and thus, $(d) = (a) + (b)$.

Assume now that

$$(d) = (a) + (b) = (a, b).$$

Since $(a) \subseteq (d)$ and $(b) \subseteq (d)$, d divides both a and b. Assume that t divides both a and b, so that $(a) \subseteq (t)$ and $(b) \subseteq (t)$. Then,

$$(d) = (a) + (b) \subseteq (t),$$

which means that t divides d, and d is indeed a gcd of a and b.

(2) By (1), if a and b are relatively prime, then

$$(1) = (a) + (b),$$

which yields the result. Conversely, if

$$ax + by = 1,$$

then

$$(1) = (a) + (b),$$

and 1 is a gcd of a and b. □

Given two nonnull elements $a, b \in A$, if a is an irreducible element and a does not divide b, then a and b are relatively prime. Indeed, if d is not a unit and d divides both a and b, then $a = dp$ and $b = dq$ where p must be a unit, so that

$$b = ap^{-1}q,$$

and a divides b, a contradiction.

Theorem 32.12. *Let A be ring. If A is a PID, then A is a UFD.*

Proof. First, we prove that every nonnull element that is a not a unit can be factored as a product of irreducible elements. Let $\mathcal{S}$ be the set of nontrivial principal ideals (a) such that $a \neq 0$ is not a unit and cannot be factored as a product of irreducible elements (in particular, a is not irreducible). Assume that $\mathcal{S}$ is nonempty. We claim that every ascending chain in $\mathcal{S}$ is finite. Otherwise, consider an infinite ascending chain

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots .$$

It is immediately verified that

$$\bigcup_{n \geq 1} (a_n)$$

is an ideal in A. Since A is a PID,

$$\bigcup_{n \geq 1} (a_n) = (a)$$