# Principal Ideal Domains and Factorization

A *principal ideal domain (PID)* is an integral domain $R$ in which every ideal is principal, i.e. of the form

$$(a) = \{ra | r \in R\}$$

for some $a \in R$.

An element $a \neq 0$ in a ring $R$ is said to be *irreducible* if $a$ is not a unit and whenever $a = bc$ then one of $b$, $c$ is a unit.

An element $a \neq 0$ of a ring $R$ is said to be *prime* if $a$ is not a unit and whenever $a|bc$ then either $a|b$ or $a|c$.

**Proposition 1.** *If $R$ is an integral domain then a prime element is necessarily irreducible.*

*Proof.* Take $a$ prime in $R$, an integral domain. Then $a$ is not a unit. Also, if $a = bc$ then $a|bc$ and so wlog we may assume $a|b$ so $b = ra$ for some $r \in R$ and so $a = arc$; as $R$ is an integral domain, $1 = rc$ and $c$ is a unit. □

**Proposition 2.** *An irreducible element in a PID is prime.*

*Proof.* Take $a$ irreducible in a PID $R$. Suppose $a|bc$. Consider

$$(a, b) = \{\lambda a + \mu b | \lambda, \mu \in R\} \triangleleft R.$$

As $R$ is a PID we have $(a, b) = d$ for some $d \in R$. Now, $d|a$ and so we can write $a = de$, say. As $a$ is irreducible, EITHER $d$ is a unit and so $(a, b) = (1) = R$ and we can write $1 = \lambda a + \mu b$ for some $\lambda, \mu \in R$ — but then $c = \lambda ca + \mu bc$, and as $a|\lambda ca$ and $a|\mu bc$ we have $a|c$; OR $e$ is a unit, in which case $d = ae^{-1}$ and $a|d$ but then $d|b$ (because $b \in (d)$) and so $a|b$. This shows that $a$ is prime. □

**Proposition 3.** *Every PID is Noetherian.*

*Proof.* Let $R$ be a PID and suppose we have an ascending chain

$$(a_1) \subset (a_2) \subset (a_3) \subset \dots$$

of ideals in $R$. Then

$$\bigcup_{i=1}^{\infty} (a_i) \triangleleft R.$$

So

$$\bigcup_{i=1}^{\infty} (a_i) = (b)$$

for some $b \in R$. So $b \in (a_k)$ for some $k$, and then

$$(b) \subset (a_k) \subset (a_{k+1}) \subset \ldots \subset (b)$$

and so

$$(a_k) = (a_{k+1}) = (a_{k+2}) = \ldots.$$

$\square$

**Proposition 4.** *In a PID, every non-zero element factorizes as a product of irreducible elements ("units are empty products").*

*Proof.* Suppose not. Then there is a non-factorizable element $a$, say. $a$ is not irreducible and so we can write $a = a_1 b_1$ a proper factorization and where we have $a_1$, say, non-factorizable. Continuing this argument we get $a_1 = a_2 b_2$, $a_2 = a_3 b_3$, and so on, proper factorizations with each $a_i$ a non-factorizable element, i.e. we have a sequence $a, a_1, a_2, a_3, \ldots$ with

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \ldots$$

contradicting Proposition 3. $\square$

**Theorem 5.** *In a PID, any non-zero element can be factorized as $a = up_1 \ldots p_k$ where $u$ is a unit, $p_1, p_2, \ldots, p_k$ are prime, and this factorization is essentially unique in the sense that if $a = up_1 \ldots p_k = vq_1 \ldots q_l$ are two prime factorizations then $k = l$ and, after renumbering the $q_i$, we have $p_i \sim q_i$, i.e. there exists a unit $w_i$ such that $p_i = w_i q_i$.*

*Proof.* In a PID we have factorization into irreducibles; but the irreducibles are prime; so any $a \neq 0$ (whether $a$ is a unit or not) can be written in the form $a = up_1 \ldots p_k$.

Suppose $a = up_1 \ldots p_k = vq_1 \ldots q_l$. Then $p_k | vq_1 \ldots q_l$ so, as $p_k$ prime, $p_k$ must divide some $q_j$ so by renumbering we can assume $p_k | q_l$. Then $p_k \sim q_l$, say $p_k = wq_l$ where $w$ is a unit. Then $up_1 \ldots p_{k-1} w q_l = vq_1 \ldots q_{l-1} q_l$ and cancelling $q_l$, we get $uwp_1 \ldots p_{k-1} = vq_1 \ldots q_{l-1}$ and so we complete by induction. $\square$