Journal of Number Theory 168 (2016) 64–71

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Discriminants of cyclic cubic orders

Jun Ho Lee [a], Stéphane R. Louboutin [b,*,1]

[a] Department of Mathematics Education, Mokpo National University, 1666, Yeongsan-ro, Cheonggye-myeon, Muan-gun, Jeonnam 58554, Republic of Korea
[b] Aix Marseille Université, CNRS, Centrale Marseille, I2M, UMR 7373, 13453 Marseille, France

ARTICLE INFO

Article history:
Received 7 December 2015
Received in revised form 22 March 2016
Accepted 12 April 2016
Available online 2 June 2016
Communicated by M. Pohst

MSC:
11R16
11R29

Keywords:
Cubic field
Quartic field
Module
Basis
Discriminant

ABSTRACT

Let α be a cubic algebraic integer. Assume that the cubic number field $\mathbb{Q}(\alpha)$ is Galois. Let α_1, α_2 and α_3 be the real conjugates of α. We give an explicit $\mathbb{Z}$-basis and the discriminant of the $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant totally real cubic order $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$. This new result is completely different from the one previously obtained in the case that the cubic field $\mathbb{Q}(\alpha)$ is not Galois.

1. Introduction

Let

$$\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$$

* Corresponding author.
E-mail addresses: junho@mokpo.ac.kr (J.H. Lee), stephane.louboutin@univ-amu.fr (S.R. Louboutin).
[1] Postal address: Institut de Mathématiques de Marseille, Aix Marseille Université, 163 Avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France.

http://dx.doi.org/10.1016/j.jnt.2016.04.015
0022-314X/

be the minimal polynomial of a cubic algebraic integer α. Let α_1, α_2 and α_3 be the complex conjugates of α, i.e. the complex roots of $\Pi_\alpha(X)$. Then

$$\Omega_3 = \{1, \alpha_1, \alpha_1^2, \alpha_2, \alpha_2\alpha_1, \alpha_2\alpha_1^2\}$$

is a $\mathbb{Z}$-generating system of the order $\mathbb{M}_3 = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ (see [LL14, LEMMA 4.4]). Moreover, assume that the cubic number field $\mathbb{K} = \mathbb{Q}(\alpha)$ is not Galois. Then its normal closure $\mathbb{N} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ is a sextic number field with Galois group isomorphic to the symmetric group $\mathfrak{S}_3$, Ω_3 is a $\mathbb{Z}$-basis of the $\mathrm{Gal}(\mathbb{N}/\mathbb{Q})$-invariant sextic order $\mathbb{M}_3 = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ and the discriminant $d_{\mathbb{M}_3}$ of $\mathbb{M}_3$ is given by $d_{\mathbb{M}_3} = d_\alpha^3$, where $0 \neq d_\alpha \in \mathbb{Z}$ is the discriminant of $\Pi_\alpha(X)$ (see [LL14, Lemma 8.1]). More generally, we have (see [Lou16]):

Theorem 1. *Let α be an algebraic integer of degree $n \geq 2$. Let $0 \neq d_\alpha \in \mathbb{Z}$ be the discriminant of its minimal polynomial $\Pi_\alpha(X) \in \mathbb{Z}[X]$. Let $\alpha_1, \cdots, \alpha_n$ be the complex conjugates of α, i.e. the complex roots of $\Pi_\alpha(X)$. Then $\Omega_n := \{\alpha_1^{e_1} \cdots \alpha_n^{e_n};\ 0 \leq e_k \leq n-k\}$ is a $\mathbb{Z}$-generating system of the order $\mathbb{M}_n := \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$. Moreover, if $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \cdots, \alpha_n)/\mathbb{Q})$ is isomorphic to the symmetric group $\mathfrak{S}_n$, then $\mathbb{M}_n$ is a free $\mathbb{Z}$-module of rank $n!$, of $\mathbb{Z}$-basis Ω_n and of discriminant $D_{\mathbb{M}_n} = D_\alpha^{n!/2}$.*

The aim of this paper is to show that, surprisingly, obtaining such a result for Galois number fields seems much more difficult. We will deal with the simplest Galois case: we assume that the number field $\mathbb{K} = \mathbb{Q}(\alpha)$ is cubic Galois, hence cyclic. Clearly, $\mathbb{M}_3 = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is a free $\mathbb{Z}$-module of rank 3. We determine a $\mathbb{Z}$-basis and the discriminant $d_{\mathbb{M}_3}$ of this $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$-invariant cubic order $\mathbb{M}_3$, solving the problem raised in [LL14, Section 8.4]:

Theorem 2. *Let $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ be the minimal polynomial of a cubic algebraic integer α. Assume that the cubic number field $\mathbb{K} = \mathbb{Q}(\alpha)$ is Galois, i.e. assume that the discriminant $d_\alpha = -4a^3c - 4b^3 + a^2b^2 + 18abc - 27c^2$ of $\Pi_\alpha(X)$ is a perfect square, say $d_\alpha = D^2$, $D \in \mathbb{Z}$. Let α_1, α_2 and α_3 be the three complex conjugates of α, i.e. the three complex roots of $\Pi_\alpha(X)$. Set*

$$\Delta = \gcd(D, 3b - a^2, 3ac - b^2).$$

Let $x, y, z \in \mathbb{Z}$ be such that

$$\Delta = xD + y(3b - a^2) + z(3ac - b^2)$$

and set

$$\eta = x\alpha_1^2 + y\alpha_2 + z\alpha_2\alpha_1^2. \tag{1}$$

Then $\{1, \alpha_1, \eta\}$ is a $\mathbb{Z}$-basis of the $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant order $\mathbb{M}_3 = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ and $d_{\mathbb{M}_3} = \Delta^2$ divides d_α.