Additional Exercises:

① $\alpha = a+b\sqrt{D}$, $N(\alpha) = a^2 - b^2D$

(a) Let $\alpha = a+b\sqrt{D}$, $\beta = c+d\sqrt{D}$. Then $N(\alpha) = a^2-b^2D$ & $N(\beta) = c^2-d^2D$.

$\alpha\beta = (a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD) + (ad+bc)\sqrt{D}$ &

$N(\alpha\beta) = (ac+bdD)^2 - (ad+bc)^2D$

$= a^2c^2 + 2acbdD + b^2d^2D^2 - (a^2d^2 + 2adbc + b^2c^2)D$

$= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D$

$= (a^2-b^2D)(c^2-d^2D)$

$= N(\alpha)\,N(\beta)$.

(b) If $\alpha \in \mathbb{Z}[\sqrt{D}]$, $\alpha = a+b\sqrt{D}$, where $a,b \in \mathbb{Z}$.

$N(\alpha) = a^2-b^2D$, & $a^2, b^2, D \in \mathbb{Z} \Rightarrow N(\alpha) \in \mathbb{Z}$.

(c) If $\alpha = a+b\left(\frac{1+\sqrt{D}}{2}\right)$, $a,b \in \mathbb{Z}$, then

$\alpha = (a+\frac{b}{2}) + (\frac{b}{2})\sqrt{D}$, so $N(\alpha) = (a+\frac{b}{2})^2 - (\frac{b}{2})^2D$

$= a^2 + ab + \frac{b^2}{4} - \frac{b^2}{4}D$

$= a^2 + ab + \frac{b^2}{4}(1-D)$.

Since $D \equiv 1 \pmod 4$, $1-D$ is divisible by 4, so $\frac{1-D}{4} \in \mathbb{Z}$. Since we also have $a,b \in \mathbb{Z}$, it follows that $N(\alpha) \in \mathbb{Z}$.

(d)(i)($\Rightarrow$) Suppose $\alpha \in \mathbb{Z}[D]$ is a unit. Then $\exists\, \beta \in \mathbb{Z}[\sqrt{D}]$ s.t. $\alpha\beta = 1$. Thus

$N(\alpha\beta) = N(1)$

$N(\alpha)N(\beta) = 1$, by (a)

Since $N(\alpha), N(\beta) \in \mathbb{Z}$ by (b), we see that either $N(\alpha) = N(\beta) = 1$ or $N(\alpha) = N(\beta) = -1$.

($\Leftarrow$): Suppose $N(\alpha) = 1$ for $\alpha = a+b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Then $a^2-b^2D = 1$.

$(a+b\sqrt{D})(a-b\sqrt{D}) = a^2-b^2D = 1$ & $a-b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, so α is a unit.

Similarly, if $N(\alpha) = -1$, then $(a+b\sqrt{D})(-a+b\sqrt{D}) = -a^2+b^2D = 1$, so α is a unit.

(ii) ($\Rightarrow$): Same as in (i).

($\Leftarrow$): Suppose $N(\alpha) = 1$ for $\alpha = a+b(\frac{1+\sqrt{D}}{2})$, $a,b \in \mathbb{Z}$. Then

$\alpha = (a+\frac{b}{2}) + \frac{b}{2}\sqrt{D}$ & $N(\alpha) = (a+\frac{b}{2})^2 - (\frac{b}{2})^2D = 1$.

$[(a+\frac{b}{2}) + \frac{b}{2}\sqrt{D}][(a+\frac{b}{2}) - \frac{b}{2}\sqrt{D}] = (a+\frac{b}{2})^2 - (\frac{b}{2})D = 1$, so we just need to show $\beta = (a+\frac{b}{2}) - \frac{b}{2}\sqrt{D} \in \{a' + b'(\frac{1+\sqrt{D}}{2}) \mid a', b' \in \mathbb{Z}\}$

Let $b' = -b$. Then,

$\beta = a - \frac{b'}{2} + \frac{b'}{2}\sqrt{D}$

$= a - b' + \frac{b'}{2} + \frac{b'}{2}\sqrt{D}$

$= (a-b') + b'(\frac{1+\sqrt{D}}{2})$, & $a-b', b' \in \mathbb{Z}$.

Thus α is a unit.

Similarly, if $N(\alpha) = -1$, then

$[(a+\frac{b}{2}) + \frac{b}{2}\sqrt{D}][-(a+\frac{b}{2}) + \frac{b}{2}\sqrt{D}] = -(a+\frac{b}{2})^2 + (\frac{b}{2})D = 1$, & $-(a+\frac{b}{2}) + \frac{b}{2}\sqrt{D} = -\beta$, & so is an element of our set. Thus, α is a unit.

② (a) Let $\alpha = a+bi$, $\beta = c+di \in \mathbb{Z}[i]$. Suppose $\beta \neq 0$ & $\alpha\beta = 0$. We will show that $\alpha = 0$.

$0 = \alpha\beta = (a+bi)(c+di) = ac - bd + (ad+bc)i$

$\Rightarrow ac - bd = 0$ and $ad + bc = 0$.

Since $\beta \neq 0$, either $c \neq 0$ or $d \neq 0$.

If $c \neq 0$, then $a = \frac{bd}{c} \Rightarrow \frac{bd}{c} \cdot d + bc = 0$

$\Rightarrow bd^2 + bc^2 = 0$

$b(d^2 + c^2) = 0$. Since $d^2 + c^2 \neq 0$, $b = 0$.

Since $a = \frac{bd}{c}$, $a = 0 \Rightarrow \alpha = 0$.

If $d \neq 0$, then $a = \frac{-bc}{d}$, and in a similar manner we get $\alpha = 0$.

Therefore $\mathbb{Z}[i]$ has no zero divisors & so is an integral domain.

Note: You could also say $\mathbb{Z}[i] \subseteq \mathbb{C}$, & $\mathbb{C}$ is a field. Since by #4 all fields are integral domains, $\mathbb{C}$ has no zero divisors, & therefore $\mathbb{Z}[i]$ doesn't, either.

(b) The smallest field containing $\mathbb{Z}[i]$ is $\mathbb{Q}[i]$.

③ $\mathcal{P}(X)$ is a ring: It is clear that $\mathcal{P}(X)$ is closed under $+$ & $\cdot$.

- $\mathcal{P}(X)$ is an abelian gp under $+$:
  - associative: Let $A, B, C \in \mathcal{P}(X)$.

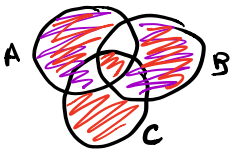
$$A + (B+C) = A \Delta (B \Delta C) = (A \setminus (B \Delta C)) \cup ((B \Delta C) \setminus A)$$
$$= (A \setminus (B \setminus C \cup C \setminus B)) \cup ((B \setminus C \cup C \setminus B) \setminus A)$$
$$= (A \setminus (B \cup C)) \cup (A \cap B \cap C) \cup (B \setminus (C \cup A)) \cup (C \setminus (B \cup A))$$

$$(A+B)+C = (A \Delta B) \Delta C = ((A \Delta B) \setminus C) \cup (C \setminus (A \Delta B))$$
$$= ((A \setminus B \cup B \setminus A) \setminus C) \cup (C \setminus (A \setminus B \cup B \setminus A))$$
$$= (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (C \cap A \cap B)$$

As these sets are equal, Δ is associative.

Note: here's the Venn diagram proof

$B \Delta C$, $A \Delta (B \Delta C)$



$A \Delta B$, $(A \Delta B) \Delta C$

The blue set & the red set are the same.

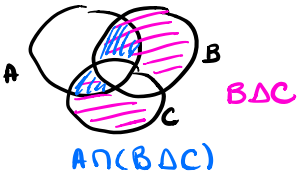
  - Abelian: Let $A, B \in \mathcal{P}(X)$. $A \Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \Delta A$.
  - Identity: $\emptyset \in \mathcal{P}(X)$. For any $A \in \mathcal{P}(X)$, $A \Delta \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$, so $\emptyset$ is the identity.
  - Inverses: Let $A \in \mathcal{P}(X)$. Then $A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset$, so every element is its own (additive) inverse.

Thus $(\mathcal{P}(X), +)$ is an abelian gp. We next show $(\mathcal{P}(X), +, \cdot)$ is a ring:

- $\cdot$ is assoc: Let $A, B, C \in \mathcal{P}(X)$. Then $x \in (A \cap B) \cap C \Leftrightarrow x \in A \cap B$ and $x \in C$, $\Leftrightarrow x \in A$ and $x \in B$ and $x \in C \Leftrightarrow x \in A$ and $x \in B \cap C \Leftrightarrow x \in A \cap (B \cap C)$.

- $\cdot$ is commutative: Let $A, B \in \mathcal{P}(X)$. Then $x \in A \cap B \Leftrightarrow x \in A$ and $x \in B \Leftrightarrow x \in B$ and $x \in A \Leftrightarrow x \in B \cap A$, so $A \cdot B = B \cdot A$.
- Distributive laws: Since $\cdot$ is commutative, we only need to check the left distributive property. Let $A, B, C \in \mathcal{P}(X)$.

$$\begin{aligned} A \cdot (B + C) &= A \cap (B \triangle C) = A \cap (B \setminus C \cup C \setminus B) \\ &= A \cap (B \setminus C) \cup A \cap (C \setminus B) \\ &= (A \cap B) \setminus C \cup (A \cap C) \setminus B \\ &= (A \cap B) \setminus (A \cap C) \cup (A \cap C) \setminus (A \cap B) \\ &= (A \cdot B) \setminus (A \cdot C) \cup (A \cdot C) \setminus (A \cdot B) \\ &= A \cdot B + A \cdot C \end{aligned}$$



Note: use the Venn diagram to help figure out the equalities.

- unity: $X \in \mathcal{P}(X)$, & for any $A \in \mathcal{P}(X)$, $A \cdot X = A \cap X = A$, so X is unity.

Therefore, $(\mathcal{P}(X), +, \cdot)$ is a commutative ring with unity.

$\mathcal{P}(X)$ is not a field: Let $A \in \mathcal{P}(X)$, $A \neq \emptyset, X$. Then for all $B \in \mathcal{P}(X)$, $A \cdot B = A \cap B \subseteq A$, so $A \cdot B \neq X$. Thus A does not have a multiplicative inverse.

$\mathcal{P}(X)$ is not an integral domain: Let $A \in \mathcal{P}(X)$, $A \neq \emptyset, X$, & let $B = X \setminus A$. Then $A \cdot B = A \cap (X \setminus A) = \emptyset$. Since $A \neq X$, $B = X \setminus A \neq \emptyset$, so we have found two non-zero (i.e. $\neq \emptyset$) elts whose product is 0 (since $0 = \emptyset$).

To find char $\mathcal{P}(X)$, we consider unity, which is X.
char $\mathcal{P}(X)$ is the smallest $n \in \mathbb{Z}^+$ s.t. $nX = \underbrace{X + X + \cdots + X}_{n} = \emptyset$.
$X + X = X \triangle X = \emptyset$, so char $\mathcal{P}(X) = 2$.

④ Let F be a field, & suppose $\exists a, b \in F$ w/ $a \neq 0$ and $ab = 0$.
Since $a \neq 0$, $a^{-1} \in F$, and

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(0) \\ (a^{-1}a)b &= 0 \\ 1 \cdot b &= 0 \\ b &= 0 \end{aligned}$$

Therefore, F is an integral domain.

⑤ Since R, S are non-trivial, $0_R \neq 1_R$ & $0_S \neq 1_S$. Consider the elts $(0_R, 1_S), (1_R, 0_S) \in R \times S$. Neither of these elts is $0_{R \times S} = (0_R, 0_S)$, but $(0_R, 1_S) \cdot (1_R, 0_S) = (0_R \cdot 1_R, 1_S \cdot 0_S) = (0_R, 0_S) = 0_{R \times S}$.
Therefore, $R \times S$ is not an integral domain.