Supplement on computing integral bases

Let F be an algebraic number field and $\mathcal{O}_F \subset F$ the ring of algebraic integers in F. Recall that one can always easily construct a $\mathbb{Q}$-basis B for F that consists entirely of algebraic integers, i.e., $B \subset \mathcal{O}_F$ (how?). However, such a basis will not necessarily be an *integral basis* in the sense defined in class, that is, a basis such that $\mathrm{Span}_{\mathbb{Z}} B = \mathcal{O}_F$. We saw that B is an integral basis if and only if $|\Delta(B)|$ is minimal among bases that are contained in $\mathcal{O}_F$. We wish to write out in more detail the algorithm for determining if a given basis is an integral basis, and for computing an integral basis if the given one is not. To check whether or not B is an integral basis, we need to see if there are elements $\alpha \in \mathcal{O}_F$ that are not in the $\mathbb{Z}$-span of B.

Lemma 0.1 *If $Span_{\mathbb{Z}} B = \{b_1, b_2, \ldots, b_n\} \subsetneq \mathcal{O}_F$ then there is an element $\alpha \in \mathcal{O}_F$ of the form*

$$\alpha = (1/p) \sum_{i=1}^{n} r_i b_i$$

where
(1) p is a prime such that $p^2 | \Delta(B)$;
(2) $r_i \in \{0, 1, \ldots, p-1\}$; and
(3) $r_j = 1$ for some index j.

Proof.

Note first that if $c \in \mathrm{Span}_{\mathbb{Z}} B$, then $x \in \mathrm{Span}_{\mathbb{Z}} B$ iff $x + c \in \mathrm{Span}_{\mathbb{Z}} B$. In particular, if $x \notin \mathrm{Span}_{\mathbb{Z}} B$, then $x + c \notin \mathrm{Span}_{\mathbb{Z}} B$. Furthermore, since B is a $\mathbb{Q}$-linearly independent set, any way of writing an element $x \in F$ as a $\mathbb{Q}$-linear combination of B is unique. Thus, if $x = \sum c_i b_i$ for $c_i \in \mathbb{Q}$ such that some $c_i \notin \mathbb{Z}$, then $x \notin \mathrm{Span}_{\mathbb{Z}} B$. That is, there is no other way to write it as an integral combination of elements of B.

Now to the proof. By assumption, there is a $\beta \in \mathcal{O}_F \setminus \mathrm{Span}_{\mathbb{Z}} B$. But since B is a $\mathbb{Q}$-linear basis of F, β is in the $\mathbb{Q}$-span of B. So we can write

$$\beta = (1/N) \sum c_i b_i$$

for $N \in \mathbb{Z}$, $N \neq \pm 1$, and $c_i \in \mathbb{Z}$, not all divisible by N. In fact, after dividing out all extraneous factors, we can assume that $\mathrm{hcf}(N, c_1, \ldots, c_n) = 1$. Let p be a prime divisor of N. Then there is some j such that $p \nmid c_j$. But then $\beta' = (N/p)\beta \in \mathcal{O}_F$ has the expression

$$\beta' = (1/p) \sum c_i b_i$$

and $p \nmid c_j$ so $\beta' \notin \mathrm{Span}_{\mathbb{Z}} B$. Using Bezout's lemma, find $k, l \in \mathbb{Z}$ such that $kc_j + lp = 1$. Then $\beta'' = k\beta' + lb_j \in \mathcal{O}_F$ can be written

$$\beta'' = (1/p) \sum s_i b_i$$

with $s_j = 1$, and hence, $\beta'' \notin \mathrm{Span}_{\mathbb{Z}} B$. For each i, we can apply the division algorithm to write $s_i = m_i p + r_i$ for a unique $r_i \in \{0, 1, \ldots, p-1\}$. Note that since $s_j = 1$, we have $m_j = 0$ and $r_j = 1$. We see that

$$\alpha = \beta'' - \sum m_i b_i = (1/p) \sum r_i b_i$$

then satisfies the conditions of the lemma, except we need to check that $p^2 \mid \Delta(B)$. We replace the basis B by the basis of algebraic integers B' with b_j removed from B and α added instead. The change of basis matrix is

$$C = (C_1, C_2, \ldots, C_n)$$

where the i-th column C_i for $i \neq j$ is the standard basis vector e_i with 1 in the i-th entry and zero elsewhere, while C_j is the vector $(r_1/p, r_2/p, \ldots, r_n/p)^T$. So we see easily that $\det(C) = \pm 1/p$. Therefore,

$$\Delta(B') = \Delta(B)/p^2.$$

But we know that $\Delta(B') \in \mathbb{Z}$. So we must have $p^2 \mid \Delta(B)$. $\square$

Starting from a given basis B, we compute $\Delta(B)$. If $\Delta(B)$ is square-free, that is, for all prime factors p of $\Delta(B)$, $p^2 \nmid \Delta(B)$, then we conclude right away that B is an integral basis. If there are some square prime divisors, then we search for algebraic integers α of the form given in the lemma. Of course, at this stage, we need to be good at determining if a given algebraic number is an algebraic integer. We will discuss this point in detail in due course. In any case, if the search produces no algebraic integers of that form, then we know that B is an integral basis, even if $\Delta(B)$ has square factors. On the other hand, if we do find an $\alpha \in \mathcal{O}_F$ of the given form, then we replace the basis B by the basis of algebraic integers B' described in the proof with b_j of B replaced by α. Then

$$\Delta(B') = \Delta(B)/p^2$$

and $|\Delta(B')|$ will now be strictly smaller than $|\Delta(B)|$. Applying this process recursively, we will eventually arrive at an integral basis. In the language of computer science, this is a *terminating algorithm* for computing an integral basis.

Once an integral basis B has been found, it is reasonable to say that we have computed the ring $\mathcal{O}_F$ itself, since we can describe it precisely as the $\mathbb{Z}-$linear combinations of the elements of B.