Minimal degree of an algebraic number with respect to a number field containing it

Artūras Dubickas (Vilnius University)
e-mail: arturas.dubickas@mif.vu.lt

Let β be an algebraic number of degree $d \geq 2$ over the field of rational numbers $\overline{\mathbb{Q}}$, and let L be a number field containing this number β. Then, we say that the *minimal degree of* β *with respect to the field* L is the smallest degree of a polynomial $f \in \mathbb{Q}[x]$ for which $\beta = f(\alpha)$ for some $\alpha \in L$ which is the primitive element of L over $\mathbb{Q}$, namely, $L = \mathbb{Q}(\alpha)$. We denote this quantity by $\deg_L(\beta)$. The quantity $\deg_L(\beta)$ in some sense represents the 'shortest' representation of an algebraic number in terms of a generator of a field containing it [1]. By the definition, it is clear that

$$\deg_L(\beta) = \deg_L(a + b\beta)$$

for any rational numbers a and $b \neq 0$.

Setting $D = [L : \mathbb{Q}(\beta)]$, we trivially have $\deg_L(\beta) = 1$ if $D = 1$, since then β itself is a generator of L over $\mathbb{Q}$ and we can take $f(x) = x$. In fact, for any $D \geq 2$ one has

$$\deg_L(\beta) \geq D.$$

Indeed, suppose that $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Note that α is of degree dD over $\mathbb{Q}$, since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : \mathbb{Q}] = [L : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd.$$

Let α_j, $j = 1, \dots, dD$, be the conjugates of α. Clearly, the conjugates of β are all of the form $f(\alpha_j)$, $j = 1, \dots, dD$. Since β is of degree d over $\mathbb{Q}$, the list $f(\alpha_j)$, $j = 1, \dots, dD$, contains exactly d distinct elements and each of them occurs exactly D times. By the fundamental theorem of algebra, at most $\deg f$ numbers $f(c_j)$ for distinct $c_j \in \mathbb{C}$ can be equal. This implies $D \leq \deg f$ and completes the proof of the inequality. (A slightly different proof of this inequality is given in [1, Prop. 2.1].)

For example, for $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, we have $\deg_L(\beta) = 4$, because $\alpha = \sqrt{3} + 3\sqrt{5} - 5\sqrt{6} + \sqrt{10}$ is a generator of L over $\mathbb{Q}$ and

$$\sqrt{2} = \frac{\alpha^4 - 416\alpha^2 + 16804}{11760}.$$

However, for $\beta = \sqrt{2} + c\sqrt{3}$, with nonzero rational number c, its minimal degree with respect to L depends on the arithmetic properties of the elliptic curve $y^2 = x(x - 3c^2)(x + 2 - 3c^2)$ and equality $\deg_L(\sqrt{2} + c\sqrt{3}) = 2$ rarely happens [1].

In [2], we prove that for $d = D = 2$ we always have equality, namely, $\deg_L(\beta) = D = 2$. However, it seems very likely that for a 'random' β of degree $d \geq 3$ and a 'random' degree D extension L of $\mathbb{Q}(\beta)$ one should expect the strict inequality $\deg_L(\beta) > D$, which means that there is no 'short' representation of β in terms of a generator α. The problem seems to be difficult already for $D = 2$, when L is a quadratic extension of $\mathbb{Q}(\beta)$, and so we are looking for a possible expression of β as a quadratic polynomial in a generator α of L. In [2], we also prove that for each totally real algebraic number β of degree $d \geq 3$ there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$. The same is proved for many (but not all) cubic algebraic numbers β.

References

[1] C. M. Park and S. W. Park, *Minimal degrees of algebraic numbers with respect to primitive elements,* Int. J. Number Theory **18** (2022), 485–500.

[2] A. Dubickas, *Minimal degree of an element of a number field with respect to its quadratic extension,* (to appear).