell + \cdots + a_n^\ell$$

$$-(b_1^1b_2^1 \cdots b_n^1 + b_1^2b_2^2 \cdots b_n^2 + \cdots b_1^mb_2^m + \cdots + b_n^m)$$

$$= a_1^1a_2^1 \cdots a_n^1 + a_1^2a_2^2 \cdots a_n^2 + \cdots a_1^\ell a_2^\ell + \cdots + a_n^\ell$$

$$+(-b_1^1)b_2^1 \cdots b_n^1 + (-b_1^2)b_2^2 \cdots b_n^2 + \cdots + (-b_1^m)b_2^m + \cdots b_n^m)$$

$$\text{(since each } -b_1^i \in A_i\text{, since } A_i \text{ is a ring)}$$

$$\in A_1A_2 \cdots A_n (\text{a finite sum of products of elements of } A_1, A_2, \ldots, A_n).$$

Theorem III.2.6(i) (continued)

Theorem III.2.6. Let $A_1, A_2, \ldots, A_n, B, C$ be left (respectively, right) ideals in a ring R.

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are left (respectively, right) ideals.

Proof. (i) (continued) Let $r \in R$. Then

$$r(a_1^1 a_2^1 \cdots a_n^1 + a_1^2 a_2^2 \cdots a_n^2 + \cdots a_1^m a_2^m + \cdots + a_n^m)$$
$$= (ra_1^1)a_2^1 \cdots a_n^1 + (ra_1^2)a_2^2 \cdots a_n^2 + \cdots (ra_1^m)a_2^m + \cdots + a_n^m)$$
$$\in A_1 A_2 \cdots A_n \text{ since } A_1 \text{ is a left ideal.}$$

So by Theorem III.2.2, $A_1 A_2 \cdots A_n$ is a left ideal. □

Theorem III.2.7

Theorem III.2.7. Let R be a ring and I an ideal of R. Then the additive quotient group R/I is a ring with multiplication given by

$$(a + I)(b + I) = ab + I.$$

If R is commutative or has an identity, then the same is true of R/I.

Proof. First, we show that multiplication as defined is well-defined. Suppose we have the coset equivalences $a + I = a' + I$ and $b + I = b' + I$. Since $a' \in a' + I = a + I$ then $a' = a + i$ for some $i \in I$. Similarly $b' = b + j$ for some $j \in I$. Consequently $a'b' = (a + i)(b + j) = ab + ib + aj + ij$. Since I is an ideal,

$$a'b' - ab = (ab + ib + aj + ij) - ab = ib + aj + ij \in I.$$

Therefore $a'b' + I = ab + I$ (their difference is in I) by Corollary I.4.3(iii). So multiplication is well defined.

Theorem III.2.7 (continued)

Theorem III.2.7. Let R be a ring and I an ideal of R. Then the additive quotient group R/I is a ring with multiplication given by

$$(a + I)(b + I) = ab + I.$$

If R is commutative, then the same is true of R/I. If 1_R is the identity in R then $1_R + I$ is the identity in R/I.

Proof. (continued) Now we already know that $(R/I, +)$ is an abelian group by Note III.2.B. Since multiplication is defined in terms of representatives, associativity and distribution (and commutivity of multiplication, if present in R) follows from the corresponding properties in R. Hence R/I is a ring. □

Theorem III.2.8

Theorem III.2.8. If $f : R \to S$ is a homomorphism of rings then the kernel of f is an ideal in R. Conversely if I is an ideal in R then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is an onto homomorphism (epimorphism) of rings with kernel I.

Proof. By Theorem I.5.5 (restricting our attention to the additive groups corresponding to the rings), $\text{Ker}(f)$ is an additive subgroup of R. If $x \in \text{Ker}(f)$ and $r \in R$ then $f(rx) = f(r)f(x) = f(r)0 = 0$, whence $rx \in \text{Ker}(f)$. Similarly, of course, $xr \in \text{Ker}(f)$. Therefore $\text{Ker}(f)$ is an (two sided) ideal.

By Theorem I.5.5 the map π is an onto homomorphism (epimorphism) of groups with kernel I. Since $\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$ for all $a, b \in R$ then π is also an onto homomorphism of rings. □

Theorem III.2.15

Theorem III.2.15. If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$

$$ab \in P \text{ implies } a \in P \text{ or } b \in P \qquad (1)$$

then P is prime. Conversely if P is prime and R is commutative, then P satisfies condition (1).

Proof. Suppose P is an ideal, $P \neq R$, and (1) is satisfied. If A and B are ideals such that $AB \subset P$ and A is not a subset of P, then there exists an element $a \in A \setminus P$. For every $b \in B$, $ab \in AB \subset P$, whence by (1) $b \in P$ since $a \notin P$. So $B \subset P$. Therefore P is prime.
Conversely, suppose P is prime and R is commutative. Let $ab \in P$. Then the principal ideal (ab) is contained in P by Definition III.2.4. Since R is commutative, Theorem III.2.5(iii) implies that $(a)(b) \subset (ab)$, so we have $(a)(b) \subset P$. Since P is prime, then either $(a) \subset P$ or $(b) \subset P$. Ergo $a \in P$ or $b \in P$ and (1) follows. □

Theorem III.2.16

Theorem III.2.16. In a commutative ring R with identity $1_R \neq 0$, an ideal P is prime if and only if the quotient ring R/P is an integral domain.

Proof. Suppose P is a prime ideal. By Theorem III.2.7, R/P is commutative with (multiplicative) identity $1_R + P$ and "zero element" $0 + P = P$. Now if $1_R \in P$, then $P = R$ since P is an ideal of R. But by definition, a prime ideal is a proper subring, so $P \neq R$ and $1_R \notin P$. So $1_R + P \neq P$. Furthermore, R/P has no zero divisors since $(a+P)(b+P) = 0 + P = P$ implies $ab + P = P$ (by Theorem III.2.7) which implies $ab \in P$ and so $a \in P$ or $b \in P$ since P is prime. Therefore $a + P = 0 + P = P$ or $b + P = 0 + P = P$. Hence R/P is an integral domain.

Theorem III.2.16 (continued)

Theorem III.2.16. In a commutative ring R with identity $1_R \neq 0$, an ideal P is prime if and only if the quotient ring R/P is an integral domain.

Proof (continued). Conversely, suppose R/P is an integral domain. Then (by part of the definition of integral domain) $1_R + P \neq 0 + P = P$ so $1_R \notin P$. Therefore $P \neq R$. Since R/P is an integral domain then it has no zero divisors and so $ab \in P$ implies $ab + P = P$ which implies $(a+P)(b+P) = 0 + P = P$ (by Theorem III.2.7); so $a + P = 0 + P = P$ or $b + P = 0 + P = P$ since there are no zero divisors in R/P. Hence $a \in P$ or $b \in P$. Therefore, by Theorem III.2.15, P is a prime ideal. □

Theorem III.2.18

Theorem III.2.18. In a nonzero ring R with identity, maximal ideals always exist. In fact, every ideal in R (except R itself) is contained in a maximal ideal. This also holds for left ideals and right ideals.
Proof. Since $\{0\}$ is an ideal (the trivial ideal) and $\{0\} \neq R$, then if we show the second statement, we will know that $\{0\}$ lies in a maximal ideal and so "ideals always exist" (that is, the first statement follows). We apply Zorn's Lemma. For a given ideal A in R ($A \neq R$), let $\mathcal{S}$ be the set of all ideals B in R such that $A \subset B \neq R$. $\mathcal{S} \neq \varnothing$ since $A \in \mathcal{S}$. Partially order $\mathcal{S}$ by set theoretic inclusion. In order to apply Zorn's Lemma, we must show that every chain $\mathcal{C} = \{C_i \mid i \in I\}$ of ideals in $\mathcal{S}$ has an upper bound in $\mathcal{S}$. Let $C = \cup_{i \in I} C_i$. We claim that C is an ideal. If $a, b \in C$ then for some $i, j \in I$, $a \in C_i$, and $b \in C_j$. Since $\mathcal{C}$ is a chain then either $C_i \subset C_j$ or $C_j \subset C_i$ (say $C_j \subset C_i$). Hence $a, b \in C_i$ and since C_i is an ideal then $a - b \in C_i$ and $ra, ar \in C_i$ for all $r \in R$ by Theorem III.2.2. Therefore $a, b \in C$ implies $a - b$ and ra (and ar) are in $C_i \subset C$. Consequently C is an ideal by Theorem III.2.2.

Theorem III.2.18 (continued)

Theorem III.2.18. In a nonzero ring R with identity, maximal ideals always exist. In fact, every ideal in R (except R itself) is contained in a maximal ideal. This also holds for left ideals and right ideals.

Proof (continued). Since $A \subset C_i$ for every $i \in I$, then $A \subset \cup_{i \in I} C_i = C$. Since each $C_i \in \mathcal{S}$ then $C_i \neq R$ for all $i \in I$. Consequently $1_R \notin C_i$ for all $i \in I$ (otherwise, since C_i is a subring of R, $C_i = R$), whence $1_R \notin \cup C_i = C$. Therefore, $C \neq R$ and hence $C \in \mathcal{S}$. "Clearly" C is an upper bound for the chain $\mathcal{C}$. Thus every chain in $\mathcal{C}$ has an upper bound and the hypotheses of Zorn's Lemma are satisfied. Hence $\mathcal{S}$ contains a maximal element. This maximal element is a maximal ideal in R that contains A. The result is shown similarly for left and right ideals. □

Theorem III.2.19

Theorem III.2.19. If R is a commutative ring such that $RR = R^2 = R$ (in particular, if R has an identity) then every maximal ideal M in R is prime.

Proof. Suppose M is a maximal ideal. ASSUME M is not prime. Then by the contrapositive of the first claim of Theorem III.2.15, there exists $ab \in M$ where $a \notin M$ and $b \notin M$. Then each of the ideals $M + (a)$ and $M + (b)$ properly contain M (since $0, a \in (a)$ and $0, b \in (b)$). Since M is maximal, then $R = M + (a) = M + (b)$. Since R is commutative (and so the center of R is R itself) and $ab \in M$, then Theorem III.2.5(iii) gives $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$ and $(b) = \{rb + nb \mid r \in R, n \in \mathbb{Z}\}$; so the elements of $(a)(b)$ are of the form

$$(r_1a + na)(r_2b + nb) = r_1r_2ab + (nr_2)ab + (nr_1)ab + n^2ab$$

$$= (r_1r_2 + nr_1 + nr_2)ab + n^2ab \in \{rab + nab \mid r \in R, n \in \mathbb{Z}\} = (ab).$$

Theorem III.2.19 (continued)

Theorem III.2.19. If R is a commutative ring such that $RR = R^2 = R$ (in particular, if R has an identity) then every maximal ideal M in R is prime.

Proof (continued). That is, $(a)(b) \subset (ab) \subset M$. Therefore

$$R = R^2 = (M + (a))(M + (b)) = M^2 + (a)M + M(b) + (a)(b)$$

$$\subset M^2 + (a)M + M(b) + (ab) \subset M$$

(since M is an ideal $(a)M \subset M$ and $M(b) \subset M$). But $R \subset M$ contradicts the fact that M as a maximal ideal satisfies $M \neq R$, a CONTRADICTION. So the assumption that M is not prime is false and hence M is prime. □

Theorem III.2.20

Theorem III.2.20. Let M be an ideal in a ring R with identity $1_R \neq 0$.

(i) If M is maximal and R is commutative then the quotient ring R/M is a field.

(ii) If the quotient ring R/M is a division ring, then M is maximal.

Proof. (i) Suppose M is maximal and R is commutative. By Theorem III.2.19, M is prime (since R has an identity and hence $R^2 = R$), whence R/M is an integral domain by Theorem III.2.16. To show R/M is a field, we just need to show that nonzero cosets have multiplicative inverses in R/M. Let $a + M \neq 0 + M$. Then $a \notin M$, whence M is a proper subset of $M + (a)$ $(0 \in (a))$. Since M is maximal, we must have $M + (a) = R$. Since R is commutative, $1_R = m + ra$ for some $m \in M$ and $r \in R$ by Theorem III.2.5(v). Thus $1_R - ra = m \in M$; that is, 1_R and ra lie in the same coset of M. Whence $1_R + M = ra + M = (r + M)(a + M)$. Thus $r + M$ is the multiplicative inverse of $a + M$ in R/M. Therefore R/M is a field.

Theorem III.2.20 (continued)

Theorem III.2.20. Let M be an ideal in a ring R with identity $1_R \neq 0$.

(i) If M is maximal and R is commutative then the quotient ring R/M is a field.

(ii) If the quotient ring R/M is a division ring, then M is maximal.

Proof. (ii) Suppose R/M is a division ring. Then $1_R + M \neq 0 + M = M$ by Definition III.1.5 of division ring. Whence $1_R \notin M$ and so $M \neq R$. If N is an ideal such that $M \subset N$, $M \neq N$, then let $a \in N \setminus M$. Then $a + M$ has a multiplicative inverse in R/M (since R/M is a division ring), say $(a+M)(b+M) = 1_R + M$. Consequently $ab + M = 1_R + M$ and $ab - 1_R = c \in M$. Since $a \in N$ and N is an ideal, then $ab \in N$. Since $M \subset N$ then $ab - 1_R \in N$. Since ideals are subrings then $(ab - 1_R) - ab = -1_R \in N$ and $1_R \in N$. Then $N = R$ and so M is maximal. □

Corollary III.2.21

Corollary III.2.21. The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent.

(i) R is a field.

(ii) R has no proper ideals.

(iii) $\{0\}$ is a maximal ideal in R.

(iv) Every nonzero homomorphism of rings $R \to S$ is injective (a "monomorphism").

Proof. Now $R \cong R/\{0\}$ is a field if and only if $\{0\}$ is a maximal ideal by Theorem III.2.20 so (i) and (iii) are equivalent. Next, $\{0\}$ is a maximal ideal if and only if R has no proper ideals, so (ii) and (iii) are equivalent. Finally, for every ideal I, with $I \neq R$, the canonical map $\pi : R \to R/I$ is a nonzero homomorphism with kernel I by Theorem III.2.8. Since π is one to one if and only if $\mathrm{Ker}(\pi) = I = \{0\}$ by Theorem I.2.3(i), then (iv) holds for the canonical homomorphism if and only if R has no proper ideals.

Corollary III.2.21 (continued)

Corollary III.2.21. The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent.

(i) R is a field.

(ii) R has no proper ideals.

(iii) $\{0\}$ is a maximal ideal in R.

(iv) Every nonzero homomorphism of rings $R \to S$ is injective (a "monomorphism").

Proof (continued). Now any homomorphism $h : R \to S$ can be expressed in terms of the canonical homomorphism since with $I = \mathrm{Ker}(h)$ as:

$$R \xrightarrow{\pi} R/I \cong \mathrm{Im}(h) \subset S, \qquad h : R \to \mathrm{Im}(h)$$

So (ii) and (iv) are equivalent. □

Theorem III.2.23

Theorem III.2.23. Let $\{R_i \mid i \in I\}$ be a nonempty family of rings S a ring and $\{\varphi_i : S \to R_i \mid i \in I\}$ 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 $\pi_i\varphi = \varphi_i$ for all $i \in I$ where π_i is the canonical projection of Theorem III.2.22. 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 there is a unique homomorphism of groups $\varphi : S \to \prod_{i\in I} R_i$ such that $\pi_i\varphi = \varphi_i$ for all $i \in I$. Let $s_1, s_2 \in S$. Then

$$\begin{aligned} \pi_i\varphi(s_1s_2) &= \varphi_i(s_1s_2) \\ &= \varphi_i(s_1)\varphi_i(s_2) \text{ since } \varphi_i \text{ is a ring homomorphism} \\ &= \pi_i\varphi(s_1)\pi_2\varphi(s_2) \text{ for all } i \in I. \end{aligned}$$

So $\varphi(s_1s_2) = \varphi(s_1)\varphi(s_2)$. Thus $\prod_{i\in I} R_i$ is a product in the category of rings (see Definition I.7.2; the morphisms π_i are the canonical projections and φ is the unique morphism). By Theorem I.7.3, the product is determined up to isomorphism. □

Theorem III.2.24

Theorem III.2.24. Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that

(i) $A_1 + A_2 + \cdots + A_n = R$, and

(ii) for each k, with $1 \le k \le n$,
$A_k \cap (A_1 + A_2 + \cdots + A_{k-1} + A_{k+1} + \cdots A_n) = \{0\}$.

Then there is a ring isomorphism $R \cong A_1 \times A_2 \times \cdots \times A_n$.

Proof. In the proof of Theorem I.8.6 it is shown that the map $\varphi : A_1 \times A_2 \times \cdots \times A_n \to R$ given by $(a_1, a_2, \ldots, a_n) \mapsto a_1 + a_2 + \cdots + a_n$ is an isomorphism of additive groups. We need only verify the homomorphism property for multiplication. Observe that if $i \ne j$ and $a_i \in A_i$, $a_j \in A_j$ then by (ii) $a_i a_j \in A_i \cap A_j = \{0\}$ implies such $a_i a_j = 0$. So

$$\varphi((a_1, a_2, \ldots, a_n))\varphi((b_1, b_2, \ldots, b_n)) = (a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n)$$

$$= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n = \varphi((a_1 b_a, a_2 b_2, \ldots, a_n b_n)).$$

So φ is a ring homomorphism and since it is one to one and onto (as a group isomorphism), φ is a ring isomorphism. □

Theorem III.2.25, Chinese Remainder Theorem

Theorem III.2.25. Chinese Remainder Theorem.
Let $A_1, A_2, \ldots, A_n$ be ideals in a ring R such that $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \ne j$. If $b_1, b_2, \ldots, b_n \in R$, then there exists $b \in R$ such that

$$b \equiv b_i (\text{mod } A_i) \text{ for } i = 1, 2, \ldots, n.$$

Furthermore, b is uniquely determined up to congruence modulo the ideal

$$A_1 \cap A_2 \cap \cdots \cap A_n.$$

Proof. Since $A_1 + A_2 = A_1 + A_3 = R$ then

$$\begin{aligned} R^2 &= (A_1 + A_2)(A_1 + A_2) - A_1^2 + A_1 A_3 + A_2 A_1 + A_2 A_3 \\ &\subset A_1 + A_2 A_3 \text{ since } A_1^2 \subset A_1 \text{ and } A_1 A_3 \subset A_1,\ A_2 A_1 \subset A_1 \\ &\qquad \text{since } A_1 \text{ is an ideal} \\ &\subset A_1 + (A_2 \cap A_3) \text{ since } A_2 A_3 \subset A_2 \text{ and } A_2 A_3 \subset A_3 \\ &\qquad \text{since } A_2 \text{ and } A_3 \text{ are ideals.} \end{aligned}$$

Theorem III.2.25, Chinese Remainder Theorem (continued 1)

Proof (continued). Consequently, since $R = A_1 + R^2$, $R = A_1 + R^2 \subset A_1 + (A_2 + (A_2 \cap A_3)) = A_1 + (A_1 \cap A_3) \subset R$. Therefore $R = A_1 + (A_2 \cap A_3)$. We now apply mathematical induction. Suppose $R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1})$. Then

$$\begin{aligned} R^2 &= (A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1}))(\underbrace{A_1 + A_k}_{=R \text{ by hypothesis}}) \\ &= A_1^2 + (A_2 \cap A_3 \cap \cdots A_{k-1})A_1 + A_1 A_k + (A_2 \cap A_3 \cap \cdots A_{k-1})A_k \\ &\subset A_1 + (A_2 \cap A_3 \cdots \cap A_{k-1} \cap A_k) \text{ as above.} \end{aligned}$$

So

$$\begin{aligned} R &= R^2 + A_1 \text{ by hypothesis} \\ &\subset A_1 + (A_2 \cap A_3 \cap \cdots \cap A_k) \subset R. \end{aligned}$$

Theorem III.2.25, Chinese Remainder Theorem (continued 2)

Proof (continued). Therefore $R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_k)$ and the induction step holds. So $R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_n)$. A similar argument holds for each $k = 1, 2, \ldots, n$ to give $R = A_k + (\cap_{i \ne k} A_i)$. Consequently for each k there exists $a_k \in A_k$ and $r_k \in \cap_{i \ne k} A_k$ such that $b_k = a_k + r_k$ (for the given b_k's). Furthermore, since $b_k - r_k = a_k \in A_k$ and $r_i \in A_i$ for $i \ne k$ then $r_k \equiv b_k$ (mod A_k) and $r_k \equiv 0$ (mod A_i) for $i \ne k$. Let $b = r_1 + r_2 + \cdots + r_n$. Then $b \equiv b_i$ (mod A_i) since $r_k \equiv 0$ (mod A_i) for $i \ne k$. Finally, if $c \in R$ is such that $c \equiv b_i$ (mod A_i) for every i then $b \equiv c$ (mod A_i) for each i whence $b - c \in A_i$ for each i. Therefore $b - c \in \cap_{i=1}^n A_i$ and $b \equiv c$ (mod $\cap A_i$). So b is unique up to congruence as claimed. □

Corollary III.2.26

Corollary III.2.26. Let $m_1, m_2, \ldots, m_n$ be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$. If $b_1, b_2, \ldots, b_n$ are any integers, then the system of congruences

$$x \equiv b_1 (\text{mod } m_1),\ x \equiv b_2 (\text{mod } m_2), \ldots,\ x \equiv b_n (\text{mod } m_n)$$

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

Proof. Let $R = \mathbb{Z}$.
Let $A_i = (m_i)$. Then $\cap_{i=1}^n A_i = (m)$. Since $(m_i, m_j) = 1$ then by Theorem 0.6.5 there are integers k_i and k_j such that $(m_i, m_j) = 1 = k_i m_i + k_j m_j$. So $1 \in A_i + A_j$ and hence $A_i + A_j = \mathbb{Z}$. Notice that $R^2 = \mathbb{Z}^2 = \mathbb{Z}$ since $\mathbb{Z}$ has unity 1 and so $R^2 + A_i = R$ since $0 \in A_i$. So by Theorem III.2.25, b exists as claimed. □

Corollary III.2.27

Corollary III.2.27. If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then there is a monomorphism of rings

$$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n.$$

If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$, then θ is an isomorphism of rings.

Proof. Consider the family of (onto) homomorphisms $\pi_k : R \to R/A_k$ (the canonical homomorphisms) for $k = 1, 2, \ldots, n$. By Theorem III.2.23, this family induces a homomorphism of rings $\theta_1 : R \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$ with $\theta_1(r) = (r + A_1, r + A_2, \ldots, r + A_n)$. Now $\text{Ker}(\theta_1)$ consists of those elements of R mapped to the additive identity $(0 + A_1) \times (0 + A_2) \times \cdots \times (0 + A_n) = A_1 \times A_2 \times \cdots \times A_n$; so $\text{Ker}(\theta_1) = A_1 \cap A_2 \cap \cdots \cap A_n$.

Corollary III.2.27 (continued 1)

Corollary III.2.27. If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then there is a monomorphism of rings

$$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n.$$

If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$, then θ is an isomorphism of rings.

Proof (continued). With $I = A_1 \cap A_2 \cap \cdots \cap A_n$ as an ideal which is a subset of $\text{Ker}(\theta_1)$, by Theorem III.2.9 there is a homomorphism $\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$ where $\theta(a + I) = \theta_1(a) = (a + A_1, a + A_2, \ldots, a + A_n)$. Notice $\text{Ker}(\theta) = I$, so θ is one to one (a monomorphism). However, θ may no be onto ("surjective"; see Exercise III.2.26). So the first claim holds.

Corollary III.2.27 (continued 2)

Corollary III.2.27. If $A_1, A_2, \ldots, A_n$ are ideals in a ring R, then there is a monomorphism of rings

$$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n.$$

If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$, then θ is an isomorphism of rings.

Proof (continued). For the second claim, the hypothesis of Theorem III.2.25 are satisfied, so for any $(b_1 + A_1, b_2 + A_2, \ldots, b_n + A_n) \in R/A_1 \times R/A_2 \times \cdots \times R/A_n$, there exists $b \in R$ such that $b \equiv b_i \ (\text{mod } A_i)$ for all i. Thus

$$\begin{aligned} \theta(b + \cap A_i) &= (b + A_1, b + A_2, \ldots, b + A_n) \\ &= (b_1 + A_1, b_2 + A_2, \ldots, b_n + A_n) \\ &\quad \text{by the congruence } b \equiv b_i \ (\text{mod } A_i) \end{aligned}$$

and so θ is onto $R/A_1 \times R/A_2 \times \cdots \times R/A_n$. So θ is, as claimed, as isomorphism. □