PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 77(91) (2005), 67–70

TWO EXERCISES CONCERNING THE DEGREE OF THE PRODUCT OF ALGEBRAIC NUMBERS

Artūras Dubickas

Communicated by Aleksandar Ivić

ABSTRACT. Let k be a field, and let α and β be two algebraic numbers over k of degree d and ℓ, respectively. We find necessary and sufficient conditions under which $\deg(\alpha\beta) = d\ell$ and $\deg(\alpha + \beta) = d\ell$. Since these conditions are quite difficult to check, we also state a simple sufficient condition for such equalities to occur.

Let k be a field, and let k^{a} be an algebraic closure of k. Suppose that $\alpha \in k^{\mathrm{a}}$ is of degree d over k. If $\beta \in k^{\mathrm{a}}$ has degree ℓ over k then $[k(\alpha, \beta) : k] \leqslant d\ell$, so any $\gamma \in k(\alpha, \beta)$ has degree at most $d\ell$ over k. In particular, $\alpha\beta$ and $\alpha + \beta$ both have degree at most $d\ell$ over k. Furthermore, for a 'generic' β of degree ℓ we have equality, namely, $\alpha\beta$ and $\alpha+\beta$ are both of degree $d\ell$. For some problems concerning linear forms in conjugate algebraic numbers and the Mahler measure of an algebraic number (over $\mathbb{Q}$) we have $\alpha \in k^{\mathrm{a}}$ satisfying certain conditions (see, e.g., [1], [3]) and need to enlarge the set of such numbers by either multiplying or by adding a 'generic' β (of degree ℓ) in the sense that $\alpha\beta$ (or $\alpha + \beta$) has 'generic' degree $d\ell$. How one can be sure that a particular β have the required properties?

In this note we state some simple *sufficient*, *necessary* and *necessary and sufficient* conditions on β in order that $\alpha\beta$ (or $\alpha+\beta$) is of maximal possible degree. We begin with the following *necessary and sufficient* condition.

THEOREM 1. *Suppose that $\alpha \in k^{\mathrm{a}}$ is of degree d over k and $\beta \in k^{\mathrm{a}}$ is of degree ℓ over k. Then $\alpha\beta$ is of degree $d\ell$ over k if and only if β is of degree ℓ over $k(\alpha)$ and $\alpha \in k(\alpha\beta)$. Similarly, $\alpha + \beta$ is of degree $d\ell$ over k if and only if β is of degree ℓ over $k(\alpha)$ and $\alpha \in k(\alpha + \beta)$.*

PROOF. The proof follows easily from the following standard diagram:

2000 *Mathematics Subject Classification*: 11R04, 11R32, 12E99.
Key words and phrases: field, algebraic number, degree, root of unity.

$$\begin{array}{ccccc} k & — & E = k(\alpha)\cap k(\beta) & — & k(\beta) \\ & & \diagdown & & \diagdown \\ & & k(\alpha) & — & k(\alpha,\beta) \end{array}$$

Indeed, since

$$[k(\alpha\beta):k] \leqslant [k(\alpha,\beta):k] = [k(\alpha,\beta):k(\alpha)][k(\alpha):k] = [k(\alpha,\beta):k(\alpha)]d \leqslant d\ell,$$

we have $[k(\alpha\beta):k] = d\ell$ if and only if $k(\alpha,\beta) = k(\alpha\beta)$ and $[k(\alpha,\beta):k(\alpha)] = \ell$. Of course, $k(\alpha,\beta) = k(\alpha\beta)$ implies that $\alpha \in k(\alpha\beta)$. But then also $\beta \in k(\alpha\beta)$ and so $\alpha \in k(\alpha\beta)$ implies that $k(\alpha,\beta) = k(\alpha\beta)$ too. Consequently, the conditions $k(\alpha,\beta) = k(\alpha\beta)$ and $\alpha \in k(\alpha\beta)$ are equivalent. On the other hand, $[k(\alpha,\beta):k(\alpha)] = \ell = [k(\beta):k]$ if and only if the minimal polynomial of β over k is irreducible over the field $k(\alpha)$, that is β has degree ℓ over $k(\alpha)$. This proves the theorem for $\alpha\beta$. The proof of the theorem for the sum $\alpha+\beta$ is precisely the same. □

Set $E = k(\alpha)\cap k(\beta)$ (see the diagram). The degree of β over E is equal to the degree of β over $k(\alpha)$ (see, for instance, [2]). So if E is a proper extension of k then the degree of β over $k(\alpha)$ is smaller than ℓ. Consequently, Theorem 1 implies that $E = k(\alpha)\cap k(\beta) = k$ is a *necessary* condition for $\deg(\alpha\beta) = d\ell$ (and for $\deg(\alpha+\beta) = d\ell$) to occur.

Unfortunately, the condition $\alpha \in k(\alpha\beta)$ of Theorem 1 is quite difficult to check. This raises the question on whether there is a simple method of finding many different β satisfying $\deg(\alpha\beta) = d\deg\beta$. The next theorem gives a *sufficient* condition for this equality to occur.

THEOREM 2. *Suppose that α is an algebraic number of degree d over a field k of characteristic zero, and let K be a normal closure of $k(\alpha)$ over k. If $L = k(\beta)$ is a normal extension of k of degree ℓ and $L\cap K = k$ then* $\deg(\alpha+\beta) = d\ell$. *If, in addition, β is torsion-free then* $\deg(\alpha\beta) = d\ell$.

Recall that (as in [3]) β is called *torsion-free* if β'/β is not a root of unity for any $\beta' \neq \beta$, where β' and β are conjugate over k. The condition on β to be torsion-free is necessary in the multiplicative part of Theorem 2. Indeed, the example $k = \mathbb{Q}$, $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$ with $d = \ell = 2$ and $\mathbb{Q}(\sqrt{2})\cap\mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ shows that $\alpha\beta = \sqrt{6}$ is of degree 2 over $\mathbb{Q}$, although $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ are normal extensions and $d\ell = 4$. Of course, if β is not torsion-free, we can add to it an element $k_0 \in k$ and consider $\beta_0 = \beta + k_0$ instead. Since $L = k(\beta) = k(\beta_0)$ for any $k_0 \in k$, it is sufficient to take k_0 for which $\beta_0 = \beta + k_0$ is torsion-free. (Below, we will show that such k_0 exists: see Theorem 3.) In the above example we can take $k_0 = 1$. Then $\beta_0 = 1+\sqrt{3}$ and $\alpha\beta_0 = \sqrt{6}+\sqrt{2}$ is of degree 4 over $\mathbb{Q}$.

PROOF OF THEOREM 2. The conditions of the theorem imply that LK is a Galois extension of k (see [4] for all standard facts about Galois extensions which are used here). Therefore $\alpha'+\beta'$ is conjugate to $\alpha+\beta$ for arbitrary pair α',β', where α' and α are conjugate over k and β' is conjugate to β over k. Hence $\deg(\alpha+\beta) \leqslant d\ell$ with inequality being strict if and only if $\alpha+\beta = \alpha'+\beta'$ with certain $\alpha' \neq \alpha$ and $\beta' \neq \beta$. Assume that $\alpha+\beta = \alpha'+\beta'$. Then $L \cap K = k$ implies that $\gamma := \alpha - \alpha' = \beta' - \beta \in k$, because $\alpha' \in K$, $\beta' \in L$. Let σ be an automorphism of K taking α to α'. Suppose that σ is of order $t > 1$, so that $\sigma^t(\alpha) = \alpha$. Then by adding t equalities $\gamma = \sigma^j(\alpha) - \sigma^{j+1}(\alpha)$ corresponding to $j = 0, 1, \dots, t-1$ we obtain that $t\gamma = 0$. Since $\operatorname{char} k = 0$, this can only occur if $\gamma = 0$, giving $\alpha' = \alpha$ and $\beta' = \beta$, a contradiction.

Similarly, $\deg(\alpha\beta) \leqslant d\ell$, where $\deg(\alpha\beta) < d\ell$ if and only if $\alpha\beta = \alpha'\beta'$ with certain $\alpha' \neq \alpha$ and $\beta' \neq \beta$. Now, a similar argument shows that $\gamma := \beta'/\beta = \alpha/\alpha'$ can lie in k, but only if γ is a root of unity (see also [5]). More precisely, if $\sigma : \beta \to \beta'$ is of order t then

$$\left(\frac{\beta'}{\beta}\right)^t = \gamma^t = \frac{\sigma(\beta)}{\beta}\frac{\sigma^2(\beta)}{\sigma(\beta)} \cdots \frac{\beta}{\sigma^{t-1}(\beta)} = 1$$

so β is not torsion-free, a contradiction. This proves Theorem 2. □

We will conclude by showing the following.

THEOREM 3. *For each $\beta \in k^{\mathrm{a}}$, where k is a field of characteristic zero, there is a $k_0 \in k$ such that $\beta + k_0$ is torsion-free.*

PROOF. Suppose that there is a $\beta \in k^{\mathrm{a}}$ such that $\beta + k_0$ is not torsion-free for each $k_0 \in \mathbb{Z}$, where $\mathbb{Z}$ is a prime subfield of k. Then, for some fixed β' (which is conjugate to β over k and $\beta' \neq \beta$), $\omega := (\beta' + k_0)/(\beta + k_0)$ is a root of unity for infinitely many $k_0 \in \mathbb{Z}$. By Corollary 1.3 of [2], the degree of ω over k is bounded, so there is an absolute constant $n_0 \in \mathbb{N}$, $n_0 > 1$, and infinitely many $k_0 \in \mathbb{Z}$ for which $(\beta' + k_0)^{n_0} = (\beta + k_0)^{n_0}$. Subtracting the left-hand side of this equality from its right-hand side and dividing by $\beta - \beta'$ we obtain that

$$\xi_0 + \xi_1 k_0 + \dots + \xi_{n_0-1} k_0^{n_0-1} = 0,$$

where the coefficients $\xi_j = \binom{n_0}{j}(\beta^{n_0-j} - \beta'^{n_0-j})/(\beta - \beta') \in k(\beta, \beta')$, $j = 0, 1, \dots,$ $n_0 - 1$, do not depend on k_0. Now, by taking any n_0 distinct elements k_0 (among infinitely many) in order that a respective determinant would be non-zero, we deduce that $\xi_0 = \xi_1 = \dots = \xi_{n_0-1} = 0$. However, $\xi_{n_0-1} = n_0 \neq 0$, a contradiction. □

This research was partially supported by the Lithuanian State Science and Studies Foundation and by INTAS grant no. 03-51-5070.

References

[1] J. D. Dixon and A. Dubickas, *The values of Mahler measures*, Mathematika, (to appear).

[2] P. Drungilas and A. Dubickas, *On subfields of a field generated by two conjugate algebraic numbers*, Proc. Edinburgh Math. Soc. **47** (2002), 119–123.

[3] A. Dubickas, *On the degree of a linear form in conjugates of an algebraic number*, Illinois J. Math. **46** (2002), 571–585.

[4] S. Lang, *Algebra,* 3rd ed., Graduate texts in mathematics 211, Springer-Verlag, New York, Berlin, 2002.
[5] C. J. Smyth, *Conjugate algebraic numbers on conics*, Acta Arith. **40** (1982), 333–346.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius 03225, Lithuania
arturas.dubickas@maf.vu.lt

(Received 01 08 2004)