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 def 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 def 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 def b ($\Rightarrow\!\Leftarrow$). Thus a must not be coprime to 20.

Suppose a is *not* coprime to 20. Then by def 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 $\mathbb{Z}_{20}$. $\square$

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 def 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 $\mathbb{Z}_5[i]$. $\square$

Exercise 13.30. Let d be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ 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 $\mathbb{Q}[\sqrt{d}]$ is a field, we must show $1/(a + b\sqrt{d})$ can be written in the form $\alpha + \beta\sqrt{d}$.

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

Thus $\mathbb{Q}[\sqrt{d}]$ is a field. $\square$

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 $ba = 1$. $\square$

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

Solution. By def 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

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

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 def zero-divisor. Thus $\mathbb{Z}_2[i]$ is not an integral domain by def integral domain. Thus $\mathbb{Z}_2[i]$ is not a field by def 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 $\lhd$ 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 $R \not\lhd \mathbb{Z} \oplus \mathbb{Z}$ 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. □

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. □

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

a. $\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$

b. $\langle a \rangle = \langle 6 \rangle + \langle 8 \rangle$

c. $\langle a \rangle = \langle m \rangle + \langle n \rangle$

Solution. □

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. □

Exercise 14.13. Find a positive integer a such that

1. $\langle a \rangle = \langle 3 \rangle \langle 4 \rangle$
2. $\langle a \rangle = \langle 6 \rangle \langle 8 \rangle$
3. $\langle a \rangle = \langle m \rangle \langle n \rangle$

Solution. □

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

Solution. □