Recall: Let R be a ring and $R[x]$ be the polynomial ring over R. Then

1. If R is commutative, then $R[x]$ is commutative.
2. If R contains identity, then $R[x]$ contains the same identity as R.
3. If R is an integral domain, then $R[x]$ is an integral domain.

Proof of (3). For the third condition, it is sufficient to show that if R has no zero divisors, then $R[x]$ has no zero divisors. Let $p(x) = \sum_{j=0}^{n} a_j x^j$ with $a_n \neq 0$ and $q(x) = \sum_{j=0}^{m} b_j x^j$ with $b_m \neq 0$. For the addition of $p(x)$ and $q(x)$,

$$p(x) + q(x) = \sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j = \sum_{j=0}^{\max\{n,m\}} (a_j + b_j) x^j \tag{1}$$

and for the multiplication,

$$p(x)q(x) = \left(\sum_{j=0}^{n} a_j x^j \right) \left(\sum_{j=0}^{m} b_j x^j \right) = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j \tag{2}$$

Considering (2), to show that the product is a nonzero polynomial, observe that we have

$$p(x)q(x) = a_n b_n x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \cdots + a_0 b_0$$

Since R is an integral domain and $a_n, b_m \neq 0$, then $a_n b_m \neq 0$. Therefore, $p(x)q(x) \neq 0$. Thus, $R[x]$ has no zero divisors. □

Example 1. Consider the set $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}, i^2 = -1\}$. Then $(\mathbb{Z}[i], +, \cdot)$ is a ring. We show that $\mathbb{Z}[i]$ is an integral domain, i.e. commutative ring with identity, and has no zero divisors.

1. $\mathbb{Z}[i]$ is commutative because of complex numbers is also commutative.
2. $1 = 1 + 0i \in \mathbb{Z}[i]$, so $\mathbb{Z}[i]$ contains the identity.
3. Let $a + ib, c + id \in \mathbb{Z}[i]$ such that $(a + ib)(c + id) = 0$. Then we multiply both sides by the complex conjugates so that

$$\begin{aligned} (a - ib)(c - id)(a + ib)(c + id) &= 0 \\ (a^2 + b^2)(c^2 + d^2) &= 0 \end{aligned}$$

   Then without loss of generality, $a^2 + b^2 = 0$ implies that $a = b = 0$, so then $c \neq 0$ and $d \neq 0$ and thus, $\mathbb{Z}[i]$ has no zero divisors, as required.

Definition 1. Let R be a ring. We say that $S \subset R$ is a subring of R, and write $S \leq R$[1], if S is a ring using the same addition and multiplication as R.

[1]Whenever I use the notation $S \leq R$, I mean that S is a subring of R. It is a similar notation as saying that H is a subgroup of G, or $H \leq G$, in group theory.

Example 2. $\{0\} \leq R$ and $R \leq R$, which are known as the *trivial subrings* of R.

Example 3. The following are examples of subrings of one another:

$$n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{C}[x]$$

and also,

$$\mathbb{Z} \leq \mathbb{Z}[i] \leq \mathbb{C}$$

Example 4. $\mathbb{Z}_n \not\leq \mathbb{Z}$. Indeed, recall that $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. Then addition $+_n$ and $\cdot_n$ are not the same operations as operations over $\mathbb{Z}$, namely $+$ and $\cdot$.

Consider $\mathbb{Z}_3 = \{0, 1, 2\}$, where

$$\begin{aligned} 0 &= \{..., -6, -3, 0, 3, 6, ...\} \\ 1 &= \{..., -5, -2, 1, 4, 7, ...\} \\ 2 &= \{..., -4, -1, 2, 5, 8, ...\} \end{aligned}$$

When we define addition in $\mathbb{Z}_3$,

$$a +_3 b = [a] + [b] = [a + b] = a + b \bmod 3$$

Similarly, multiplication is defined as

$$a \cdot_3 b = [a] \cdot [b] = [a \cdot b] = a \cdot b \bmod 3$$

Proposition 1. *Let R be a ring and let $S \subset R$. Then $S \leq R$ if and only if*

1. *$S \neq \emptyset$.*
2. *If $r, s \in S$, then $rs \in S$.*
3. *If $r, s \in S$, then $r + (-s) \in S$.*

Example 5. Take $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5, 6\}$. Then $S \leq R$ where $S = \{0, 3\}$. Is S a ring with identity? By the multiplication table,

$\cdot_3$	0	3
0	0	0
3	0	3

See that $3 \cdot_6 3 = 3$