Example of a non-monogenic number field by Dedekind

Ferran Espuña Bertomeu

December 27, 2023

Claim 1. *$f(X) = X^3 - X^2 - 2X - 8$ is irreducible over $\mathbb{Q}$.*

Proof. Suppose f splits over $\mathbb{Q}$. It must do so in polynomials of degree 1 and 2. Therefore, it has a root in $\mathbb{Q}$. By the rational root theorem, the only possible rational roots of f are $\pm 1, \pm 2, \pm 4, \pm 8$. None of these are roots of f. $\square$

Remark 2. Let θ be a root of f. Then, $K = \mathbb{Q}(\theta)$ is a field extension of $\mathbb{Q}$ of degree 3, and a $\mathbb{Q}$-basis of K is $B \coloneqq \{1, \theta, \theta^2\}$. Expressed in this basis, the multiplication by θ is given by the matrix

$$T_\theta^B = M \coloneqq \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

Claim 3. *$\alpha \coloneqq 4/\theta \in \mathcal{O}_K$.*

Proof. Clearly $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha) \Rightarrow \alpha$ must be a root of a monic irreducible degree 3 polynomial g over $\mathbb{Q}$. We will show that in fact g has integer coefficients. Multiplying by α is expressed by the matrix

$$T_\alpha^B = N \coloneqq 4M^{-1} = \begin{pmatrix} -1 & 4 & 0 \\ -1/2 & 0 & 4 \\ 1/2 & 0 & 0 \end{pmatrix}$$

Multiplying the column vector $(1, 0, 0)^T$ by this matrix repeatedly, we get:

$$\alpha = \begin{pmatrix} -1 \\ -1/2 \\ 1/2 \end{pmatrix}^B, \ \alpha^2 = \begin{pmatrix} -1 \\ 5/2 \\ -1/2 \end{pmatrix}^B, \ \alpha^3 = \begin{pmatrix} 11 \\ -3/2 \\ -1/2 \end{pmatrix}^B \tag{1}$$

To calculate the coefficients of g, we want to express α^3 as a linear combination of $\{1, \alpha, \alpha^2\}$. That is, we want to compute:

$$\begin{pmatrix} 1 & -1 & -1 \\ 0 & -1/2 & 5/2 \\ 0 & 1/2 & -1/2 \end{pmatrix}^{-1} \begin{pmatrix} 11 \\ -3/2 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 8 \\ -2 \\ -1 \end{pmatrix}$$

Therefore, $g(X) = X^3 + X^2 + 2X - 8$, Which has integer coefficients.

□

Claim 4. *$\{1, \theta, \alpha\}$ is an integral basis of $\mathcal{O}_K$.*

Proof. We know that all three elements are in $\mathcal{O}_K$. Furthermore, they are linearly independent over $\mathbb{Q}$ (otherwise, $a\theta + 4b/\theta + c = 0 \Rightarrow a\theta^2 + c\theta + 4b = 0$, which is impossible since $\{1, \theta, \theta^2\}$ are linearly independent over $\mathbb{Q}$). Therefore, they form a $\mathbb{Q}$-basis of K. Furthermore, they are algebraic integers, as we have proved. Let us calculate the discriminant of this basis. We will use the formula proved in class:

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\operatorname{Tr}(\alpha_i \alpha_j)_{i,j=1}^n) \tag{2}$$

In this case, we have already calculated the matrix corresponding to multiplication by α and θ. We can also note that $\alpha\theta = 4 \in \mathbb{Q}$, so it has trace $3 \times 4 = 12$ (similarly, $\operatorname{Tr}(1) = 3$), and that

$$T_{\theta^2}^B = M^2 = \begin{pmatrix} 0 & 8 & 8 \\ 0 & 2 & 10 \\ 1 & 1 & 3 \end{pmatrix}$$

and

$$T_{\alpha^2}^B = N^2 = \begin{pmatrix} -1 & 4 & 16 \\ 5/2 & -2 & 0 \\ -1/2 & 2 & 0 \end{pmatrix}$$

Therefore, we can calculate (2) as follows:

$$\begin{vmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\theta) & \operatorname{Tr}(\alpha) \\ \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta\alpha) \\ \operatorname{Tr}(\alpha) & \operatorname{Tr}(\theta\alpha) & \operatorname{Tr}(\alpha^2) \end{vmatrix} = \begin{vmatrix} 3 & 1 & -1 \\ 1 & 5 & 12 \\ -1 & 12 & -3 \end{vmatrix} = -503$$

Since the discriminant is a square-free integer (in fact, it is prime) it has to be $\operatorname{disc}(K)$ (by theory, it has to be a square times $\operatorname{disc}(K)$). Therefore, $\{1, \theta, \alpha\}$ is an integral basis of $\mathcal{O}_K$. □

Claim 5. *K is not monogenic.*

Proof. Suppose that $\{1, \beta, \beta^2\}$ is an integral basis of $\mathcal{O}_K$. Let $\beta = a+b\theta+c\alpha$, with $a, b, c \in \mathbb{Z}$. We may assume a $= 0$, since otherwise we can replace β by $\beta - a$ and we still have an integral basis. Then, $\beta^2 = b^2\theta^2 + 2bc\alpha\theta + c^2\alpha^2$. We have already calculated α and α^2 in (1). Also remember that $\alpha\theta = 4$. All in all,

$$\beta = \begin{pmatrix} -c \\ b - {}^{c}\!/_{2} \\ {}^{c}\!/_{2} \end{pmatrix}^B, \; \beta^2 = \begin{pmatrix} 8bc - c^2 \\ {}^{5c^2}\!/_{2} \\ b^2 - {}^{c^2}\!/_{2} \end{pmatrix}^B$$

So the change of basis matrix from $\{1, \beta, \beta^2\}$ to $\{1, \theta, \alpha\}$ is

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1/2 \\ 0 & 0 & 1/2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -c & 8bc - c^2 \\ 0 & b - c/2 & 5c^2/2 \\ 0 & c/2 & b^2 - c^2/2 \end{pmatrix}$$

with determinant $2 \times \frac{1}{4}(4b^3 - 2bc^2 - 2b^2c - 4c^3) = 2b^3 - bc^2 - b^2c - 2c^3$. This is always even, so it cannot be ± 1, which is a necessary (in fact, also sufficient) condition for $\{1, \beta, \beta^2\}$ to be an integral basis. $\square$