basis of ideal in algebraic number field

Canonical name	BasisOfIdealInAlgebraicNumberField
Date of creation	2013-03-22 17:51:15
Last modified on	2013-03-22 17:51:15
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	9
Author	pahio (2872)
Entry type	Theorem
Classification	msc 12F05
Classification	msc 11R04
Classification	msc 06B10
Synonym	basis of ideal in number field
Related topic	IntegralBasis
Related topic	IdealNorm
Related topic	AlgebraicNumberTheory
Defines	basis of ideal
Defines	ideal basis
Defines	discriminant of the ideal

Theorem. Let $\mathcal{O}_K$ be the maximal order of the algebraic number field K of degree n. Every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ has a *basis*, i.e. there are in $\mathfrak{a}$ the linearly independent numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that the numbers

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n,$$

where the m_i's run all rational integers, form precisely all numbers of $\mathfrak{a}$. One has also

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$

i.e. the basis of the ideal can be taken for the system of generators of the ideal.

Since $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of the field extension $K/\mathbb{Q}$, any element of $\mathfrak{a}$ is uniquely expressible in the form $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n$.

It may be proven that all bases of an ideal $\mathfrak{a}$ have the same discriminant $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$, which is an integer; it is called the *discriminant of the ideal*. The discriminant of the ideal has the minimality property, that if $\beta_1, \beta_2, \ldots, \beta_n$ are some elements of $\mathfrak{a}$, then

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) \geqq \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \quad \text{or} \quad \Delta(\beta_1, \beta_2, \ldots, \beta_n) = 0$$

But if $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$, then also the β_i's form a basis of the ideal $\mathfrak{a}$.

Example. The integers of the quadratic field $\mathbb{Q}(\sqrt{2})$ are $l + m\sqrt{2}$ with $l, m \in \mathbb{Z}$. Determine a basis $\{\alpha_1, \alpha_2\}$ and the discriminant of the ideal a) $(6-6\sqrt{2}, 9+6\sqrt{2})$, b) $(1-2\sqrt{2})$.

a) The ideal may be seen to be the principal ideal (3), since the both generators are of the form $(l + m\sqrt{2}) \cdot 3$ and on the other side, $3 = 0 \cdot (6 - 6\sqrt{2}) + (3 - 2\sqrt{2})(9 + 6\sqrt{2})$. Accordingly, any element of the ideal are of the form

$$(m_1 + m_2\sqrt{2}) \cdot 3 = m_1 \cdot 3 + m_2 \cdot 3\sqrt{2}$$

where m_1 and m_2 are rational integers. Thus we can infer that

$$\alpha_1 = 3, \quad \alpha_2 = 3\sqrt{2}$$

is a basis of the ideal concerned. So its discriminant is

$$\Delta(\alpha_1, \alpha_2) = \begin{vmatrix} 3 & 3\sqrt{2} \\ 3 & -3\sqrt{2} \end{vmatrix}^2 = 648.$$

b) All elements of the ideal $(1-2\sqrt{2})$ have the form

$$\alpha = (a+b\sqrt{2})(1-2\sqrt{2}) = (a-4b)+(b-2a)\sqrt{2} \quad \text{with } a,\, b \in \mathbb{Z}. \tag{1}$$

Especially the rational integers of the ideal satisfy $b-2a=0$, when $b=2a$ and thus $\alpha = a-4\cdot 2a = -7a$. This means that in the presentation $\alpha = m_1\alpha_1+m_2\alpha_2$ we can assume α_1 to be 7. Now the rational portion $a-4b$ in the form (1) of α should be splitted into two parts so that the first would be always divisible by 7 and the second by $b-2a$, i.e. $a-4b = 7m_1+(b-2a)x$; this equation may be written also as

$$(2x+1)a-(x+4)b = 7m_1.$$

By experimenting, one finds the simplest value $x=3$, another would be $x=10$. The first of these yields

$$\alpha = 7(a-b)+(b-2a)(3+\sqrt{2}) = m_1\cdot 7+m_2(3+\sqrt{2}),$$

i.e. we have the basis

$$\alpha_1 = 7, \quad \alpha_2 = 3+\sqrt{2}.$$

The second alternative $x=10$ similarly would give

$$\alpha_1 = 7, \quad \alpha_2 = 10+\sqrt{2}.$$

For both alternatives, $\Delta(\alpha_1,\, \alpha_2) = 392$.