Integral bases and translation

We wish to investigate the effect of a change of variable $x \mapsto x - r$ on a basis of algebraic integers. That is, in an algebraic number field $K = \mathbb{Q}[\alpha]$ of degree d, if the primitive element α is an algebraic integer, then we have paid particular attention to the basis $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ of algebraic integers. One word of caution: when we refer to *a basis of algebraic integers*, we are referring to a basis of the $\mathbb{Q}$-vector space K whose elements are algebraic integers. On the other hand, somewhat confusingly, the name *integral basis* is reserved for a basis of algebraic integers that is furthermore a $\mathbb{Z}$-basis of the $\mathbb{Z}$-module $\mathcal{O}_K$. That is, a $\mathbb{Q}-$basis $\{b_1, b_2, \ldots, b_d\}$ of K is an integral basis if the $b_i \in \mathcal{O}_K$ and any $x \in \mathcal{O}_K$ can be written

$$\Sigma n_i b_i$$

for $n_i \in \mathbb{Z}$. (Note that the uniqueness of the n_i follows from the fact that the b_i form a $\mathbb{Q}$-basis for K.)

For examples where many significant computations in the number field can be done readily by hand, it is important to produce situations where B as above is an integral basis. Recall that this happens if and only if the discriminant $\Delta(B)$ is minimal among discriminants of integral basis. We are interested in the effect of the translation $\alpha \mapsto \beta = a + r$ for an $r \in \mathbb{Z}$. Put $B' = \{1, \beta, \beta^2, \cdots, \beta^{d-1}\}$. Using theorem 102, it was shown in Corollary 105 that

$$\Delta(B) = \Delta(B')$$

Here is a more informative way to see this equality (which has been suggested in the Practical Summary). We examine the change of basis matrix from B to B'. Then the formula

$$\beta^i = \alpha^i + i\alpha^{i-1}r + \binom{i}{2}\alpha^{i-2}r^2 + \cdots + i\alpha r^{i-1} + r^i$$

for each i shows that the matrix has the form

$$P = \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & & * \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & & \\ \cdots & & & & \end{pmatrix}$$

that is, upper triangular with 1's on the diagonal. In particular, it is an integral matrix with determinant 1. Since

$$\Delta(B') = \det(P)^2 \Delta(B)$$

this clearly implies the equality of discriminants. But more importantly, its inverse P^{-1} is also integral. That is to say,

(*) we can also write the α^i an a linear combination of the β^i with integral coefficients.

This is a direct proof that *B is an integral basis if and only if B' is an integral basis.* There are further consequences. Suppose $x \in K$. We examine the coefficients with respect to the two bases:

$$x = \Sigma c_i \alpha^i = \Sigma c_i' \beta^i$$

Now suppose the coefficients $\{c_0, c_1, \ldots, c_{d-1}\}$ with respect to the basis B have the properties:

(1) for all i, $c_i = a_i/p$ with $a_i \in \mathbb{Z}$;

(2) some $a_i/p \notin \mathbb{Z}$.

Then the coefficients $\{c_0', c_1', \ldots, c_{d-1}'\}$ with respect to the basis B' have the same two properties.

Property (1) is obvious from property (*). Similarly, if all $c_i' \in \mathbb{Z}$, then all $c_i \in \mathbb{Z}$, again by property (*), establishing (2) for B'. These observations can be very useful for finding integral bases.

Consider the case of $K = \mathbb{Q}[\alpha]$ where α is a root of the irreducible polynomial $f(x) = x^4 - p$ for $p \equiv 3 \mod 4$. The discriminant is easily computed to be

$$\Delta(B) = N(f'(\alpha)) = N(4\alpha^3) = 4^4(-p)^3$$

As usual, to see if B is an integral basis, we need to check for the possibility of algebraic integers among

$$\Sigma c_i \alpha^i$$

where the $c_i = k/l$ for l a prime such that $l^2 | \Delta(B)|$ and $0 \leq k < l$. The possible l's are of course $l = 2$ and $l = p$. The possibility of $l = p$ is easily dispensed with using the convenient theorem 107. But the possibility of $l = 2$ should give us pause. This we handle as follows: Consider $\beta = \alpha - 1$. Then the minimal polynomial for β is

$$g(x) = (x+1)^4 - p = x^4 + 4x^3 + 6x^2 + 4x + 1 - p$$

Now, the assumption $p \equiv 3 \mod 4$ is easily seen to imply that $g(x)$ is Eisenstein for the prime 2.

Suppose there were an algebraic integer of the form

$$c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$$

with $c_i = k/2$, $k = 0$ or $k = 1$ and some $k \neq 0$. There would be an algebraic integer of the form

$$c_0' + c_1'\beta + c_2'\beta^2 + c_3'\beta^3$$

with the c_i' having the same properties. This is impossible by theorem 107. Therefore, the prime 2 is also ruled out and $B = \{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis.