Definition 23.1

Let R be an integral domain, and let $a, b \in R$. We say that a *divides* b if $b = ac$ for some $c \in R$. We then write: $a \mid b$.

Theorem 23.2

If R is an integral domain and $a, b \in R$ are non-zero elements then $a \sim b$ and only if $a \mid b$ and $b \mid a$.

Proof. If $a \mid b$ and $b \mid a$ then $b = ca$ and $a = db$. This gives $b = cdb$. Since R is an integral domain, we obtain that $cd = 1$, so c, d are units and $d = c^{-1}$. Therefore $a \sim b$.

Conversely, if $a \sim b$ then $b = ua$ for some unit u, and so $a \mid b$. Also, $a = u^{-1}b$, so $b \mid a$. □

Example

- In $\mathbb{Z}$ we have:

$$\{\text{prime elements}\} = \{\pm \text{ prime numbers}\} = \{\text{irreducible elements}\}$$

- By the proof of Theorem 22.5, in $\mathbb{Z}[\sqrt{-5}]$ the element $\alpha = 2 + \sqrt{5}i$ is irreducible. On the other hand α is not a prime element since $\alpha \mid (3 \cdot 3)$ but $\alpha \nmid 3$.

Theorem 23.3

If R is an integral domain and $a \in R$ is a prime element then a is irreducible.

Proof. Let $a \in R$ be a prime element and let $a = bc$. We want to show that either b or c must be a unit in R.

We have $a \mid (bc)$. Since a is a prime element it implies that $a \mid b$ or $a \mid c$.

We can assume that $a \mid b$. Since also $b \mid a$, thus by Theorem 23.2 we obtain that $a \sim b$, i.e. $a = bu$ for some unit $u \in R$. Therefore $bc = a = bu$. Since R is an integral domain, this gives $u = c$, and so c is s unit. □

Theorem 23.4

If R is a UFD and $a \in R$ then a is an irreducible element if and only if a is a prime element.

Proof. ($\Leftarrow$) This follows from Theorem 23.3.

($\Rightarrow$) Assume that $a \in R$ is irreducible and that $a \mid (bc)$. We want to show that either $a \mid b$ or $a \mid c$.

If $b = 0$, then $b = a \cdot 0$ so $a \mid b$. If b is a unit, then $c = b^{-1}bc$ so $a \mid c$.

As a consequence, we can assume that b, c are non-zero, non-units.

Since $a \mid (bc)$ there is $d \in R$ such that $bc = ad$. Assume that d is not a unit. Since R is a UFD we have decompositions:

$$b = b_1 \cdot \ldots \cdot b_m, \qquad c = c_1 \cdot \ldots \cdot c_n, \qquad d = d_1 \cdot \ldots \cdot d_p$$

where b_i, c_j, d_k are irreducible. This gives

$$b_1 \cdot \ldots \cdot b_m \cdot c_1 \cdot \ldots \cdot c_n = a \cdot d_1 \cdot \ldots \cdot d_p$$

By the uniqueness of decomposition in UFDs this implies that either $a \sim b_i$ for some i or $a \sim c_j$ for some j. In the first case we get $a \mid b$, and in the second case $a \mid c$.

If d is a unit the argument is similar. □

Theorem 23.5

An integral domain R is a UFD if and only if the following conditions are satisfied:

1) Every non-zero, non-unit element of R is a product of irreducible elements.
2) Every irreducible element in R is a prime element.

Proof. ($\Rightarrow$) This follows from the definition of UFD and Theorem 23.4.

(⇐) Assume that R satisfies conditions 1) - 2) of the theorem. We only need to show that if $b_1, \ldots, b_k$, $c_1, \ldots, c_l$ are irreducible elements in R such that

$$b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_l$$

then $k = l$, and after reordering of the factors we have $b_1 \sim c_1$, …, $b_k \sim c_k$.

We argue by induction with respect to k.

If $k = 1$ then we have $b_1 = c_1 \cdot \ldots \cdot c_l$. Since b_1 is irreducible, this implies that $l = 1$, and so $b_1 = c_1$.

Next, assume that the uniqueness property holds for some k and that we have

$$b_1 \cdot \ldots \cdot b_k \cdot b_{k+1} = c_1 \cdot \ldots \cdot c_l$$

where b_i, c_j are irreducible elements. This implies that $b_{k+1} \mid (c_1 \cdot \ldots \cdot c_l)$. By condition 2) we get that b_{k+1} is a prime element. It follows that $b_k \mid c_j$ for some $1 \leq j \leq l$. We can assume that $b_{k+1} \mid c_l$. Then $c_l = ab_{k+1}$ for some $a \in R$. Since c_l, b_{k+1} are irreducible, a must be a unit. This shows that $b_{k+1} \sim c_l$. Furthermore, we obtain from here that

$$b_1 \cdot \ldots \cdot b_k \cdot b_{k+1} = c_1 \cdot \ldots \cdot c_{l-1} \cdot ab_{k+1}$$

Since R is an integral domain this gives

$$b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_{l-1}a$$

Since b_k is irreducible and a is a unit, the product $c_{l-1}a$ is an irreducible element. Therefore, by the inductive assumption we get that $k = l - 1$, and that after reordering of factors we have

$$b_1 \sim c_1, \ldots, \quad b_{k-1} \sim c_{k-1}, \quad b_k \sim c_{l-1}a \sim c_{l-1}$$

□