example of ring which is not a UFD

Canonical name	ExampleOfRingWhichIsNotAUFD
Date of creation	2013-03-22 15:08:19
Last modified on	2013-03-22 15:08:19
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	7
Author	alozano (2414)
Entry type	Example
Classification	msc 13G05
Synonym	example of a ring of integers which is not a UFD
Related topic	DeterminingTheContinuationsOfExponent
Defines	example of a number ring which is not a UFD

Example 1. We define a ring $R = \mathbb{Z}[\sqrt{-5}] = \{n + m\sqrt{-5} : n, m \in \mathbb{Z}\}$ with addition and multiplication inherited from $\mathbb{C}$ (notice that R is the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{-5})$). Notice that the only `http://planetmath.org/UnitsOfQuadraticFields`units of R are $R^\times = \{\pm 1\}$. Then:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}). \tag{1}$$

Moreover, $2,\ 3,\ 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible elements of R and they are not associates (to see this, one can compare the norm of every element). Therefore, R is not a UFD.

However, the ideals of R `http://planetmath.org/DivisibilityInRings`factor uniquely into prime ideals. For example:

$$(6) = (2, 1 + \sqrt{-5})^2 \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

where $\mathfrak{P} = (2, 1 + \sqrt{-5})$, $\mathfrak{Q} = (3, 1 + \sqrt{-5})$, and $\overline{\mathfrak{Q}} = (3, 1 - \sqrt{-5})$ are all prime ideals (see `http://planetmath.org/PrimeIdealDecompositionInQuadraticExtensionsOf` ideal decomposition of quadratic extensions of $\mathbb{Q}$). Notice that:

$$\mathfrak{P}^2 = (2), \quad \mathfrak{Q} \cdot \overline{\mathfrak{Q}} = (3), \quad \mathfrak{P} \cdot \mathfrak{Q} = (1 + \sqrt{-5}), \quad \mathfrak{P} \cdot \overline{\mathfrak{Q}} = (1 - \sqrt{-5}).$$

Thus, Eq. (**??**) above is the outcome of different rearrangements of the product of prime ideals:

$$(6) = \mathfrak{P}^2 \cdot (\mathfrak{Q} \cdot \overline{\mathfrak{Q}}) = (\mathfrak{P} \cdot \mathfrak{Q}) \cdot (\mathfrak{P} \cdot \overline{\mathfrak{Q}}).$$

Notice also that if $\mathfrak{P}$ was a principal ideal then there would be an element $\alpha \in R$ with $(\alpha) = \mathfrak{P}$ and $(\alpha)^2 = (2)$. Thus such a number α would have norm 2, but the norm of $n + m\sqrt{-5}$ is $n^2 + 5m^2$ so it is clear that there are no algebraic integers of norm 2. Therefore $\mathfrak{P}$ is not principal. Thus R is not a PID.