unique factorization and ideals in ring of integers

Canonical name	UniqueFactorizationAndIdealsInRingOfIntegers
Date of creation	2015-05-06 15:32:53
Last modified on	2015-05-06 15:32:53
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	17
Author	pahio (2872)
Entry type	Theorem
Classification	msc 13B22
Classification	msc 11R27
Synonym	equivalence of UFD and PID
Related topic	ProductOfFinitelyGeneratedIdeals
Related topic	PIDsAreUFDs
Related topic	NumberFieldThatIsNotNormEuclidean
Related topic	DivisorTheory
Related topic	FundamentalTheoremOfIdealTheory
Related topic	EquivalentDefinitionsForUFD

Theorem. Let O be the maximal order, i.e. the ring of integers of an algebraic number field. Then O is a unique factorization domain if and only if O is a principal ideal domain.

Proof. 1º. Suppose that O is a PID.

We first state, that any prime number π of O generates a prime ideal (π) of O. For if $(\pi) = \mathfrak{ab}$, then we have the principal ideals $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$. It follows that $(\pi) = (\alpha\beta)$, i.e. $\pi = \lambda\alpha\beta$ with some $\lambda \in O$, and since π is prime, one of α and β must be a unit of O. Thus one of $\mathfrak{a}$ and $\mathfrak{b}$ is the unit ideal O, and accordingly (π) is a maximal ideal of O, so also a prime ideal.

Let a non-zero element γ of O be split to prime number factors π_i, ϱ_j in two ways: $\gamma = \pi_1 \cdots \pi_r = \varrho_1 \cdots \varrho_s$. Then also the principal ideal (γ) splits to principal prime ideals in two ways: $(\gamma) = (\pi_1) \cdots (\pi_r) = (\varrho_1) \cdots (\varrho_s)$. Since the prime factorization of ideals is unique, the $(\pi_1), \ldots, (\pi_r)$ must be, up to the , identical with $(\varrho_1), \ldots, (\varrho_s)$ (and $r = s$). Let $(\pi_1) = (\varrho_{j_1})$. Then π_1 and ϱ_{j_1} are associates of each other; the same may be said of all pairs (π_i, ϱ_{j_i}). So we have seen that the factorization in O is unique.

2º. Suppose then that O is a UFD.

Consider any prime ideal $\mathfrak{p}$ of O. Let α be a non-zero element of $\mathfrak{p}$ and let α have the prime factorization $\pi_1 \cdots \pi_n$. Because $\mathfrak{p}$ is a prime ideal and divides the ideal product $(\pi_1) \cdots (\pi_n)$, $\mathfrak{p}$ must divide one principal ideal $(\pi_i) = (\pi)$. This means that $\pi \in \mathfrak{p}$. We write $(\pi) = \mathfrak{pa}$, whence $\pi \in \mathfrak{p}$ and $\pi \in \mathfrak{a}$. Since O is a Dedekind domain, every its ideal can be generated by two elements, one of which may be chosen freely (see the two-generator property). Therefore we can write

$$\mathfrak{p} = (\pi, \gamma), \quad \mathfrak{a} = (\pi, \delta).$$

We multiply these, getting $\mathfrak{pa} = (\pi^2, \pi\gamma, \pi\delta, \gamma\delta)$, and so $\gamma\delta \in \mathfrak{pa} = (\pi)$. Thus $\gamma\delta = \lambda\pi$ with some $\lambda \in O$. According to the unique factorization, we have $\pi \mid \gamma$ or $\pi \mid \delta$.

The latter alternative means that $\delta = \delta_1\pi$ (with $\delta_1 \in O$), whence $\mathfrak{a} = (\pi, \delta_1\pi) = (\pi)(1, \delta_1) = (\pi)(1) = (\pi)$; thus we had $\mathfrak{pa} = (\pi) = \mathfrak{p}(\pi)$ which would imply the absurdity $\mathfrak{p} = (1)$. But the former alternative means that $\gamma = \gamma_1\pi$ (with $\gamma_1 \in O$), which shows that

$$\mathfrak{p} = (\pi, \gamma_1\pi) = (\pi)(1, \gamma_1) = (\pi)(1) = (\pi).$$

In other words, an arbitrary prime ideal $\mathfrak{p}$ of O is principal. It follows that all ideals of O are principal. Q.E.D.