for some unit $u_{i_0} \in A$ and some index $i_0$, $1 \leq i_0 \leq m+n$. As a consequence, if $1 \leq i_0 \leq m$, then $a$ divides $b$, and if $m+1 \leq i_0 \leq m+n$, then $a$ divides $c$. This proves that $(2')$ holds.

Let us now assume that $(2')$ holds. Assume that

$$a = a_1 \cdots a_m = b_1 \cdots b_n,$$

where $a_i \in A$ and $b_j \in A$ are irreducible. Without loss of generality, we may assume that $m \leq n$. We proceed by induction on $m$. If $m = 1$,

$$a_1 = b_1 \cdots b_n,$$

and since $a_1$ is irreducible, $u = b_1 \cdots b_{i-1} b_{i+1} b_n$ must be a unit for some $i$, $1 \leq i \leq n$. Thus, (2) holds with $n = 1$ and $a_1 = b_i u$. Assume that $m > 1$ and that the induction hypothesis holds for $m - 1$. Since

$$a_1 a_2 \cdots a_m = b_1 \cdots b_n,$$

$a_1$ divides $b_1 \cdots b_n$, and in view of $(2')$, $a_1$ divides some $b_j$. Since $a_1$ and $b_j$ are irreducible, we must have $b_j = u_j a_1$, where $u_j \in A$ is a unit. Since $A$ is an integral domain,

$$a_1 a_2 \cdots a_m = b_1 \cdots b_{j-1} u_j a_1 b_{j+1} \cdots b_n$$

implies that

$$a_2 \cdots a_m = (u_j b_1) \cdots b_{j-1} b_{j+1} \cdots b_n,$$

and by the induction hypothesis, $m - 1 = n - 1$ and $a_i = v_i b_{\tau(i)}$ for some units $v_i \in A$ and some bijection $\tau$ between $\{2, \ldots, m\}$ and $\{1, \ldots, j-1, j+1, \ldots, m\}$. However, the bijection $\tau$ extends to a permutation $\sigma$ of $\{1, \ldots, m\}$ by letting $\sigma(1) = j$, and the result holds by letting $v_1 = u_j^{-1}$. $\square$

As a corollary of Proposition 32.2. we get the converse of Proposition 32.1.

**Proposition 32.3.** *Let $A$ be a factorial ring. For any $a \in A$ with $a \neq 0$, the principal ideal $(a)$ is a prime ideal iff $a$ is irreducible.*

*Proof.* In view of Proposition 32.1, we just have to prove that if $a \in A$ is irreducible, then the principal ideal $(a)$ is a prime ideal. Indeed, if $bc \in (a)$, then $a$ divides $bc$, and by Proposition 32.2, property $(2')$ implies that either $a$ divides $b$ or $a$ divides $c$, that is, either $b \in (a)$ or $c \in (a)$, which means that $(a)$ is prime. $\square$

Because Proposition 32.3 holds, in a UFD, an irreducible element is often called a *prime*.

In a UFD $A$, every nonzero element $a \in A$ that is not a unit can be expressed as a product $a = a_1 \cdots a_n$ of irreducible elements $a_i$, and by property (2), the number $n$ of factors only depends on $a$, that is, it is the same for all factorizations into irreducible factors. We agree that this number is 0 for a unit.

**Remark:** If $A$ is a UFD, we can state the factorization properties so that they also applies to units: