EMBEDDING OF AN ORDER INTO A MAXIMAL ORDER

Horst G. Zimmer

(Springer LNM 262 [1972] pp 25–27)

Let there be given a finite dimensional commutative algebra $\mathfrak{A}$ of degree n over $\mathbb{Q}$ and an order $\mathfrak{o}$ in $\mathfrak{A}$ such that

$$\mathfrak{A} \;=\; \mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

It is our goal to find the maximal order $\mathfrak{O}$ in $\mathfrak{A}$ containing $\mathfrak{o}$. We assume the order $\mathfrak{o}$ in $\mathfrak{A}$ to be defined by means of a basis $\omega_1, \omega_2, \ldots, \omega_n$ over $\mathbb{Z}$ together with a multiplication table. All orders in $\mathfrak{A}$ considered in this section are also supposed to be given by a $\mathbb{Z}$-basis that is expressed in terms of the basis ω_1, $\omega_2, \ldots, \omega_n$ of $\mathfrak{o}$.

The task proposed was first solved by Berwick (1927). Subsequently, Zassenhaus (1967) developed a more general algorithm which was implemented in the form of an effective computer program. The basic idea is to build up a tower of intermediate orders

$$\mathfrak{o} \subset \mathfrak{o}_1 \subset \cdots \subset \mathfrak{o}_m \subset \mathfrak{o}_{m+1} \subset \cdots \subset \mathfrak{O}$$

so as to reach $\mathfrak{O}$ after a finite number of steps.

A remark concerning effectiveness is in order. The maximal order $\mathfrak{O}$ over $\mathfrak{o}$ sought cannot be effectively constructed by a search procedure which finds $\mathfrak{O}$ among all (finitely many) orders between $\mathfrak{o}$ and $d^{-1}\mathfrak{o}$ where d is the discriminant of $\mathfrak{o}$.

Rather we proceed in the following fashion. Let us assume that we have arrived already at an intermediate order $\mathfrak{o}_m$ and that $\mathfrak{o}_m \neq \mathfrak{O}$. We wish to construct $\mathfrak{o}_{m+1}$. To this end we introduce for a rational prime p the *p-radical* of $\mathfrak{o}$, $\mathfrak{R}_{p,m}$, that is, the ideal containing $p\mathfrak{o}_m$ which is defined by

$$\mathfrak{R}_{p,m} \;=\; \bigl\{\, x \in \mathfrak{o}_m \;\big|\; x \bmod p\mathfrak{o}_m \text{ is nilpotent} \,\bigr\}.$$

The construction of $\mathfrak{o}_{m+1}$ is now based on the following

Theorem. *Suppose that $\mathfrak{o}_m \neq \mathfrak{O}$. Then there exists a prime p, whose square divides the discriminant d_m of the order $\mathfrak{o}_m$, such that the $\mathfrak{o}_m$-quotient module $[\mathfrak{R}_{p,m}/\mathfrak{R}_{p,m}]$ is an order in $\mathfrak{A}$ that contains $\mathfrak{o}_m$ properly.*

Here, the quotient module $[\mathfrak{R}_{p,m}/\mathfrak{R}_{p,m}]$ consists of those elements in $\mathfrak{A}$ which multiply $\mathfrak{R}_{p,m}$ into itself.

On the grounds of this theorem we know that, amongst all primes p with $p^2 \mid d_m$, there can be found a prime (the smallest such) for which the definition

$$\mathfrak{o}_{m+1} \;=\; [\mathfrak{R}_{p,m}/\mathfrak{R}_{p,m}]$$

yields an order $\mathfrak{o}_{m+1}$ properly containing $\mathfrak{o}_m$. As soon as an intermediate order $\mathfrak{o}_h$ in the above tower is found for which there is no prime p with $p^2 \mid d_h$ such that $[\mathfrak{R}_{p,h}/\mathfrak{R}_{p,h}]$ properly contains $\mathfrak{o}_h$, the desired maximal order

$$\mathfrak{O} \;=\; \mathfrak{o}_h$$

has been reached.

Note that the discriminants d_m and d_{m+1} of the orders $\mathfrak{o}_m$ and $\mathfrak{o}_{m+1}$ respectively are subject to the relation

$$d_m \;=\; (\det T_m)^2 d_{m+1}$$

where T_m^{-1} is the $n \times n$ transition matrix over $\mathbb{Z}$ by which a $\mathbb{Z}$-basis of $\mathfrak{o}_{m+1}$ is expressed in terms of a $\mathbb{Z}$-basis of $\mathfrak{o}_m$. From this remark it can also be seen that there is only a finite number of candidates $\mathfrak{o}_m$ competing for $\mathfrak{O}$.

In order to obtain a $\mathbb{Z}$-basis of $\mathfrak{o}_{m+1}$ from a $\mathbb{Z}$-basis of $\mathfrak{o}_m$ we use the *p-trace radical* of $\mathfrak{o}_m$, that is, the ideal

$$\mathfrak{T}_{p,m} \;=\; \bigl\{\, x \in \mathfrak{o}_m \;\big|\; \mathrm{tr}(x\mathfrak{o}_m) \subseteq p\mathbb{Z} \,\bigr\},$$

where tr denotes the trace function belonging to the regular representation of $\mathfrak{o}_m$. We have then

$$p\mathfrak{o}_m \;\subseteq\; \mathfrak{R}_{p,m} \;\subseteq\; \mathfrak{T}_{p,m}$$

with the equality sign standing on the right hand side whenever $p > n$. Using these inclusions we first determine a suitable $\mathbb{Z}$-basis for $\mathfrak{T}_{p,m}$ in terms of a $\mathbb{Z}$-basis of $\mathfrak{o}_m$ and then derive from it a $\mathbb{Z}$-basis for $\mathfrak{R}_{p,m}$ and, finally, a $\mathbb{Z}$-basis for $[\mathfrak{R}_{p,m}/\mathfrak{R}_{p,m}]$. All this is accomplished by matrix operations involving matrices with entries in $\mathbb{Z}$.

The effectiveness of this algorithm can be further improved by dealing simultaneously rather than separately with those primes p for which

$$p^2 \mid d \quad\text{and}\quad p > n.$$

Specifically, on defining the number

$$d_0 \;=\; \textstyle\prod_{p^2 \mid d,\; p>n} p$$

we introduce the ideals $\mathfrak{R}_{d_0,m}$, $\mathfrak{T}_{d_0,m}$ instead of $\mathfrak{R}_{p,m}$, $\mathfrak{T}_{p,m}$ respectively and proceed in an analogous manner to that outlined above.

The algorithm is naturally of particular interest in the case in which $\mathfrak{A} = K$ is a finite algebraic number field over $\mathbb{Q}$ because it facilitates the construction of the ring $\mathfrak{O}$ of all algebraic integers in K.