Journal of Number Theory 167 (2016) 394–406

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Families of cyclic cubic fields

Steve Balady

Department of Mathematics, University of Maryland, College Park, MD 20742, United States

ARTICLE INFO

Article history:
Received 16 November 2015
Received in revised form 26 March 2016
Accepted 27 March 2016
Available online 29 April 2016
Communicated by David Goss

Keywords:
Cyclic cubic fields
Fundamental units

ABSTRACT

We describe a procedure for generating families of cyclic cubic fields with explicit fundamental units. This method generates all known families and gives new ones.

In [5], Shanks considered what he termed the “simplest cubic fields,” defined as the splitting fields of the polynomials

$$S_n = X^3 + (n+3)X^2 + nX - 1. \tag{0.1}$$

In particular, he showed that if the square root of the polynomial discriminant is squarefree, then the roots of S_n form a system of fundamental units for its splitting field. The analysis of this family was extended by Lettl [4] and Washington [7]. Lecacheux [3], and later Washington [8], discovered a second one-parameter family with a similar property: if a certain specified chunk of the polynomial discriminant is squarefree, the roots of the polynomial form a system of fundamental units. Kishi [2] found a third such family.

E-mail address: sbalady@math.umd.edu.

http://dx.doi.org/10.1016/j.jnt.2016.03.011
0022-314X/

In the following, we show that there are many, many more families of cubics with this property. The first three sections generalize the procedure of Washington [8] and follow the model of that paper. The fourth section is dedicated to examples: we exhibit a new one-parameter family and describe a method for generating arbitrarily many more.

1. The families

Let $f(n)$ and $g(n)$ be polynomials with integral coefficients, and assume that the following condition holds:

$$\lambda = \frac{f^3 + g^3 + 1}{fg} \text{ is a polynomial with integral coefficients.} \tag{1.1}$$

Examples will be given in Section 4. For now we remark only that this condition implies that $f|(g^3+1)$ and $g|(f^3+1)$; in particular, f and g have no common factors. If Condition (1.1) is satisfied, the pair (f, g) determines a one-parameter family of polynomials as follows:

$$P_{f,g}(X) = X^3 + a(n)X^2 + \lambda(n)X - 1, \text{ where}$$
$$a = 3(f^2 + g^2 - fg) - \lambda(f + g).$$

Note that $P_{f,g}$ is symmetric in f and g, so we'll assume that $\deg f \leq \deg g$. If this inequality is strict, then $\deg \lambda < \deg a$. Together with the rational root theorem, this implies that $P_{f,g}$ is irreducible for all but a small finite list of $n \in \mathbb{Z}$. For the rest of this paper, we will make the standing assumptions that $\deg f < \deg g$ and then fix an integer n for which $P_{f,g}$ is irreducible. This is practical for theoretical purposes, though we note that the case where both f and g are constant is also of potential interest.

The discriminant of $P_{f,g}$ is

$$D_P = (f - g)^2(3a + \lambda^2)^2 \neq 0,$$

so $P_{f,g}$ determines a cyclic cubic field which we denote $K_{f,g}$ (or sometimes just K). Thus $P_{f,g}$ has three real roots which we denote θ_1, θ_2, θ_3. Since the constant term of $P_{f,g}$ is a unit in $\mathbb{Z}$, these roots are units in the ring of integers $\mathcal{O}_{K_{f,g}}$.

Lemma 1.1. *The $\mathbb{Z}_3$ action of the Galois group on the roots of $P_{f,g}$ is given by*

$$G(\theta) = \frac{f\theta - 1}{(f^2 + g^2 - fg)\theta - g}.$$

Proof. Assume $P(\theta) = 0$. Since 1, θ, and θ^2 are linearly independent over $\mathbb{Q}$, we have $G(\theta) \neq \theta$. A messy but straightforward calculation shows that $P(G(\theta)) = 0$. □