Definition 1. Define $\mathbb{Z}[\sqrt{-5}]$ to be the following subset of the complex numbers

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

where $i = \sqrt{-1}$.

1. Prove that $\mathbb{Z}[\sqrt{-5}]$ is a commutative ring with 1. (Hint: Use the fact that it is a subset of the ring $\mathbb{C}$.)
   Is it an integral domain? Why or why not?

   **Remark.** We’ll refer to the ring $R = \mathbb{Z}[\sqrt{-5}]$ as $R$ for the purposes of this worksheet. The ring $R$ is similar in definition to the ring of Gaussian integers ($\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$), but is algebraically very different.

2. Define a function $N : R \to \mathbb{Z}$ by $N(a + bi\sqrt{5}) = a^2 + 5b^2$ (this is the square of the distance from $a + bi\sqrt{5}$ to the origin in the complex plane). Verify that for any $x, y \in R$, we have $N(xy) = N(x) \cdot N(y)$. (Hint: You can do this by explicit calculation, or by remembering things about the geometry of multiplying complex numbers.)

3. Show that if $u \in R$ is a unit, then $N(u) = 1$. Conclude that 1 and $-1$ are the only units in $R$.

4. Check that 41 $\in \mathbb{Z}$ is irreducible (i.e. check that 41 is a prime number).

5. Show that 41 $\in R$ is reducible by finding an integer $a \in \mathbb{Z}$ such that $(a + i\sqrt{5})(a - i\sqrt{5}) = 41$.

   **Remark.** The fact that 41 factors in $R$ even though it is irreducible in the subring $\mathbb{Z}$ may seem strange. But really this is no weirder than the fact that $x^2 + 1$ factors in $\mathbb{C}[x]$ even though it is irreducible in $\mathbb{Q}[x]$.

6. Use the function $N$ to show that 2 and 3 are still irreducible in $R$.

7. Use the function $N$ to show that $1 + i\sqrt{5}$ and $1 - i\sqrt{5}$ are also irreducible in $R$.

8. Use the above to give two distinct factorizations of 6 $\in R$ into irreducibles. To be sure that your factorizations are genuinely different, you’ll need to check that none of the irreducibles in question are associates.

   **Moral.** The Fundamental Theorem of Arithmetic does not carry over to the integral domain $R$ because there can be too many factorizations into irreducibles. That is to say, $R$ is not a unique factorization domain.