Canad. Math. Bull. Vol. 63 (3), 2020 pp. 481–483
http://dx.doi.org/10.4153/S0008439519000274

On the Discriminants of the Powers of an Algebraic Integer

Stéphane R. Louboutin

Abstract. For α an algebraic integer of any degree $n \geqslant 2$, it is known that the discriminants of the orders $\mathbb{Z}[\alpha^k]$ go to infinity as k goes to infinity. We give a short proof of this result.

In this note, all algebraic numbers and number fields that occur are supposed to be contained in $\mathbb{C}$. Let

$$0 \neq D_\alpha = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2 \in \mathbb{Z}$$

be the discriminant of the minimal polynomial

$$\Pi_\alpha(X) = X^n - a_{n-1}X^{n-1} + \cdots + (-1)^n a_0 \in \mathbb{Z}[X]$$

of an algebraic integer α of degree n where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α, *i.e.*, are the n distinct roots of $\Pi_\alpha(X)$.

The present Theorems 1 and 3 follow from [Dub]. However, we feel that the short proofs presented here may be worth reading.

Theorem 1 *Let ε be an algebraic unit that is not a root of unity. Then $|D_{\varepsilon^k}|$ tends to infinity as k tends to infinity.*

Proof Since $\mathbb{Q}(\varepsilon)$ has only finitely many subfields, by considering subsequences if necessary, we may assume that $k \in \{k \ge 1; \mathbb{Q}(\varepsilon^k) = \mathbb{K}\}$, where $\mathbb{K}$ is a given number field. Set $m = (\mathbb{K} : \mathbb{Q}) \ge 2$. Since ε is not a root of unity, the ε^k's are pairwise distinct elements of the unit group $\mathbb{Z}_\mathbb{K}^\times$ of the ring $\mathbb{Z}_\mathbb{K}$ of algebraic integers of $\mathbb{K}$. Therefore, it suffices to show that for any given $A > 0$ the set $X = \{\eta \in \mathbb{Z}_\mathbb{K}^\times; \mathbb{Q}(\eta) = \mathbb{K} \text{ and } |D_\eta| \le A\}$ is finite. Let $\overline{\mathbb{K}}$ be the normal closure of $\mathbb{K}$. Let σ_i, $1 \le i \le m$, be the embeddings of $\mathbb{K}$ in $\mathbb{C}$, with $\sigma_m = \mathrm{Id}$. Hence, $\sigma_i(\mathbb{K}) \subseteq \overline{\mathbb{K}}$. Let S be the set of places of $\overline{\mathbb{K}}$ above the rational primes less than or equal to A. Set $Y = \{\eta \in \mathbb{Z}_{\overline{\mathbb{K}}}^\times; \eta - 1 \text{ is a } S\text{-unit of } \mathbb{Z}_{\overline{\mathbb{K}}}\}$. By Siegel's theorem, Y is finite. Now, let $\eta \in X$. Then $\sigma_i(\eta) - \eta$ divides D_η in $\mathbb{Z}_{\overline{\mathbb{K}}}$ for $1 \le i \le m-1$. Hence, $\sigma_i(\eta) - \eta$ is a S-unit and so is each $\sigma_i(\eta)/\eta$. Therefore,

$$\phi\colon \eta \in X \longrightarrow \phi(\eta) = \Big(\frac{\sigma_1(\eta)}{\eta}, \ldots, \frac{\sigma_{m-1}(\eta)}{\eta}\Big) \in Y^{m-1}$$

is well defined and $\phi(\eta) = \phi(\eta')$ if and only if η'/η is invariant under the action of all the σ_i's, hence if and only if $\eta' = \pm\eta$. Therefore, X is finite and $\#X \le 2(\#Y)^{m-1}$. ∎

Received by the editors May 13, 2019.
Published online on Cambridge Core May 22, 2019.
AMS subject classification: **11R04**, 11R29, 11J86.
Keywords: discriminant, algebraic integer.

Lemma 2 *Let $\beta \neq 0$ be an algebraic integer in a number field $\mathbb{K}$ of degree $m > 1$. Let $\sigma_1, \dots, \sigma_m$ be the m embeddings of $\mathbb{K}$ in $\mathbb{C}$. Assume that β is not a root of unity. Set $\rho_k = |\sigma_k(\beta)|$ and assume that $\rho_1 \geq \dots \geq \rho_m$. Then*

$$F_{\mathbb{K}}(\beta) := \prod_{i=1}^{m-1} |\sigma_i(\beta)|^{m-i} > 1.$$

Moreover, $F_{\mathbb{K}}(\beta) \geq |N_{\mathbb{K}/\mathbb{Q}}(\beta)|^{\frac{m-1}{2}}$.

Proof We have $\prod_{i=1}^m \rho_i = |N_{\mathbb{K}/\mathbb{Q}}(\beta)| \geq 1$ and

$$F_{\mathbb{K}}(\beta) = \Big(\prod_{i=1}^m \rho_i\Big)^{\frac{m-1}{2}} \times \begin{cases} \prod_{i=1}^{(m-1)/2} (\rho_{\frac{m+1}{2}-i}/\rho_{\frac{m+1}{2}+i})^i & (m \text{ odd}), \\ \Big(\prod_{i=1}^m \frac{\rho_1}{\rho_i}\Big)^{\frac{1}{2}} \times \prod_{i=1}^{(m-2)/2} (\rho_{\frac{m+2}{2}-i}/\rho_{\frac{m+2}{2}+i})^i & (m \text{ even}). \end{cases}$$

Since $\rho_k \geq \rho_l$ for $k \leq l$, we have $F_{\mathbb{K}}(\beta) \geq |N_{\mathbb{K}/\mathbb{Q}}(\beta)|^{\frac{m-1}{2}} \geq 1$. Moreover, $F_{\mathbb{K}}(\beta) = 1$ would imply $\rho_1 = \dots = \rho_m = 1$ and β would be a root of unity, a contradiction. ∎

Theorem 3 *Let $\alpha \neq 0$ be an irrational algebraic integer which is not a root of unity. Then $|D_{\alpha^k}|$ tends exponentially to infinity with k ranging over the infinite set $\{k \geq 1; \alpha^k \notin \mathbb{Q}\}$.*

Proof Since $\mathbb{Q}(\alpha)$ has only finitely many subfields, by considering subsequences if necessary, we may assume that $k \in \mathcal{E}_{\mathbb{K}} := \{k \geq 1; \mathbb{Q}(\alpha^k) = \mathbb{K}\}$, where $\mathbb{K}$ is a given number field of degree m and ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}$. By assumption, $m \geq 2$. Let $\sigma_1, \dots, \sigma_m$ be m of the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ such that their restrictions to $\mathbb{K}$ give the m distinct embeddings of $\mathbb{K}$ in $\mathbb{C}$.

We may assume that $|\alpha_1| \geq \dots \geq |\alpha_m|$, where $\alpha_k = \sigma_k(\alpha)$.

By Lemma 2, $F_{\mathbb{K}}(\alpha^k) = F_{\mathbb{K}}(\alpha^{k_0})^{k/k_0}$ goes exponentially to infinity with $k \in \mathcal{E}_{\mathbb{K}}$, where $k_0 = \min \mathcal{E}_{\mathbb{K}}$. Now,

$$|D_{\alpha^k}| = \prod_{1 \leq i < j \leq m} |\alpha_i^k - \alpha_j^k|^2 = F_{\mathbb{K}}(\alpha^k)^2 \prod_{1 \leq i < j \leq m} |1 - \alpha_j^k/\alpha_i^k|^2,$$

Since $\alpha_j^k/\alpha_i^k \neq 1$ for $1 \leq i < j \leq m$ and $k \in \mathcal{E}_{\mathbb{K}}$, from Baker type estimates there are effectively computable constants $C_1 > 0$, C_2 such that

$$|1 - \alpha_j^k/\alpha_i^k| \geq C_1 k^{-C_2}$$

for $1 \leq i < j \leq m$ and $k \in \mathcal{E}_{\mathbb{K}}$ (*e.g.*, see [Gross, Lemma 1] or [Dub, Lemma 1]). The desired result follows. ∎

In the cubic and totally imaginary quartic cases we have results more explicit than Theorems 1 and 3; see [Lou10, Theorem 1] or [Lou15, Theorem 9] for cubic units of negative discriminant, see [Lou12] or [Lou15, Theorem 33] for cubic units of positive discriminant, and see [Lou10, Theorem 2] for totally imaginary quartic units.

Acknowledgements We would like to thank J. Oesterlé for the proof of Theorem 1 (Allahabad (Inde), 22nd November 2017). We also thank J.-H. Evertse and K. Győry for their comments in October 2018 on Theorems 1 and 3. In particular J.-H. Evertse sent us an email explaining how using Baker's estimates and [EG, Corollary 6.2.1] could help us to finish the proof of Theorem 3. In other words, we greatly thank J.-H. Evertse for the argument we use in the last four lines of the proof of Theorem 3. ■

References

[Dub] A. Dubickas, *On the discriminant of the power of an algebraic number*. Stud. Sci. Math. Hungar. 44(2007), 27–34. https://doi.org/10.1556/SScMath.2006.1001

[EG] J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*. New Math. Monogr., 32, Cambridge University Press, Cambridge, 2017. https://doi.org/10.1017/CBO9781316160763

[Gross] E. H. Grossman, *Units and discriminants of algebraic number fields*. Comm. Pure Appl. Math. 27(1974), 741–747. https://doi.org/10.1002/cpa.3160270603

[Lou10] S. Louboutin, *On some cubic or quartic algebraic units*. J. Number Theory 130(2010), 956–960. https://doi.org/10.1016/j.jnt.2009.09.002

[Lou12] S. Louboutin, *On the fundamental units of a totally real cubic order generated by a unit*. Proc. Amer. Math. Soc. 140(2012), 429–436. https://doi.org/10.1090/S0002-9939-2011-10924-9

[Lou15] S. Louboutin, *Fundamental units for some orders generated by a unit*. In: *Publ. Math. Besançon Algèbre et Théorie des Nombres*, Presses Univ. Franche-Comté, Besançon, 2015, pp. 41–68.

Aix Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France
e-mail: stephane.louboutin@univ-amu.fr