Exercise 13.4. List all zero-divisors of $\mathbb{Z}_{20}$. Can you see a relationship between the zero-divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?

Solution. By definition zero-divisor, we wish to find all $a_{\neq 0} \in R = \mathbb{Z}_{20}$ such that $\exists b_{\neq 0} \in R$ where $ab \equiv 0 \pmod{20}$. That is, we wish to find all $a_{\neq 0} \in R$ such that $ab = 20n$ for some $n \in \mathbb{Z}$ where $b_{\neq 0} \in R$. We can rewrite this as

$$ab = 20n \quad \Longrightarrow \quad \frac{ab}{20} = n.$$

Suppose a is coprime to 20. Then by definition coprime, a and 20 share no common factors. So $2 \nmid a$ and $5 \nmid a$ which implies $2p + 5q \nmid a \; \forall p, q \in \mathbb{Z}$. That is, a is not divisible by any linear combination of 2 and 5 with integer coefficients, and consequently by any divisor (nor by any multiple) of 20. We know a is an integer, so

$$n = \frac{ab}{20} = a \cdot \frac{b}{20} \in \mathbb{Z} \quad \Longleftrightarrow \quad \frac{b}{20} \in \mathbb{Z}.$$

Then $b \equiv 0 \pmod{20}$, but $b \not\equiv 0$ by definition b ($\Rightarrow\Leftarrow$). Thus a must not be coprime to 20.

Suppose a is *not* coprime to 20. Then by definition coprime, a shares at least one common factor with 20. Let this factor be p. Then $a = pq$ and $20 = pr$ for some $q, r \in \mathbb{Z}_{20}$. Suppose $b = r$. Then,

$$ab = 20n \quad \Longleftrightarrow \quad pqr = prn \quad \Longleftrightarrow \quad r = n.$$

We know $r \in \mathbb{Z}$, so all numbers not coprime to 20 in $\mathbb{Z}_{20}$ are zero-divisors.

So we have that a coprime to 20 $\Longrightarrow a$ not zero-divisor and a not coprime to 20 $\Longrightarrow a$ is zero-divisor. That is, $a \in \mathbb{Z}_{20}$ is a zero divisor $\Longleftrightarrow a$ is not coprime to 20. Thus the set of all zero divisors of $\mathbb{Z}_{20}$ is {2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18}.

The set of zero-divisors of $\mathbb{Z}_{20}$ and the set of units of $\mathbb{Z}_{20}$ are disjoint and form a partition of $\mathbb{Z}_{20}$. □

Exercise 13.24. Find a zero-divisor in $\mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5\}$.

Solution. Let $R = \mathbb{Z}_5[i]$. By definition zero-divisor, $r_{\neq 0} \in R$ is a zero-divisor of R if there exists some $s_{\neq 0} \in R$ such that $rs \equiv 0 \pmod 5$. Consider the elements $r = 2 + i$ and $\overline{r} = 2 - i$. Notice

$$rs = (2 + i)(2 - i) = 4 - 2i + 2i + 1 = 5 + 0i \equiv 0 \pmod 5.$$

Thus r is a zero-divisor of $\mathbb{Z}_5[i]$. □

Exercise 13.30. Let d be a positive integer. Prove that $[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in\}$ is a field.

Solution. Viewed as an element of $\mathbb{R}$, the multiplicative inverse of any element of the form $a + b\sqrt{d}$ is $1/(a + b\sqrt{d})$. To verify that $[\sqrt{d}]$ is a field, we must show $1/(a + b\sqrt{d})$ can be written in the form $\alpha + \beta\sqrt{d}$. Observe that

$$\frac{1}{a + b\sqrt{d}} = \frac{1}{a + b\sqrt{d}} \cdot \frac{a - b\sqrt{d}}{a - b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - ab\sqrt{d} + ab\sqrt{d} - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d}.$$

Thus $[\sqrt{d}]$ is a field. □

Exercise 13.31. Let R be a ring with unity 1. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies $ba = 1$.

Solution. We have that $a_{\neq 0}, b_{\neq 0} \in R \implies ab \neq 0$. Suppose $ab = 1$. Then

$$\begin{aligned} ab &= 1 \\ aba &= a \\ aba - a &= 0 \\ a(ba - 1) &= 0 \end{aligned}$$

Notice that a is nonzero, so $ba - 1 = 0$ and thus $ba = 1$. □

Exercise 13.32. Let $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field.

Solution. By definition field, we need only verify each nonzero element of R has a multiplicative inverse. The nonzero elements of R are $\{2, 4, 6, 8\}$. By Exercise 12.2, we know the unity of R is 6. Thus, we must find some $b \in R$ for each $a \in \mathbb{R}$ such that $ab = 6$. Then, we can see that

$$\begin{aligned} 2 \cdot 8 = 16 \equiv 6 \pmod{10}, &\qquad 4 \cdot 4 = 16 \equiv 6 \pmod{10}, \\ 6 \cdot 6 = 36 \equiv 6 \pmod{10}, &\qquad 8 \cdot 2 = 16 \equiv 6 \pmod{10}. \end{aligned}$$

Thus R is a field. □

Exercise 13.42. Construct a multiplication table for $\mathbb{Z}_2[i]$, the ring of Gaussian integers modulo 2. Is this ring a field? Is it an integral domain?

Solution. We know $\mathbb{Z}_2[i] = \{a + bi \mid a, b \in \mathbb{Z}_2\} = \{0, i, 1, 1 + i\}$

Then the multiplication table is

	0	i	1	$1+i$
0	0	0	0	0
i	0	1	i	$1+i$
1	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

Since $(1 + i)^2 = 0$, it is a zero-divisor of $\mathbb{Z}_2[i]$ by definition zero-divisor. Thus $\mathbb{Z}_2[i]$ is not an integral domain by definition integral domain. Thus $\mathbb{Z}_2[i]$ is not a field by definition field. □

Exercise 13.43. The nonzero elements of $\mathbb{Z}_3[i]$ form an abelian group of order 8 under multiplication. Is it isomorphic to $\mathbb{Z}_8,\ \mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

Solution. We know

$$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\} = \{0, i, 2i, 1, 1 + i, 1 + 2i, 2, 2 + i, 2 + 2i\},$$

so let $G = \{i, 2i, 1, 1 + i, 1 + 2i, 2, 2 + i, 2 + 2i\}$. By thm, a group isomorphism must preserve the order of elements of the group. Thus we can test the orders of the elements of G to find an isomorphism. Consider the element $\alpha = 1 + i$. Notice, $(1 + i)^2 = 2i \equiv -i \pmod 3$, so $(1 + i)^4 = -1$ and $|\alpha|$ has order 8. By thm, the order of an element of an external direct product is the LCM of the orders of the elements. Then $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ can not have any elements of order 8, but $\mathbb{Z}_8$ can. Thus the set of nonzero elements of $\mathbb{Z}_3[i]$ is isomorphic to $\mathbb{Z}_8$. □

Note (Notation). I will use $\leq$ to denote subring and $\trianglelefteq$ for ideal.

Exercise 14.4. Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Solution. Consider the set $R = \{(x, x) \mid x \in \mathbb{Z}\}$. Notice

$$(\alpha, \alpha) - (\beta, \beta) = (\alpha - \beta, \alpha - \beta) \in R \tag{1}$$

$$(\alpha, \alpha) \cdot (\beta, \beta) = (\alpha\beta, \alpha\beta) \in R, \tag{2}$$

so $R \leq \mathbb{Z} \oplus \mathbb{Z}$ by the subring test. Consider the elements $a = (\alpha, \alpha) \in R$ and $r = (\beta, \gamma) \in \mathbb{Z} \oplus \mathbb{Z}$ such that $\beta \neq \gamma$. Then,

$$ar = (\alpha, \alpha) \cdot (\beta, \gamma) = (\alpha\beta, \alpha\gamma).$$

We know $\beta \neq \gamma$, so $\alpha\beta \neq \alpha\gamma$. Then $(\alpha\beta, \alpha\gamma) \notin R$ whence $R \ntrianglelefteq \mathbb{Z} \oplus \mathbb{Z}$ by the ideal test. □

Exercise 14.6. Find all maximal ideals in
a. $\mathbb{Z}_8$ **b.** $\mathbb{Z}_{10}$ **c.** $\mathbb{Z}_{12}$ **d.** $\mathbb{Z}_n$

Solution. **a.** $\mathbb{Z}_8$
The proper ideals of $\mathbb{Z}_8$ are $\triangleleft 0 = \{0\}$, $\triangleleft 2 = \{0, 2, 4, 6\}$, and $\triangleleft 4 = \{0, 4\}$. Since $\triangleleft 0 \subset \triangleleft 4 \subset \triangleleft 2 \subset \mathbb{Z}_8$, $\triangleleft 2$ is the only maximal ideal of $\mathbb{Z}_8$.

b. $\mathbb{Z}_{10}$
The proper ideals of $\mathbb{Z}_{10}$ are $\triangleleft 0 = \{0\}$, $\triangleleft 2 = \{0, 2, 4, 6, 8\}$, and $\triangleleft 5 = \{0, 5\}$. Since $\triangleleft 0 \subset \triangleleft 5, \triangleleft 2 \subset \mathbb{Z}_{10}$, $\triangleleft 2$ and $\triangleleft 5$ are the only maximal ideals of $\mathbb{Z}_{10}$.

c. $\mathbb{Z}_{12}$
The proper ideals of $\mathbb{Z}_{12}$ are $\triangleleft 0 = \{0\}$, $\triangleleft 2 = \{0, 2, 4, 6, 8, 10\}$, $\triangleleft 3 = \{0, 3, 6, 9\}$, $\triangleleft 4 = \{0, 4, 8\}$, and $\triangleleft 6 = \{0, 6\}$. Notice $\triangleleft 0 \subset \triangleleft 4 \subset \triangleleft 2 \subset \mathbb{Z}_{12}$ and $\triangleleft 0 \subset \triangleleft 6 \subset \triangleleft 3 \subset \mathbb{Z}_{12}$. Thus $\triangleleft 2$ and $\triangleleft 3$ are the only maximal ideals of $\mathbb{Z}_{12}$.

d. $\mathbb{Z}_n$
Suppose the prime factorization of n is $n = \prod_{i=1}^{m} p_i^{k_i}$. I claim[1] the only maximal ideals of $\mathbb{Z}_n$ are $\triangleleft p_1, \triangleleft p_2, \ldots, \triangleleft p_m$, the principal ideals generated by the prime factors of n.

Claim 1. First, I claim[2] that the factor ring $\mathbb{Z}_n / \triangleleft d$ is isomorphic to $\mathbb{Z}_{n/d}$.

Claim 2. By definition isomorphism, we must show there exists a bijective homomorphism $\phi : \mathbb{Z}_n / \triangleleft d \to \mathbb{Z}_{n/d}$. Consider the mapping $\phi : \mathbb{Z}_n / \triangleleft d \to \mathbb{Z}_{n/d}$ such that $\phi(a + \triangleleft d) = a \mod \frac{n}{d}$. By definition homomorphism, we must show that $\phi(a) + \phi(b) = \phi(a + b)$. Consider the elements $a + \triangleleft d, b + \triangleleft d \in \mathbb{Z}_n / \triangleleft d$. Then

$$\begin{aligned} \phi(a) + \phi(b) &= \left(a \mod \frac{n}{d}\right) + \left(b \mod \frac{n}{d}\right) \\ &= (a + b) \mod \frac{n}{d} \\ &= \phi(a + b). \end{aligned}$$

Thus ϕ is a homomorphism. To show ϕ is bijective, we must show ϕ is both injective and surjective.

To see that ϕ is surjective, we must ensure every element in $\mathbb{Z}_{n/d}$ is mapped to by some element in $\mathbb{Z}_n / \triangleleft d$. Consider any $c \in \mathbb{Z}_{n/d}$. Then, let $a \in \mathbb{Z}_n$ such that $a \mod d = a \mod \frac{n}{d} = c$. Then $\phi(a + \triangleleft d) = a \mod \frac{n}{d} = c$. Thus ϕ is surjective.

To see that ϕ is injective, suppose we have $a + \lhd d, b + \lhd d \in \mathbb{Z}_n \,/\, \lhd\, d$ such that $\phi(a + \lhd d) = \phi(b + \lhd d)$. Then,

$$\phi(a + \lhd d) = \phi(b + \lhd d) \iff a \mod \frac{n}{d} = b \mod \frac{n}{d} \iff a \equiv b \pmod{\frac{n}{d}} \iff a \equiv b \pmod{d}$$

We know it is a property of cosets that $aH = bH \iff a \in bH$. Thus,

$$a + \lhd d = b + \lhd d \iff a \in b + \lhd d \iff a = b + dx,\ x \in \mathbb{Z}_n \iff a \equiv b \pmod{d}$$

Thus $\phi(a + \lhd d) = \phi(b + \lhd d) \iff a + \lhd d = b + \lhd d$ implies ϕ is injective, whence ϕ is an isomorphism from $\mathbb{Z}_n \,/\, \lhd\, d$ to $\mathbb{Z}_{n/d}$. ■

By Example 13.6 and Corollary 13.2.1, the ring $\mathbb{Z}_{n/d} \cong (\mathbb{Z}_n \,/\, \lhd\, d)$ is a field $\iff \frac{n}{d}$ is prime. By Theorem 14.4, the factor ring $\mathbb{Z}_n \,/\, \lhd\, d$ is a field $\iff \lhd d$ is a maximal ideal of $\mathbb{Z}_n$. Thus, $\lhd d$ is a maximal ideal of $\mathbb{Z}_n \iff \frac{n}{d}$ is prime. ■

□

Exercise 14.10. If A and B are ideals of a ring, show that the *sum* of A and B, $A+B = \{a+b \mid a \in A, b \in B\}$, is an ideal.

Solution. Let A and B be ideals of some ring R. By definition ideal, $ra, ar \in A$ for any $a \in A$, $r \in R$. Similarly $rb, br \in B$ for any $b \in B$, $r \in R$. Consider the element $a + b \in A + B$ and pick any $r \in R$. Then $r(a + b) = ra + rb$ and $(a + b)r = ar + br$ by properties of multiplication. Since $ra \in A$ and $rb \in B$, $ra + rb \in A + B$. Similarly, $ar + br \in A + B$. Thus $A + B$ is an ideal of R by def ideal. □

Exercise 14.11. In the ring of integers, find a positive integer a such that

a. $\lhd a = \lhd 2 + \lhd 3$

b. $\lhd a = \lhd 6 + \lhd 8$

c. $\lhd a = \lhd m + \lhd n$

Solution. **a.** $\lhd a = \lhd 2 + \lhd 3$

By definition of principal ideal, $\lhd 2 = \{2k \mid k \in \mathbb{Z}\}$ and $\lhd 3 = \{3k \mid k \in \mathbb{Z}\}$. So any element $\gamma \in \lhd 2 + \lhd 3$ must be of the form $\gamma = 2\alpha + 3\beta$, where $\alpha, \beta \in \mathbb{Z}$. We know 2 and 3 are both prime and are thus relatively prime, so by Bezout's Identity there exist integers s, t such that $2s + 3t = 1$. Notice that for any $k \in \mathbb{Z}$,

$$k = k(2s + 3t) = 2ks + 3kt$$

by properties of multiplication. Thus we can generate any integer k by letting $\alpha = ks$ and $\beta = kt$. Thus $\lhd 2 + \lhd 3 = \mathbb{Z} = \lhd 1$ and $a = 1$.

b. $\lhd a = \lhd 6 + \lhd 8$

By definition of principal ideal, $\lhd 6 = \{6k \mid k \in \mathbb{Z}\}$ and $\lhd 8 = \{8k \mid k \in \mathbb{Z}\}$. So any element $\gamma \in \lhd 6 + \lhd 8$ must be of the form $\gamma = 6\alpha + 8\beta$, where $\alpha, \beta \in \mathbb{Z}$. Notice that while 6 and 8 are not relatively prime,

$$\gamma = 6\alpha + 8\beta = 2(3\alpha + 4\beta)$$

where $3\alpha + 4\beta \in \lhd 3 + \lhd 4$. Let us momentarily switch our attention to finding some b such that $\lhd b = \lhd 3 + \lhd 4$. Since 3 and 4 are relatively prime, we can the same logic as in part a to find that $\lhd b = \lhd 1$. Thus, $\lhd 6 + \lhd 8 = 2\mathbb{Z} = \lhd 2$ and $a = 2$.

c. $\lhd a = \lhd m + \lhd n$

By definition of principal ideal, $\lhd m = \{mk \mid k \in \mathbb{Z}\}$ and $\lhd n = \{nk \mid k \in \mathbb{Z}\}$. So any element $\gamma \in \lhd m + \lhd n$ must be of the form $\gamma = m\alpha + a\beta$, where $\alpha, \beta \in \mathbb{Z}$. If m and n relatively prime, then we can follow the proof of part a and we are done. Suppose m and n are *not* relatively prime. That is, $\gcd(m, n) = d > 1$. So any element $\gamma \in \lhd m + \lhd n$ must be of the form $\gamma = m\alpha + n\beta$. Notice that

$$\gamma = m\alpha + n\beta = d\left(\frac{m}{d}\alpha + \frac{n}{d}\beta\right),$$

where $\frac{m}{d}$ and $\frac{n}{d}$ have no common divisors by definition of GCD and are thus coprime. Thus by part a, $\lhd\frac{m}{d} + \lhd\frac{n}{d} = \lhd 1 = \mathbb{Z}$. Thus $\lhd m + \lhd n = d\mathbb{Z} = \lhd d$ and $a = d = \gcd(m, n)$.

□

Exercise 14.12. If A and B are ideals of a ring, show that the *product* of A and B, $AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in A, b_i \in B, n \in \mathbb{Z}_{>0}\}$, is an ideal.

Solution. Let A and B be ideals of some ring R. To show $AB = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}_{>0}\}$ is an ideal of R, we use the ideal test. Suppose we have some $x, y \in AB$. By def AB,

$$x = \sum_{i=1}^{n} a_i b_i \qquad y = \sum_{j=1}^{m} a'_j b'_j,$$

where $a_i, a'_j \in A$ and $b_i, b'_j \in B$. Since x and y are arbitrary, let $n < m$. Then,

$$\begin{aligned} x - y &= \sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} a'_j b'_j \\ &= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n - a'_1 b'_1 - a'_2 b'_2 - \cdots - a_m b_m \\ &= (a_1 b_1 - a'_1 b'_1) + (a_2 b_2 - a'_2 b'_2) + \cdots + (a_n b_n - a_n b_n) - a'_{n+1} b'_{n+1} - \cdots - a'_m b'_m \\ &= \sum_{i=1}^{n} (a_i + a'_i)(b_i - b'_i) - \sum_{j=n+1}^{m} a'_j b'_j. \end{aligned}$$

Since A and B are ideals, they are closed under addition/subtraction and we can write $a_i + a'_i = a''_i \in A$ and $b_i - b'_i = b''_i \in B$. Then,

$$\begin{aligned} x - y &= \sum_{i=1}^{n} a''_i b''_i - \sum_{j=n+1}^{m} a'_j b'_j \\ &= \sum_{i=1}^{n} a''_i b''_i + \sum_{j=n+1}^{m} (-a'_j) b'_j \in AB. \end{aligned}$$

Thus AB is closed under subtraction. Let $x \in AB$ and $r \in R$. By definition,

$$x = \sum_{i=1}^{n} a_i b_i,$$

where $a_i \in A$ and $b_i \in B$. Since A and B are ideals, $r a_i = \overline{a_i} \in A$ and $b_i r = \overline{b_i} \in B$ for all $r \in R$ by definition ideal. Then,

$$\begin{aligned} rx &= r\left(\sum_{i=1}^{n} a_i b_i\right) = \sum_{i=1}^{n} r a_i b_i = \sum_{i=1}^{n} \overline{a_i} b_i \in AB \\ xr &= \left(\sum_{i=1}^{n} a_i b_i\right) r = \sum_{i=1}^{n} a_i b_i r = \sum_{i=1}^{n} a_i \overline{b_i} \in AB. \end{aligned}$$

So $rx, xr \in AB$ for every $x \in AB$ and every $r \in R$. Thus AB is an ideal of R by the ideal test. □

Exercise 14.13. Find a positive integer a such that

a. $\triangleleft a = \triangleleft 3 \triangleleft 4$

b. $\triangleleft a = \triangleleft 6 \triangleleft 8$

c. $\triangleleft a = \triangleleft m \triangleleft n$

Solution. **a.** $\triangleleft a = \triangleleft 3 \triangleleft 4$

Elements of $\triangleleft 3 \triangleleft 4$ are of the form

$$\sum_{i=1}^{n} 3\alpha_i 4\beta_i = \sum_{i=1}^{n} 12\alpha_i\beta_i = 12\sum_{i=1}^{n} \alpha_i\beta_i = 12s \in \triangleleft 12,$$

where $\alpha_i, \beta_i \in \mathbb{Z}$ and $s = \sum_{i=1}^{n} \alpha_i\beta_i$. So, $\triangleleft 3 \triangleleft 4 \subseteq \triangleleft 12$. Also since $12 \in \triangleleft 3 \triangleleft 4$, we have that $\triangleleft 12 \subseteq \triangleleft 3 \triangleleft 4$. Thus $\triangleleft 3 \triangleleft 4 = \triangleleft 12$ and $a = 12$.

b. $\triangleleft a = \triangleleft 6 \triangleleft 8$
Elements of $\triangleleft 6 \triangleleft 8$ are of the form

$$\sum_{i=1}^{n} 6\alpha_i 8\beta_i = \sum_{i=1}^{n} 48\alpha_i\beta_i = 48\sum_{i=1}^{n} \alpha_i\beta_i = 48s \in \triangleleft 48,$$

where $\alpha_i, \beta_i \in \mathbb{Z}$ and $s = \sum_{i=1}^{n} \alpha_i\beta_i$. So, $\triangleleft 6 \triangleleft 8 \subseteq \triangleleft 48$. Also since $48 \in \triangleleft 6 \triangleleft 8$, we have that $\triangleleft 48 \subseteq \triangleleft 6 \triangleleft 8$. Thus $\triangleleft 6 \triangleleft 8 = \triangleleft 48$ and $a = 48$.

c. $\triangleleft a = \triangleleft m \triangleleft n$
Elements of $\triangleleft m \triangleleft n$ are of the form

$$\sum_{i=1}^{n} m\alpha_i n\beta_i = \sum_{i=1}^{n} mn\alpha_i\beta_i = mn\sum_{i=1}^{n} \alpha_i\beta_i = mns \in \triangleleft mn,$$

where $\alpha_i, \beta_i \in \mathbb{Z}$ and $s = \sum_{i=1}^{n} \alpha_i\beta_i$. So, $\triangleleft m \triangleleft n \subseteq \triangleleft mn$. Also since $mn \in \triangleleft m \triangleleft n$, we have that $\triangleleft mn \subseteq \triangleleft m \triangleleft n$. Thus $\triangleleft m \triangleleft n = \triangleleft mn$ and $a = mn$.

□

Exercise 14.14. Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Solution. Let A and B be ideals of a ring R. Let $x \in AB$. By definition of AB, we can write

$$x = \sum_{i=1}^{n} a_i b_i,$$

where $a_i \in A$ and $b_i \in B$. We wish to show $x \in A$ and $x \in B$. Since A and B are ideals of R, $\alpha \in R$ for all $\alpha \in A$ and likewise for B. Then each term $a_i b_i$ can be written $a_i r$ or $r b_i$ where $r \in R$. By def ideal, $a_i r \in A$ and $r b_i \in B$. Also by def ideal, A and B are closed under addition. Thus $x \in A$ and $x \in B$ and $x \in A \cap B$. Thus $AB \subseteq A \cap B$. □