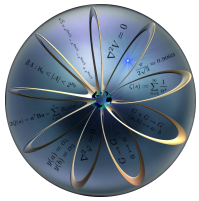

planetmath.org

Math for the people, by the people.

every PID is a UFD

Canonical name	EveryPIDIsAUFD
Date of creation	2013-03-22 16:55:51
Last modified on	2013-03-22 16:55:51
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	9
Author	rm50 (10146)
Entry type	Theorem
Classification	msc 13F07
Classification	msc 16D25
Classification	msc 11N80
Classification	msc 13G05
Classification	msc 13A15
Related topic	UFD
Related topic	UniqueFactorizationAndIdealsInRingOfIntegers

Theorem 1. *Every Principal Ideal Domain (PID) is a Unique Factorization Domain (UFD).*

The first step of the proof shows that any PID is a Noetherian ring in which every irreducible is prime. The second step is to show that any Noetherian ring in which every irreducible is prime is a UFD.

We will need the following

Lemma 2. *Every PID R is a gcd domain. Any two gcd's of a pair of elements a, b are associates of each other.*

Proof. Suppose $a, b \in R$. Consider the ideal generated by a and b, (a, b). Since R is a PID, there is an element $d \in R$ such that $(a, b) = (d)$. But $a, b \in (a, b)$, so $d \mid a, d \mid b$. So d is a common divisor of a and b. Now suppose $c \mid a, c \mid b$. Then $(d) = (a, b) \subset (c)$ and hence $c \mid d$.

The second part of the lemma follows since if c, d are two such gcd's, then $(c) = (a, b) = (d)$, so $c \mid d$ and $d \mid c$ so that c, d are associates. □

Theorem 3. *If R is a PID, then R is Noetherian and every irreducible element of R is prime.*

Proof. Let $I_1 \subset I_2 \subset I_3 \subset \ldots$ be a chain of (principal) ideals in R. Then $I_\infty = \cup_k I_k$ is also an ideal. Since R is a PID, there is $a \in R$ such that $I_\infty = (a)$, and thus $a \in I_n$ for some n. Then for each $m > n$, $I_m = I_n$. So R satisfies the ascending chain condition and thus is Noetherian.

To show that each irreducible in R is prime, choose some irreducible $a \in R$, and suppose $a = bc$. Let $d = \gcd(a, b)$. Now, $d \mid a$, but a is irreducible. Thus either d is a unit, or d is an associate of a. If d is an associate of a, then $a \mid d \mid b$ so that $a \mid b$ and c is a unit. If d is itself a unit, then we can assume by the lemma that $d = 1$. Then $1 \in (a, b)$ so that there are $x, y \in R$ such that $xa + yb = 1$. Multiplying through by c, we see that $xac + ybc = c$. But $a \mid xac$ and $a \mid ybc = ya$. Thus $a \mid c$ so that b is a unit. In either case, a is prime. □

Theorem 4. *If R is Noetherian, and if every irreducible element of R is prime, then R is a UFD.*

Proof. We show that any nonzero nonunit is R is expressible as a product of irreducibles (and hence as a product of primes), and then show that the factorization is unique.

Let $\mathcal{U} \subset R$ be the set of ideals generated by each element of R that cannot be written as a product of irreducible elements of R. If $\mathcal{U} \neq \emptyset$, then $\mathcal{U}$ has a maximal element (r) since R is Noetherian. r is not irreducible by construction and thus not prime, so (r) is not prime and thus not maximal. So there is a proper maximal ideal (s) with $(r) \subsetneq (s)$, and $s \mid r$.

Since (r) is maximal in $\mathcal{U}$, it follows that $(s) \notin \mathcal{U}$ and thus that s is a product of irreducibles. Choose some irreducible $a \mid s$; then $a \mid r$ and

$$r = ab$$

for some $b \in R$. If $(b) \notin \mathcal{U}$ (note that this includes the case where b is a unit), then b and hence r is a product of irreducibles, a contradiction. If $(b) \in \mathcal{U}$ then $(r) \subset (b)$ (since $b \mid r$). $(r) \neq (b)$ since a is not a unit, and thus $(r) \subsetneq (b)$. This contradicts the presumed maximality of (r) in $\mathcal{U}$. Thus $\mathcal{U} = \emptyset$ and each element of R can be written as a product of irreducibles (primes).

The proof of uniqueness is identical to the standard proof for the integers. Suppose

$$a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$$

where the p_i and q_j are primes. Then $p_1 \mid q_1 \cdot \ldots \cdot q_m$; since p_1 is prime, it must divide some q_j. Reordering if necessary, assume $j = 1$. Then $p_1 = u \cdot q_1$ where u is a unit. Factoring out these terms since R is a domain, we get

$$p_2 \cdot \ldots \cdot p_n = u \cdot q_2 \cdot \ldots \cdot q_m$$

We may continue the process, matching prime factors from the two sides. $\square$