prime ideal factorization is unique

Canonical name	PrimeIdealFactorizationIsUnique
Date of creation	2013-03-22 18:34:24
Last modified on	2013-03-22 18:34:24
Owner	gel (22282)
Last modified by	gel (22282)
Numerical id	9
Author	gel (22282)
Entry type	Theorem
Classification	msc 13A15
Classification	msc 13F05
Related topic	DedekindDomain
Related topic	FractionalIdeal
Related topic	PrimeIdeal
Related topic	FundamentalTheoremOfIdealTheory

The following theorem shows that the decomposition of an (integral) invertible ideal into its prime factors is unique, if it exists. This applies to the ring of integers in a number field or, more generally, to any Dedekind domain, in which every nonzero ideal is invertible.

Theorem. *Let I be an invertible ideal in an integral domain R, and that*

$$I = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$$

are two factorizations of I into a product of prime ideals. Then $m = n$ and, up to reordering of the factors, $\mathfrak{p}_k = \mathfrak{q}_k$ $(k = 1, 2, \ldots, n)$.

Here we allow the case where m or n is zero, in which case such an empty product is taken to be the full ring R.

Proof. We use induction on $m + n$. First, the case with $m + n = 0$ is trivial, so suppose that $m + n > 0$. As the set of prime ideals $\mathfrak{p}_k$, $\mathfrak{q}_k$ is partially ordered by inclusion, there must be a minimal element. After reordering, without loss of generality we may suppose that it is $\mathfrak{p}_1$. Then

$$\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n \subseteq \mathfrak{p}_1,$$

so $n \geq 1$. Furthermore, as $\mathfrak{p}_1$ is prime, this implies that $\mathfrak{q}_k \subseteq \mathfrak{p}_1$ for some k. After reordering the factors, we can take $k = 1$, so that $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$.

As $\mathfrak{p}_1$ is minimal among the prime factors, we have $\mathfrak{q}_1 = \mathfrak{p}_1$. Also, $\mathfrak{p}_1$ is a factor of the invertible ideal I and so is itself invertible. Therefore, it can be cancelled from the products,

$$\mathfrak{p}_2\cdots\mathfrak{p}_m = \mathfrak{q}_2\cdots\mathfrak{q}_n.$$

The induction hypothesis gives $m = n$ and, after reordering, $\mathfrak{p}_k = \mathfrak{q}_k$ for $k = 2, \ldots, n$. $\square$