Let R be an integral domain (i.e. a commutative, unital, non-trivial ring without any zero divisors).

Def: We say that a divides b and write $a|b$ if $b=ac$ for some $c\in R$.
While this definition works for any a,b (including 0), we will usually silently assume $a\neq 0$, $b\neq 0$.

Proposition 1: $a|b$ if and only if $bR\subseteq aR$.

In fact, if $a|b$ then $b=ac$ and $br=acr\in aR$ for every $r\in R$, so $bR\subseteq aR$. Conversely, if $bR\subseteq aR$ then $b\in aR$ (since $b\in bR$), so $b=ar$ for some r, i.e. $a|b$. ☒

Definition: We say that a,b in R are associated if $a|b$ and $b|a$.

Proposition 2: Following conditions are equivalent:

(1) a and b are associated

(2) $aR=bR$

(3) $a=bu$ for some $u\in R^\times$ (i.e. invertible in R).

Pf: $a|b \Leftrightarrow bR\subseteq aR$ so $a|b$ and $b|a$ means that $aR\subseteq bR$ and $bR\subseteq aR$ i.e. $aR=bR$. This shows that (1) and (2) are equivalent.

(2)$\Rightarrow$(3): Suppose $aR=bR$. If $a=0$ then $b=0$ and (3) holds. If $a\neq 0$ then $b\neq 0$ and $a\in bR$ and $b\in aR$ so $a=bu$ and $b=aw$ for some $u,w\in R$. Thus $a=bu=(aw)u=a(wu)$

so $a(1-wu)=0$. Since R is a domain and $a\neq 0$ we have $1-wu=0$ i.e. $wu=1$. Thus $u,w\in R^\times$ and (3) holds.

(3) $\Rightarrow$ (1) $a=bu$ then clearly $b|a$. Since $u\in R^\times$, we can multiply by u^{-1} and get $au^{-1}=b$ so $a|b$. Thus a and b are associated. ∎

Remark: The group $R^\times$ of invertible elements acts on R by left multiplication ($u*r=ur$). Two elements are associated iff they are in the same orbit of this action.

Definition: $a\in R$ is called irreducible if $a\neq 0$, $a\notin R^\times$ and whenever $a=bc$ for some $b,c\in R$ then either $b\in R^\times$ or $c\in R^\times$ (equivalently, either b or c is associated to a).

Example: Every prime number is irreducible in $\mathbb{Z}$.

Definition: $a\in R$ is called prime if $a\neq 0$ and aR is a prime ideal.

Recall that aR is a prime ideal if it has the following property: if $r\cdot s\in aR$ then $r\in aR$ or $s\in aR$. In other words, if $a|rs$ then $a|r$ or $a|s$. Thus

$a\in R$ is prime iff $a\neq 0$, $a\notin R^\times$ and if $a|bc$ for some b,c then $a|b$ or $a|c$

A famous Euclid's Lemma say that prime numbers are prime elements in $\mathbb{Z}$

Euclid's Lemma: If p is a prime (number in $\mathbb{Z}$) and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proposition 3: Every prime element is irreducible.

Pf: Let a be a prime element in R, so $a \neq 0$, $a \notin R^\times$.
If $a = b \cdot c$ for some $b, c \in R$ then $b \mid a$ and $c \mid a$.
Since $a \mid bc$ and a is prime, $a \mid b$ or $a \mid c$. If $a \mid b$ then since $b \mid a$ we get that a, b are associated and $c \in R^\times$.
If $a \mid c$ then since $c \mid a$ we get that a, c are associated and $b \in R^\times$. In any case, one of b, c is in $R^\times$. Thus a is irreducible.

Let us look at some examples.
Let $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$
and $\mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} : a, b \in \mathbb{Z}\}$.

Excersise: Show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{5}]$ are subrings of the field $\mathbb{C}$ of complex numbers. Thus they are integral domains.

Remark: Note that $a+bi = c+di$ iff $a=c$, $b=d$.
Similarly, $a+b\sqrt{5} = c+d\sqrt{5}$ iff $a=c$, $b=d$ (here $a, b, c, d \in \mathbb{Z}$).
For $a+bi \in \mathbb{Z}[i]$ define $\overline{a+bi} = a-bi$ (so $\bar{x}$ is a complex conjugate of x). Then for any $x, y \in \mathbb{Z}[i]$ we have:

① $\overline{x+y} = \bar{x}+\bar{y}$, $\overline{xy} = \bar{x}\bar{y}$.

② $(a+bi)\cdot\overline{(a+bi)} = a^2+b^2 \in \mathbb{Z}$.

Property (1) means that the conjugation is an automorphism of $\mathbb{Z}[i]$.

Similarly, for $a+b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ define $\overline{a+b\sqrt{5}} = a-b\sqrt{5}$.

Then, for any $x, y \in \mathbb{Z}[\sqrt{5}]$ we have

(1) $\overline{x+y} = \bar{x}+\bar{y}$ and $\overline{xy} = \bar{x}\cdot\bar{y}$

(2) If $x = a+b\sqrt{5}$ then $x\cdot\bar{x} = a^2-5b^2 \in \mathbb{Z}$ and $x\bar{x}=0$ if and only if $a=b=0$.

Lemma 1: $a+bi \in \mathbb{Z}[i]^\times$ iff $a=0, b=\pm 1$ or $a=\pm 1, b=0$.

Thus $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$

Pf: Suppose $(a+bi)\cdot x = 1$. Then $\overline{(a+bi)x} = 1$ so $(a-bi)\bar{x} = 1$. Thus $(a+bi)x\cdot(a-bi)\cdot\bar{x} = 1$, i.e. $(a^2+b^2)\cdot x\bar{x} = 1$. Since a^2+b^2 and $x\bar{x}$ are integers we must have $a^2+b^2 = 1$ and then $a=0$ $b=\pm 1$ or $a=\pm 1$, $b=0$. ☆

Clearly each $1,-1,i,-i$ is invertible.

Lemma 2: $\mathbb{Z}[\sqrt{5}]^\times$ is infinite.

Pf: Let $u = 2+\sqrt{5}$. Then $u\cdot(\sqrt{5}-2) = 1$, so $u \in \mathbb{Z}[\sqrt{5}]^\times$.

Since $u > 1$ we have $u < u^2 < u^3 < \dots$ and each power of u is invertible

Remark: One can prove that $\mathbb{Z}[\sqrt{5}]^\times = \{\pm u^n : n \in \mathbb{Z}\}$

Example: In $\mathbb{Z}[i]$ the element $1+2i$ is irreducible.

Pf: Suppose $1+2i = uw$ for some $u, w \in \mathbb{Z}[i]$. Then $\overline{1+2i} = \bar{u}\bar{w}$ and multiplying we get $(1+2i)(1-2i) = u\bar{u} \cdot w\bar{w}$. Since $(1+2i)(1-2i) = 5$ we have $5 = (u\bar{u})(w\bar{w})$ and $u\bar{u}, w\bar{w}$ are integers. Since 5 is a prime number, either $u\bar{u} = \pm 1$ or $w\bar{w} = \pm 1$ so either u is invertible or w is invertible. ☒

Example: In $\mathbb{Z}[\sqrt{5}]$ each of $2, 1+\sqrt{5}, 1-\sqrt{5}$ are irreducible.

Pf: Let a be one of $2, 1+\sqrt{5}, 1-\sqrt{5}$. Then $a\bar{a} = \pm 4$. If $a = uw$ then $a\bar{a} = (u\bar{u})(w\bar{w})$, so $\pm 4 = (u\bar{u})(w\bar{w})$. If $u\bar{u} = \pm 1$ then u is invertible. If $w\bar{w} = \pm 1$ then w is invertible. If none of these 2 cases happens then $u\bar{u} = \pm 2 = w\bar{w}$. We will show that this is not possible. If $u = a + b\sqrt{5}$ then $u\bar{u} = a^2 - 5b^2 = \pm 2$. This means that $a^2 \equiv \pm 2 \pmod 5$. But $0^2 \equiv 0 \pmod 5$, $1^2 \equiv 1 \pmod 5$, $2^2 \equiv -1 \pmod 5$, $3^2 \equiv -1 \pmod 5$ and $4^2 \equiv 1 \pmod 5$. So no square can be congruent to ± 2 modulo 5, and $u\bar{u} = \pm 2$ is not possible. Thus show that either u or w is invertible, i.e. a is irreducible.

Note that $2 \cdot 2 = 4 = (1+\sqrt{5})(\sqrt{5}-1)$ and $2, 1+\sqrt{5}, \sqrt{5}-1$ are irreducible. We see that $2 \mid (1+\sqrt{5})(-1+\sqrt{5})$ in $\mathbb{Z}[\sqrt{5}]$ but $2 \nmid 1+\sqrt{5}$ and $2 \nmid 1+\sqrt{5}$. So 2 is irreducible but <u>not</u> prime in $\mathbb{Z}[\sqrt{5}]$.

Note: $2 \mid a+b\sqrt{5} \Leftrightarrow (a+b\sqrt{5}) = 2(c+d\sqrt{5}) = 2c+2d\sqrt{5}$ iff a and b are even.

<u>Exercise</u>: Prove that $1+2i$ is a prime element in $\mathbb{Z}[i]$.

<u>Definition</u>: Let R be an integral domain. Consider 2 factorizations $a = \pi_1 \cdots \pi_t = \tilde{\pi}_1 \cdots \tilde{\pi}_s$ of an element $a \in R$, $a \neq 0$, $a \notin R^\times$ into a product of irreducible elements. We say that these factorizations are <u>equivalent</u> if $s = t$ and there is a permutation σ of $1, 2, \ldots, t$ such that π_i and $\tilde{\pi}_{\sigma(i)}$ are associated for $i = 1, 2, \ldots, t$.

<u>Example</u>: In $\mathbb{Z}$, the factorizations $6 = 2 \cdot 3 = (-3) \cdot (-2)$ are equivalent.

In $\mathbb{Z}[\sqrt{5}]$ the factorizations $4 = 2 \cdot 2 = (1+\sqrt{5})(\sqrt{5}-1)$ are not equivalent.

<u>Definition</u>: R is called a <u>unique factorization domain</u> (UFD) if R is an integral domain in which every non-zero, non-invertible element is either irreducible

or it is a product of irreducible elements and any two such factorizations are equivalent.

Proposition 4: If R is a UFD then every irreducible element is prime.

Pf: Let π be irreducible in R. Suppose $\pi | ab$ then $ab = \pi c$ for some c. Since R is UFD we can factor a, b, c into irreducibles: $a = a_1 \cdots a_s$, $b = b_1 \cdots b_t$, $c = c_1 \cdots c_r$ where a_i, b_i, c_i are irreducible.

Then $\pi c_1 \cdots c_r = a_1 \cdots a_s \cdot b_1 \cdots b_t$.

Since R is UFD, these 2 factorizations are equivalent. In particular π is associated with some a_i or some b_i. If π is associated with a_i then $\pi | a$. If π is associated with b_i then $\pi | b$. Then either $\pi | a$ or $\pi | b$, which shows that π is prime.

Corollary: $\mathbb{Z}[\sqrt{5}]$ is not a UFD

(We will prove later that $\mathbb{Z}[i]$ is a UFD!)

The following observation will be very useful.

Proposition 5: Let R be an integral domain. Suppose $a \in R$ can be factored as a product of prime elements: $a = \pi_1 \cdots \pi_s$ and π_i are prime. If $a = \tilde{\pi}_1 \cdots \tilde{\pi}_t$ with each $\tilde{\pi}_i$ irreducible then the two factorizations are equivalent.

Proof: Our proof goes by induction on s.

If $s=1$: $a=\pi_1=\tilde{\pi}_1\cdot\ldots\cdot\tilde{\pi}_t$. Since π_1 is prime and $\pi_1 \mid \tilde{\pi}_1\cdot\ldots\cdot\tilde{\pi}_t$ then $\pi_1 \mid \tilde{\pi}_i$ for some i. We may assume $\pi_1 \mid \tilde{\pi}_1$ (permuting the factors if necessary). Then $\tilde{\pi}_1 = \pi_1 \cdot u$ and since $\tilde{\pi}_1$ is irreducible, u must be invertible and $\tilde{\pi}_1, \pi_1$ are associated, so $u=\tilde{\pi}_2\cdot\ldots\cdot\tilde{\pi}_t$ which is not possible as $\tilde{\pi}_i$ are not invertible. This means that $t=1$ and $\pi_1=\tilde{\pi}_1$.

Suppose the result holds for $s<k$. Consider

$$a=\pi_1\cdot\ldots\cdot\pi_k=\tilde{\pi}_1\cdot\ldots\cdot\tilde{\pi}_t,\ \pi_i \text{ prime},\ \tilde{\pi}_i \text{ irreducible}.$$

Now, π_k prime and $\pi_k \mid \tilde{\pi}_1\cdot\ldots\cdot\tilde{\pi}_t$ means that $\pi_k \mid \tilde{\pi}_i$ for some i and then $\pi_k = u\tilde{\pi}_i$ for some $u\in R^\times$. Permuting the factors, we may assume $i=t$: $\pi_k = u\tilde{\pi}_t$.

Then $\pi_1\cdot\ldots\cdot\pi_{k-1}=(u\tilde{\pi}_1)\cdot\ldots\cdot\tilde{\pi}_{t-1}$ and $u\tilde{\pi}_1, \tilde{\pi}_2, \ldots, \tilde{\pi}_{t-1}$ are irreducible. By the inductive assumption these two factorizations are equivalent (so $k-1=t-1$) and since π_k and $\tilde{\pi}_t$ are associated, the original factorizations are equivalent as well. ☒

Thus we proved:

Theorem: R is a UFD if and only if every non-zero, non-invertible element in R can be factored into prime elements.

Pf: In fact, if R is a UFD, then every irreducible is prime so every non-zero, non-invertible element is a product of prime elements.

Conversely, if every $a \in R$, $a \neq 0$, $a \notin R^\times$ can be expressed as a product of prime elements then by Proposition 5 any other factorization of a into irreducibles is equivalent to the one into prime elements, hence R is UFD. ∎