equivalent definitions for UFD

Canonical name	EquivalentDefinitionsForUFD
Date of creation	2013-03-22 19:04:04
Last modified on	2013-03-22 19:04:04
Owner	joking (16130)
Last modified by	joking (16130)
Numerical id	4
Author	joking (16130)
Entry type	Theorem
Classification	msc 13G05
Related topic	UniqueFactorizationAndIdealsInRingOfIntegers

Let R be an integral domain. Define

$$T = \{u \in R \mid u \text{ is invertible}\} \cup \{p_1 \cdots p_n \in R \mid p_i \text{ is prime}\}.$$

Of course $0 \notin T$ and T is a multiplicative subset (recall that a prime element multiplied by an invertible element is again prime). Furthermore R is a UFD if and only if $T = R \backslash \{0\}$ (see the parent object for more details).

Lemma. If $a, b \in R$ are such that $ab \in T$, then both $a, b \in T$.

Proof. If ab is invertible, then (since R is commutative) both a, b are invertible and thus they belong to T. Therefore assume that ab is not invertible. Then

$$ab = p_1 \cdots p_k$$

for some prime elements $p_i \in R$. We can group these prime elements in such way that $p_1 \cdots p_n$ divides a and $p_{n+1} \cdots p_k$ divides b. Thus $a = \alpha p_1 \cdots p_n$ and $b = \beta p_{n+1} \cdots p_k$ for some $\alpha, \beta \in R$. Since R is an integral domain we conclude that $\alpha\beta = 1$, which means that both α, β are invertible in R. Therefore (for example) αp_1 is prime and thus $a \in T$. Analogously $b \in T$, which completes the proof. $\square$

Theorem. (Kaplansky) An integral domain R is a UFD if and only if every nonzero prime ideal in R contains prime element.

Proof. Without loss of generality we may assume that R is not a field, because the thesis trivialy holds for fields. In this case R always contains nonzero prime ideal (just take a maximal ideal).

,,$\Rightarrow$" Let P be a nonzero prime ideal. In particular P is proper, thus there is nonzero $x \in P$ which is not invertible. By assumption $x \in T$ and since x is not invertible, then there are prime elements $p_1, \ldots, p_k \in R$ such that $x = p_1 \cdots p_k \in P$. But P is prime, therefore there is $i \in \{1, \ldots, k\}$ such that $p_i \in P$, which completes this part.

,,$\Leftarrow$" Assume that R is not a UFD. Thus there is a nonzero $x \in R$ such that $x \notin T$. Consider an ideal (x). We will show, that $(x) \cap T = \emptyset$. Assume that there is $r \in R$ such that $rx \in T$. It follows that $x \in T$ (by lemma). Contradiction.

Since $(x) \cap T = \emptyset$ and T is a multiplicative subset, then there is a prime ideal P in R such that $(x) \subseteq P$ and $P \cap T = \emptyset$ (please, see `http://planetmath.org/Multiplicativ` entry for more details). But we assumed that every nonzero prime ideal contains prime element (and P is nonzero, since $x \in P$). Obtained contradiction completes the proof. $\square$