proof of basis of ideal in algebraic number field

Canonical name	ProofOfBasisOfIdealInAlgebraicNumberField
Date of creation	2013-03-22 17:56:43
Last modified on	2013-03-22 17:56:43
Owner	lalberti (18937)
Last modified by	lalberti (18937)
Numerical id	18
Author	lalberti (18937)
Entry type	Proof
Classification	msc 12F05
Classification	msc 11R04
Classification	msc 06B10

Although it is stated in a number field context this theorem is about $\mathbb{Z}$-modules. $\mathcal{O}_K$ is an integer ring, that is, it is the integral closure of $\mathbb{Z}$ in K. $\mathcal{O}_K$ is naturally endowed with a structure of $\mathbb{Z}$-module and so are all its ideals $\mathfrak{a}$. Therefore the situation is that we have a $\mathbb{Z}$-module (namely $\mathfrak{a}$) that is embedded in a finite dimensional vector space over $\mathbb{Q}$, namely K. It is a well-known fact that discrete $\mathbb{Z}$-modules of finite dimensional vector spaces over $\mathbb{Q}$ are free modules with finite rank (ie. they have a finite basis). This is exactly the claim of the theorem.
Therefore to prove the theorem we only need prove that $\mathfrak{a}$ is discrete (K is by definition a finite dimensional vector space over $\mathbb{Q}$ as it is an algebraic number field). Let $E := \mathbb{Q}\mathfrak{a}$, it is a finite dimensional $\mathbb{Q}$-vector subspace of K. Let n be the dimension of K over $\mathbb{Q}$, and k the dimension of E over $\mathbb{Q}$. To say that $\mathfrak{a} \subset K \cong \mathbb{Q}^n$ is a discrete $\mathbb{Z}$-module of K is equivalent to say that every sequence of elements of $\mathfrak{a}$ that converges in $\mathfrak{a}$ for the usual `http://planetmath.org/NormedVectorSpace`Euclidian norm (ie. for $x = (x_1, \ldots, x_n)\mathbb{R}^n$, $||x||^2 = \sum_{i=1}^n x_i^2$) is ultimately constant. It suffices to prove this for sequences that converges to 0 (instead of an arbitrary element of $\mathfrak{a}$) because $\mathfrak{a}$ is stable subset under addition (one can transform a sequence converging to any element of $\mathfrak{a}$ into a sequence converging to 0 by subtracting that element to the sequence).
Suppose there is a sequence of $\mathfrak{a}$ that converges to 0, we want to prove that this sequence is ultimately constant with value 0. The elements of $\mathfrak{a}$ can be seen as $\mathbb{Q}$-linear endomorphisms of K, and their characteristic polynomials have coefficients in $\mathbb{Z}$ as they are in the integral closure of $\mathbb{Z}$. In particular the determinant of these endomorphisms (which is called norm in this context) is an integer (the determinant is the constant coefficient of the characteristic polynomial), and if it were possible to find a sequence of elements of $\mathfrak{a}$ that converges to 0 the determinant would also converge to 0 as it is a continuous function. But it has just been said that the the determinant is an integer for any element of $\mathfrak{a}$, therefore for the determinants of the elements of the sequence to converge to 0 they have to be ultimately 0, that is from a certain point on, the sequence is constantly equal to 0. Since K is a field all the mappings but the 0 mapping, are injective and therefore have non-zero norm. Therefore if the norm of the elements is 0, it means that the elements themselves were 0. Hence we have proved that the sequence that converged to 0 was ultimately evenly 0. We have thus proved that $\mathfrak{a}$ is a discrete $\mathbb{Z}$-module of K.

As a reminder, here is a proof of the afore-mentioned "well-known fact"

that a discrete submodule of a finite dimensional vector space over $\mathbb{Q}$ has a basis:
First, we prove that can find a finite set of generators $\mathfrak{B}$ of E whose elements are in $\mathfrak{a}$. This is a straightforward induction on the dimension of $\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$: start with $\mathfrak{B} = \emptyset$, if there is element in E that is not in $\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$, then there is an element of $\mathfrak{a}$ that lies outside $\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$, add that element to $\mathfrak{B}$ and keep on doing this until $\dim \mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B}) = \dim E$.
At that point $E/\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$ is a finite set: the quotient $E/\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$ can be represented as the subset of $\mathbb{Q}^{\dim E}$ of elements whose projections to the element of $\mathfrak{B}$ lies in $[0, 1]$. In other words $E/\mathrm{Vect}_{\mathbb{Q}}(\mathfrak{B})$ is isomorphic to the torus $\sum_{i=1}^{i=\dim E}[0, 1]\mathfrak{B}_i$. This is a compact set, and therefore as $\mathfrak{a}$ is discrete there are only finitely many elements of $\mathfrak{a}$ that lie in the torus. Therefore by adding the element of $\mathfrak{a}$ that lie in the torus to $\mathfrak{B}$, one obtains a finite set of generators of $\mathfrak{a}$.
As $\mathbb{Z}$ is a principal ideal ring, it is again well-known that modules with finite rank (ie. that admit a finite set of generators) over a principal ideal ring can be represented as the product of a free module times a torsion module (with finite rank). Here there is no torsion as it would mean there is an element of $\mathfrak{a}$ that is sent to 0 by multiplication by an integer, and this is impossible as integers are elements of K and K is a field. Therefore $\mathfrak{a}$ itself is a free module (with finite rank).

The discriminant property can be seen intrinsically. Given an algebra of linear maps, here $\mathfrak{a}$, one can define the symmetric bilinear map $a, b \in E \mapsto \mathrm{Tr}(ab)$. If the algebra happens to have a basis, which we have just proved in our case, then the determinant of that map can be computed using the basis and this is what is called discriminant. But of course, the determinant of that map is not dependent on the basis...

The minimality property is in fact a property of Gram matrices for scalar products. The elements of $\mathfrak{a}$ can be represented as elements of $\mathrm{End}(E, E) \cong \mathbb{R}^{(\dim E)^2}$ as they are linear endomorphisms of E. The bilinear map $a, b \in E \mapsto \mathrm{Tr}(ab)$ is then no more than the Gram matrix associated to the vectors of the basis $\alpha_1, \ldots, \alpha_k$ of $\mathfrak{a}$. Indeed, taking the trace of the product of two matrices it no more than taking the sum of the pairwise products of the entries of the two matrices. The determinant of the Gram matrix is the square of the scalar factor by which volume of the unit ball is multiplied when taking its image through $\phi_\alpha : (\lambda_1, \ldots, \lambda_k) \in \mathbb{R}^{dimE} \mapsto \sum_i \lambda_i \alpha_i \in \mathrm{End}(E, E) \cong \mathbb{R}^{(dimE)^2}$. When computing the discriminant of the β_i, we look at the multiplication factor introduced by the map ϕ_β. But if M is the map that associates to the β_i their expression in terms of the α_i then $\phi_\beta = \phi_\alpha \circ M$. Therefore $\Delta(\beta_i) = det(M)^2 \Delta(\alpha_i)$. If the $\beta_1, \ldots, \beta_n$ are not linearly independent then the multiplication factor is 0 (the ball is flattened), if they are linearly independent det(M) is an integer (the β_i are linear combination of the α_i with integer coefficients), therefore $\Delta(\beta_i) \geq \Delta(\alpha_i)$. Finally $\Delta(\beta_i) = \Delta(\alpha_i)$ is equivalent to $\det(M) = 1$ which in turn is equivalent to M is invertible (1 is the only positive invertible element of $\mathbb{Z}$), which exactly means that β_i is a basis $\underline{\text{iff}}$ $\Delta(\beta_i) = \Delta(\alpha_i)$.