Let K we a number field of degree n over the rationals.

Dual basis

Let $\omega_1, ..., \omega_n$ be a basis for K over k and choose n elements, $c_1, ..., c_n$, in k. We know that the $n \times n$ matrix, $\text{Tr}(\omega_i \omega_j)$, is non-singular since

$$0 \neq \text{disc}(\omega_1, ..., \omega_n) = |\text{Tr}(\omega_i \omega_j)|^2$$

This means that there is a unique solution, $x_1, ..., x_n \in k$, to the n equations

$$\sum_{j=1}^{n} \text{Tr}(\omega_i \omega_j) x_j = \frac{c_i}{n} \quad (i = 1, ..., n)$$

Let $\alpha = \sum_{j=1}^{n} x_j \omega_j$. Using rules of the trace, we get for any i that

$$c_i = \sum_{j=1}^{n} \text{Tr}(x_j \omega_i \omega_j) = \text{Tr}(\sum_{j=1}^{n} x_j \omega_i \omega_j) = \text{Tr}(\alpha \omega_i)$$

Thus, we have demonstrated that for any choice of $c_1, ..., c_n \in k$, there is a unique $\alpha \in K$ such that $\text{Tr}(\alpha \omega_i) = c_i$. Now choose $c_{ij} = \delta_{ij}$, where δ_{ij} is the Kronecker delta. For every $i = 1, ..., n$ we get a unique $\omega_i^* \in K$ such that $\text{Tr}(\omega_i^* \omega_j) = c_{ij}$ for $j = 1, ..., n$. We call $\omega_1^*, ..., \omega_n^*$ the dual basis of $\omega_1, ..., \omega_n$. It is indeed a basis. Assume that

$$\sum_{i=1}^{n} x_i \omega_i^* = 0.$$

Multiplying by ω_j and taking the trace, we get

$$0 = \text{Tr}(\sum_{i=1}^{n} x_i \omega_i^* \omega_j) = \sum_{i=1}^{n} x_i \text{Tr}(\omega_i^* \omega_j) = x_j,$$

which shows that all the x_j's are zero.

Forms and Modules

A form $F(x_1, ..., x_m)$ of degree k is a homogenous polynomial in the variables $x_1, ..., x_m$, of degree k with coefficients in $\mathbb{Q}$. If it splits into linear factors in some extension of $\mathbb{Q}$, then it is called decomposable. It is called reducible if it can be written as the product of two forms of lower degree. Otherwise it is called irreducible. Two forms are called equivalent if one can be obtained from the other by a linear change of variables with coefficients in $\mathbb{Q}$. This defines an equivalence relation on the set of forms. Consider the equation

$$F(x_1, ..., x_m) = a$$

where a is in $\mathbb{Q}$.

Once we know the solutions to one form, we can transform them into solutions of an equivalent form. Thus, we

Let $\mu_1, ..., \mu_k$ be elements in K. The set, M, consisting of all $\mathbb{Z}$-linear combinations of these is called a module in K and the μ_i's are called the generators of the module. If M contains a basis for the vector space $K/\mathbb{Q}$, then it is called a **full module**. Otherwise it is called a **nonfull module**. By definition M is a finitely generated abelian group and by the structure theorem, M determines uniquely integers $r, s \geq 0$ and $d_1 \mid ... \mid d_s$, $d_i \geq 2$ such that

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_s\mathbb{Z}$$

But M lives inside a field, which has no zero divisors, so M must be a torsion-free $\mathbb{Z}$-module, and so $s = 0$. Thus, $M \cong \mathbb{Z}^r$, which means that M is a free abelian group of rank r. The modules in K can therefore be thought of as the finitely generated free abelian groups inside K - This means that concepts such as rank and basis now make sense for modules. In general, if we have a basis for N, say $\mu_1, ..., \mu_m$ and we choose to consider $\mathbb{Q}$-linear combinations of these, say

$$a_1\mu_1 + ... + a_m\mu_m = 0 \tag{1}$$

Then we can always find an integer $c \neq 0$ so that ca_i is an integer for all i. For example we can choose c to be th product of all denominators of the a_i, all of which are non-zero. So if $m > n$ then we would be able to choose at least one of the a_i to be non-zero. But that would mean that multiplying (1) by a suitable c would yield a non-trivial Z-linear combination, which is a contradiction. Hence the rank of a module has to be smaller than or equal to n. If N has rank $m = n$, then N is a full module, because multiplication by c in (1) will give a $\mathbb{Z}$-linear combination of the μ_i's which is zero, which implies that the a_i's are all zero. On the other hand, if N is a full module, then it has rank n since a basis for K over $\mathbb{Q}$ descends to a basis over $\mathbb{Z}$. Thus the full modules are exactly the modules of rank n, and the nonfull modules are those of rank less than n.

Once we have a module, we can of course consider the norm of the elements in it. Let $\sigma_1, ..., \sigma_n$ be the n embeddings of K into $\mathbb{C}$. We then have

$$N(x_1\mu_1 + ... + x_k\mu_k) = \prod_{i=1}^{n} \sigma_i(x_1\mu_1 + ... + x_k\mu_k) = \prod_{i=1}^{n} x_1\sigma_i(\mu_1) + ... + x_k\sigma_i(\mu_k)$$

Any term in this product occurs from choosing one of the k terms in each of the n factors, so multiplying this expression out, we get a homogenous polynomial in the variables $x_1, ..., x_n$. Let us think about what the coefficients of this polynomial are. Any term will have the form

$$x_{i_1}\sigma_1(\mu_{i_1}) \dots x_{i_n}\sigma_n(\mu_{i_n}) = x_{i_1}...x_{i_n}\sigma_1(\mu_{i_1})...\sigma_n(\mu_{i_n})$$

where the i_j signify which of the k terms in the n factors we chose. There could be many choices that lead to the same monomial, $x_{i_1}...x_{i_n}$. As such, the coefficient of this monomial will be

$$\sum_i \sigma_1(\mu_{i_1})...\sigma_n(\mu_{i_n})$$

where each i in the sum corresponds to a unique way of choosing the k terms in the n factors. Acting with an embedding on the set of all embeddings will simply permute them. Thus, acting with an embedding on the above sum will just permute the order in which the terms are added. Thus, the sum is fixed by all embeddings. But this means that all coefficients are fixed by every single embedding, which means that the coefficients are in $\mathbb{Q}$. Hence,

$$F(x_1, ..., x_k) = N(x_1\mu_1 + ... + x_k\mu_k)$$

is a form, and we call it the form associated to the generators $\mu_1, ..., \mu_k$, of the module. Since there may be many generators that lead to the same module, the forms achieved in this way may not be equal. However, it turns out that they are equivalent. If $\nu_1, ..., \nu_s$ is another set of generators for the same module, then we can write each ν_i as a $\mathbb{Z}$-linear combination of the μ_i's, i.e. for $j = 1, ..., s$, we have $\nu_j = \sum_{i=1}^k a_{ij}\mu_i$. Set for each $j = 1, ..., k$

$$x_j = \sum_{i=1}^s a_{ji}y_i$$

We see that

$$\sum_{i=1}^s y_i\nu_i = \sum_{i=1}^s y_i \sum_{j=1}^k a_{ji}\mu_j = \sum_{j=1}^k (\sum_{i=1}^s a_{ji}y_i)\mu_j = \sum_{j=1}^k x_j\mu_j$$

Which means that the forms associated to the generators $\mu_1, ..., \mu_k$ and $\nu_1, ..., \nu_s$ are equivalent.

We have seen that it is possible to construct forms from modules. The other direction is also possible. We have the theorem

Theorem 0.1.

Because of this correspondence between forms and norms of elements, we will now spend some more time investigating norms.

Coefficient rings and orders

An **order** in K is a full module in K which is also a ring with unity. We will now give a way of constructing such a ring. Given a full module M in K, we can consider an element α in K so that $\alpha M \subseteq M$. Such an element is called a **coefficient** of M, and the set of all of these is called the **coefficient ring** of M, which we will denote by $\mathfrak{O}_M$, or simply $\mathfrak{O}$, when it is clear from the context what is meant. It would be strange to call this object a ring, if it wasn't a ring, so let us check that it is. We check that $\mathfrak{O}$ is a subring of K. First it is clear that $1 \in \mathfrak{O}$ since $1M \subseteq M$ and so $\mathfrak{O}$ is non-empty. Let now α, β in $\mathfrak{O}$ and take any element in x in M. We have

$$(\alpha - \beta)x = \alpha x - \beta x \in M$$

Thus, $\alpha - \beta \in \mathfrak{O}$. Checking that we have closure under multiplication is similar and so by the subring criterion $\mathfrak{O}$ is a subring of K, In fact, $\mathfrak{O}$ is also a full module. If γ is any non-zero element of M, then $\gamma\mathfrak{O}$ is a group under addition and we have that $\gamma\mathfrak{O} \subseteq M$. Thus, $\gamma\mathfrak{O}$ is a module since subgroups of modules are modules. But then also $\mathfrak{O} = \gamma^{-1}\gamma\mathfrak{O}$ is a module. We next show that $\mathfrak{O}$ is full. Let $\alpha \in K$ be a non-zero element, and suppose $\mu_1, ..., \mu_n$ is a basis for M which is also a basis for K over $\mathbb{Q}$. Then for each i we can find a_{ij} in $\mathbb{Q}$ so that

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j$$

Choose now an integer, $c \neq 0$ so that ca_{ij} is an integer for all i, j. This implies that $c\alpha\mu_i$ is in M for all i. But this means that $c\alpha x$ is in M for any x in M, which means that $c\alpha$ is in $\mathfrak{O}$. This means that we can find non-zero integers, $c_1, ..., c_n$, so that $c_1\mu_1, ..., c_n\mu_n$ are all in $\mathfrak{O}$. This is clearly still a basis for K over $\mathbb{Q}$, which means that $\mathfrak{O}$ is full, and so $\mathfrak{O}$ is an order in K.

We now show that is also full. Let α be in K^* and consider the induced $\mathbb{Q}$ linear isomorphism from K to itself For any γ in M, we have a map $\mathfrak{O} \to M$ given by

$$\phi(x) = \gamma x$$

If γ is non-zero, then ϕ is clearly injective. If $\gamma x = y$ for some y in M, then we get $x = \gamma^{-1}y$.

Thus, there is an integer c so that $c\alpha$ is in M.

Solutions to $N(\mu) = a$, where μ is in a full module

Let $\mathfrak{O}$ be the coefficient ring of a full module M and assume that

$$N(\mu) = a,$$

for some μ in M. We have that $\epsilon\mu$ is in M if and only if ϵ is in $\mathfrak{O}$. So take now $\epsilon\mu \in M$ with $\epsilon \in \mathfrak{O}$. We get

$$N(\epsilon\mu) = N(\epsilon)N(\mu) = aN(\epsilon)$$

This means that a single solution to So if ϵ has norm 1, also $\epsilon\mu$ will be a solution. The units of $\mathfrak{O}$ are the elements with norm ±1.

Maybe all we really need to show is what all of these solutions are like. Maybe we do not need all the other parts.

Only finite many solutions up to associates

Let K/k be a finite extension of fields. If α is in K, we get a k-linear map $x \mapsto \alpha x$ from K to itself. Suppose that $\mu_1, ..., \mu_n$ is a basis for K over k. Then we can write each $\alpha\mu_i$ as a k-linear combination of the basis, or equivalently, we can find a matrix A so that

$$\begin{pmatrix} \alpha\mu_1 \\ \vdots \\ \alpha\mu_n \end{pmatrix} = A \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$$

We say that A is the matrix representation of the linear map $x \mapsto \alpha x$ with respect to the basis $\mu_1, ..., \mu_n$. The characteristic polynomial for α relative to the extension K/k, is then defined to be the characteristic polynomial of A which is defined to be

$$\phi(x) = \det(xI - A)$$

This polynomial is monic and it has coefficients which are polynomial expressions of the entries of A. From the above we observe that

$$0 = (\alpha I - A) \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$$

Thus, each row of $\alpha I - A$ induces a linear combination of our basis which is zero, which means that the rows are 0, hence the entire matrix is 0. Thus, $\phi(\alpha) = \det(\alpha I - A) = 0$.

Consider now a number field K with degree n over $\mathbb{Q}$. If α now is an element in an order $\mathfrak{O} \subseteq K$, and $\mu_1, ..., \mu_n$ is a basis for $\mathfrak{O}$ then we can write each $\alpha\mu_i \in \mathfrak{O}$ as a linear combination with coefficients in $\mathbb{Z}$, which means that the matrix representation of $x \mapsto \alpha x$ has integer entries, so the characteristic polynomial of α has integer coefficients, and α is a root. Hence α is an algebraic integer, so also the minimal polynomial of α, m_α, has integer coefficients. Both the trace and the norm occur as coefficients in m_α, so these quantities are also integers.

The ring $\mathfrak{O}$ is in particular a free abelian group of rank n, hence isomorphic to $\mathbb{Z}^n$. As $\mathfrak{O}$ is abelian, the subgroup $c\mathfrak{O}$, where $c \in \mathbb{N}$, is normal in $\mathfrak{O}$. We can therefore quotient out this subgroup to get the isomorphism

$$\mathfrak{O}/c\mathfrak{O} \cong \mathbb{Z}^n/c\mathbb{Z}^n \cong (\mathbb{Z}/c\mathbb{Z})^n$$

Now, $\mathbb{Z}/c\mathbb{Z}$ contains c elements, which means that

$$c^n = \#(\mathbb{Z}/c\mathbb{Z})^n = \#\mathfrak{O}/c\mathfrak{O}$$

Denote by $\bar{\alpha}$ the image of α in $\mathfrak{O}/c\mathfrak{O}$. Assume that $\bar{\alpha} = \bar{\beta}$ and that $|N(\alpha)| = |N(\beta)| = c$. We show that α and β are associates. Our assumptions give us that

$$\alpha = \beta + c\gamma = \beta + |N(\beta)|\gamma,$$

for some γ in $\mathfrak{D}$. So if β divides $|N(\beta)|$ in $\mathfrak{D}$, it follows that β divides α and a similar argument can be carried out to show that α divides β. Both of these together is the same as saying that α and β are associates. We now show that β divides $|N(\beta)|$ in $\mathfrak{D}$. Consider the minimal polynomial, m_β, for β over $\mathbb{Q}$. This polynomial has coefficients in $\mathbb{Z}$. Plugging in β into this polynomial we get

$$0 = m_\beta(\beta) = \beta^k + a_{k-1}\beta^{k-1} + ... + a_0$$

where $a_0 = N(\beta)$ is the constant term. Solving for a_0 we get

$$N(\beta) = -\beta(\beta^{k-1} + a_{k-1}\beta^{k-2} + ... + a_1).$$

The sum in the parenthesis is an element of $\mathfrak{D}$ because the a_i are integers and β^i is in $\mathfrak{D}$ for all $i \in \mathbb{N}$. This shows that β divides $N(\beta)$ in $\mathfrak{D}$. Thus β will also divide $\gamma N(\beta)$ for any γ in $\mathfrak{D}$, so in particular it will divide $|N(\beta)|$. We have now shown that α and β are associates. Take now a maximal set of pairwise non-associates in $\mathfrak{D}$ all with absolute norm c, and call it A. These must all map to distinct elements in $\mathfrak{D}/c\mathfrak{D}$; Otherwise we would have a contradiction to what we have just shown. This means that

$$\#A \leq \#\mathfrak{D}/c\mathfrak{D} = c^n$$

We have shown that there are only finitely many solutions to $|N(\alpha)| = c$, $\alpha \in \mathfrak{D}$, up to associates. Therefore there are also only finitely many solutions to $N(\alpha) = c$ up to associates.

Skolem's Method

Let K be a number field of degree n and let $\mu_1, ..., \mu_m$ be a set of $\mathbb{Q}$-linearly independent elements of K. These generate a nonfull module, M. Starting from these generators we can build a basis for K over $\mathbb{Q}$. We will call this basis $\mu_1, ..., \mu_m, \mu_{m+1}, ..., \mu_n$. Considering the module, call it $\bar{M}$, generated by these will give us a full module and $M \subset \bar{M}$. We wish to find solutions to the equation $N(\alpha) = a$, where α is in M. This is really the same as allowing α to be in $\bar{M}$, so finding solutions of the form

$$\alpha = \sum_{i=1}^{n} x_i \mu_i$$

where the x_i are in $\mathbb{Z}$, with the added restriction that

$$x_{m+1} = ... = x_n = 0$$

Let now $\mu_1^*, ..., \mu_m^*$ be the dual basis of $\mu_1, ..., \mu_m$. The computation

$$\mathrm{Tr}(\mu_i^* \alpha) = \mathrm{Tr}(\sum_{j=1}^{n} \mu_i^* x_j \mu_j) = \sum_{j=1}^{n} x_j \mathrm{Tr}(\mu_i^* \mu_j) = x_i$$

shows that we can recover the x_i variables in α by taking the trace of $\mu_i^* \alpha$. We can use this to reformulate the above restriction to

$$\text{Tr}(\mu_m^* \alpha) = ... = \text{Tr}(\mu_n^* \alpha) = 0$$

Since α has norm a, we can write $\alpha = \gamma_k \epsilon_1^{u_1} ... \epsilon_n^{u_r}$, $u_i \in \mathbb{Z}$, where γ is taken from a finite set of elements with norm a, and the ϵ_i is a system of independent units of K. Let $\sigma_1, ..., \sigma_n$ be the embeddings of K into $\mathbb{C}$. The restriction on the last $n - m$ variables can be written as

$$\text{Tr}(\mu_j^* \alpha) = \sum_{i=1}^{n} \sigma_i(\gamma \mu_j^* \epsilon_1^{u_1} ... \epsilon_n^{u_r}) = \sum_{i=1}^{n} \sigma_i(\gamma_k \mu_j^*) \sigma_i(\epsilon_1)^{u_1} ... \sigma_i(\epsilon_n)^{u_r} = 0$$

for $j = m + 1, ..., n$. If we can show that, for each of these equations, there are only finitely many possibilites for the u_i's, then because there are also finitely many γ's, we would have established that there are only finitely many $\alpha \in M$ such that $N(\alpha) = a$. Right now, the u_i live in $\mathbb{Z}$, but if we