planetmath.org

Math for the people, by the people.

orders in a number field

Canonical name	OrdersInANumberField
Date of creation	2013-03-22 16:52:46
Last modified on	2013-03-22 16:52:46
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	17
Author	pahio (2872)
Entry type	Topic
Classification	msc 12F05
Classification	msc 11R04
Classification	msc 06B10
Related topic	Module
Defines	module
Defines	complete
Defines	order of a number field
Defines	principal order
Defines	maximal order

If $\mu_1, \ldots, \mu_m$ are elements of an algebraic number field K, then the subset

$$M = \{n_1\mu_1 + \ldots + n_m\mu_m \in K\colon\ n_i \in \mathbb{Z}\ \ \forall i\}$$

of K is a $\mathbb{Z}$-module, called a *module in K*. If the module contains as many over $\mathbb{Z}$ linearly independent elements as is the http://planetmath.org/NumberFielddegree of K over $\mathbb{Q}$, then the module is *complete*.

If a complete module in K the unity 1 of K and is a ring, it is called an *order* (in German: *Ordnung*) in the field K.

A number α of the algebraic number field K is called a *coefficient of the module M*, if $\alpha M \subseteq M$.

Theorem 1. The set $\mathcal{L}_M$ of all coefficients of a complete module M is an order in the field. Conversely, every order $\mathcal{L}$ in the number field K is a coefficient ring of some module.

Theorem 2. If α belongs to an order in the field, then the coefficients of the http://planetmath.org/CharacteristicEquationcharacteristic equation of α and thus the coefficients of the minimal polynomial of α are rational integers.

Theorem 2 means that any order is contained in the ring of integers of the algebraic number field K. Thus this ring $\mathcal{O}_K$, being itself an order, is the greatest order; $\mathcal{O}_K$ is called the *maximal order* or the *principal order* (in German: *Hauptordnung*). The set of the orders is partially ordered by the set inclusion.

Example. In the field $\mathbb{Q}(\sqrt{2})$, the coefficient ring of the module M generated by 2 and $\frac{\sqrt{2}}{2}$ is the module $\mathcal{L}_M$ generated by 1 and $2\sqrt{2}$. The maximal order of the field is generated by 1 and $\sqrt{2}$.

References

[1] S. Borewicz & I. Safarevic: *Zahlentheorie*. Birkhäuser Verlag. Basel und Stuttgart (1966).