Iterated Galois groups of $x^2 + c$ over quadratic number field with odd class number

Chih-Chiang Kao
Department of Mathematics,
Tokyo Institute of Technology

1 Introduction

1.1 Motivation

This is a short introduction of a recent work of the author on the iterated Galois groups. The motivation comes from ℓ-adic Galois representations associated to elliptic curves. Let K be a number field and E be an elliptic curve over K without complex multiplication. Write ℓ for a prime number in $\mathbb{Z}$, and denote by G_∞ the Galois group $\varprojlim \mathrm{Gal}(K(E[\ell^n]/K))$. Serre proved his celebrated Open Image Theorem as following:

Theorem 1.1 (Serre's Open Image Theorem, 1972)**.** *The natural injection $G_\infty \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ has open image, that is*

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : G_\infty] < \infty.$$

Moreover, $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G_\infty] = 1$ for all but finitely many ℓ.

We want to give a dynamical analog of Serre's Open Image Theorem. The study of iterated Galois groups were initiated by R. W. K. Odoni [Odo85a, Odo85b, Odo88] in the 1980s. He dealt with such kind of problems over function fields and gave a conjecture for Hilbertian fields.

Let K be any field of characteristic 0, and X, T be algebraically independent over K and regard X (resp. T) as a variable (resp. parameter). The polynomials which we care about is $f_n(X,T) = X^{k_n} + T$ where k_n are positive integers greater than 1. Put $F_1(X,T) = f_1(X,T)$ and define

$$F_{n+1}(X,T) = F_n(f_{n+1}(X,T), T).$$

Odoni's main result is as follows.

Theorem 1.2 (R. W. K. Odoni. [Odo85a, Theorem 1])**.** *Let $\overline{K}$ be an algebraic closure of K. The Galois group of $F_n(X,T)$ over $\overline{K}(T)$ is isomorphic to the (natural-)wreath product*

$$C_{k_n} \wr_{U_{n-1}} (\cdots (C_{k_3} \wr_{U_2} (C_{k_2} \wr_{U_1} C_{k_1})) \cdots).$$

where C_{k_i} is the cyclic group of order k_i, for each $i = 1, \ldots, n$, and U_i is the set of roots of $F_i(X, T)$ for $i = 1, \ldots, n-1$.

Given a polynomial $f(X) \in K[X]$, we define $f^n(X) = \underbrace{f \circ f \circ \cdots \circ f(X)}_{n \text{ times}}$ for $n \geq 1$. Let K_n be the splitting field of $f^n(X)$ over K, and the Galois group of K_n over K be called the n-th iterated Galois group of $f(X)$. Let T_n be the complete d-ary rooted tree of height n and $\mathrm{Aut}(T_n)$ be the automorphism group of T_n. Odoni gave the following conjecture.

Conjecture 1.1 (Odoni, 1985)**.** Let K be a Hilbertian field of characteristic 0. There exists a monic polynomial $f(X) \in K[X]$ with degree $d \geq 2$ such that

$$\mathrm{Gal}(K_n/K) \hookrightarrow \mathrm{Aut}(T_n) \cong [S_d]^n$$

is surjective for all $n \in \mathbb{N}$ where $[S_d]^n$ is the n-fold wreath product of symmetric group S_d.

Odoni showed in [Odo85b] that $\mathrm{Gal}(K_n/K) \cong [C_2]^n$ for all $n \in \mathbb{N}$ in the case $K = \mathbb{Q}$, and $f(X) = X^2 + X + 1$. For $f(X) = X^2 + c \in \mathbb{Q}[X]$ with integers c, it can be deduced that $\mathrm{Gal}(K_n/K)$ can be embedded into $[C_2]^n$ according [Odo85a, Lemma 1.1]. Stoll [Sto92] showed that

Theorem 1.3 ([Sto92, Main Theorem p.5])**.** *There exist infinitely many $c \in \mathbb{Z}$ such that*

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong [C_2]^n \text{ for all } n \geq 1,$$

where $f(X) = X^2 + c \in \mathbb{Z}[X]$.

Recently, there are some related results when K is a more general number field. We refer the interested reader to [Li20, Li21, Loo19, BJ19, Kad20, Spe18, BIJ+19].

1.2 Main results

In this paper, we will follow Odoni and Stoll's method. First, we will show that the n-th iterated Galois group of $f(X)$ can be embedded into $[C_2]^n$. So the largest possible Galois group is isomorphic to $[C_2]^n$. Next, we will focus on quadratic number fields with odd class number and prove the following result.

Theorem 1.4. *Suppose $K = \mathbb{Q}(\sqrt{d})$ is a quadratic number field with odd class number except for $d = -1$, and $f(X) = X^2 + c \in \mathcal{O}_K[X]$, then there exist infinitely many $c \in \mathcal{O}_K \backslash \mathbb{Z}$ such that $\Omega_n \cong [C_2]^n$ for all $n \in \mathbb{N}$.*

1.3 Outline of this paper

In Section 2, we will give some criteria to determine whether $\mathrm{Gal}(K_n/K) \cong [C_2]^n$ or not. In Sections 3 and 4, we will extend the work in [Sto92, Section 2] to quadratic number field case, and determine the quadratic residue property for the fundamental units in some real quadratic number fields. In Section 5, we consider the fields K whose class numbers are odd, and prove that $\mathrm{Gal}(K_n/K) \cong [C_2]^n$, provided some conditions on c are satisfied.

Acknowledgement

The author thanks the organizers of the conference *Algebraic Number Theory and Related Topics 2022* in RIMS. This article is based on the author's talk in the conference. The author is also grateful to L.-C. Hsia for many helpful discussions.

2 Criteria for $\Omega_n \cong [C_2]^n$

In this section, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, and $\mathcal{O}_K$ be the ring of integers of K. Let c be an algebraic integer such that $|N(c)| \notin \mathbb{Q}^2$. In most cases, we only consider $c \in \mathbb{Z}[\sqrt{d}]\backslash\{0, -1\}$. For $f(X) = X^2 + c \in \mathcal{O}_K[X]$, we define

$$f^n(X) = \underbrace{f \circ f \circ \cdots \circ f(X)}_{n \text{ times}}$$

for $n \geq 1$, which is called the n-th iterated polynomial of $f(X)$. Define

$$c_1 = -c, \text{ and } c_{n+1} = f^{n+1}(0) = c_n^2 + c$$

for $n \geq 1$. Let K_n be the splitting field of $f^n(X)$ over K, and denote by

$$\Omega_n = \mathrm{Gal}(K_n/K)$$

its Galois group over K. Consider the n-fold wreath product of C_2 with itself (cf. [Odo88]),

$$[C_2]^n \coloneqq C_2 \wr_{U_{n-1}} (\cdots (C_2 \wr_{U_2} (C_2 \wr_{U_1} C_2)) \cdots),$$

where C_2 is the cyclic group of order 2, and U_i is the set of roots of $f^i(X)$. The ideas of this paper come from [Odo88], and [Sto92]. First, we have the following lemma and definition:

Lemma 2.1 (cf. [Odo88, Lemma 4.4] and [Sto92, Lemma 1.1])**.**

1. *If $c \in \mathbb{Z}[\sqrt{d}]\backslash\{0, -1\}$, then $c_n \neq 0$ for all $n \in \mathbb{N}$.*
2. *There exists a sequence $\{b_n\}_{n\geq 1}$ in $\mathcal{O}_K$ such that :*

$$c_n = \prod_{d|n} b_d, \text{ and the } \langle b_n \rangle \text{ are pairwise coprime for } n \geq 1,$$

where $\langle b_n \rangle$ is the ideal generated by b_n in $\mathcal{O}_K$.

Definition. Nonzero elements $a_1, \ldots, a_n$ in a field K are called 2-*independent* over K if their residue classes in the $\mathbb{F}_2$-vector space $K^*/(K^*)^2$ are linearly independent.

Assume that $\Omega_n \cong [C_2]^n$ for some n. Then $\Omega_{n+1} \cong [C_2]^{n+1}$ if and only if $c_1, \ldots, c_n, c_{n+1}$ are 2-independent over K. Theorem 2.1 gives us some criteria to determine whether the order of the n-th iterated Galois group is equal to $[C_2]^n$ or not.

Theorem 2.1 (cf. [Sto92, Main Theorem p.3])**.**

1. *For all $n \in \mathbb{N}$, the following statements are equivalent:*
   (a) $\Omega_n \cong [C_2]^n$;
   (b) $c_1, c_2, \ldots, c_n$ *are 2-independent over* K;
   (c) $b_1, b_2, \ldots, b_n$ *are 2-independent over* K.
2. *Suppose the class number of K is odd. If none of ub_i is a square in $\mathcal{O}_K$ for $i = 1, \ldots, n$, then $\Omega_n \cong [C_2]^n$ where u are any units in $\mathcal{O}_K$.*

Remark. Let $N(\cdot)$ be the norm of K over $\mathbb{Q}$. In Theorem 2.1, if we assume further that none of $|N(b_i)|$ is a square in $\mathbb{Q}$ for $i = 1, \ldots, n$, then the restriction on class number is not necessary.

3 Iteration sequences associated to even polynomials

The idea of this section comes from [Sto92, Section 2]. In this section, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field except for $\mathbb{Q}(\sqrt{-1})$ and $f(X) = X^2 + c \in \mathcal{O}_K[X]$. Take

$$g_c(X) = \begin{cases} |c|X^2 + \operatorname{sgn}(c) & \text{if } d > 0, \\ -cX^2 - 1 & \text{if } d < 0. \end{cases}$$

and put $\gamma_1 = 1$, $\gamma_{n+1} = g(\gamma_n)$ for $n \geq 1$. We put, for $n \geq 2$,

$$c_n = \begin{cases} |c| \cdot \gamma_n & \text{if } d > 0, \\ -c \cdot \gamma_n & \text{if } d < 0. \end{cases}$$

Suppose all $c_n \neq 0$. Then it follows that $\gamma_n \neq 0$ for all $n \in \mathbb{N}$, whence we can define $\delta_n = \prod_{t|n} \gamma_t^{\mu(n/t)}$. For $n \geq 2$, we have

$$\delta_n = \begin{cases} |b_n| & \text{if } d > 0 \text{ and } c \notin (-2, 0), \\ b_n & \text{if } d < 0. \end{cases}$$

Lemma 3.1 (cf [Sto92, Lemma 2.1])**.** *Suppose that for any positive integer n, there is an $m_n \in \mathcal{O}_K \backslash \mathcal{O}_K^*$, such that $m_n \mid \gamma_n + \gamma_{2n}$, m_n is prime to γ_n, and -1 is not a square modulo m_n. Then for all $i \geq 2$, δ_i is not a square in K.*

Similarly, if there exists $m_n \in \mathcal{O}_K \backslash \mathcal{O}_K^*$, such that $m_n \mid \gamma_n - \gamma_{2n}$, m_n is prime to γ_n, and -1 is not a square modulo m_n. Then $-\delta_i$ is not a square in K for all $i \geq 2$.

We will take $m_k = \gamma_k \pm \gamma_{k+1}$ in Lemma 3.1. Then $m_k \mid \gamma_k + \gamma_{2k}$, and m_k is prime to γ_k. Moreover, we have $\pm b_n = \delta_n \equiv -1 \pmod{m_k}$. Therefore, if we can show that -1 and $-\epsilon_d$ are not square modulo m, then none of ub_i is a square in $\mathcal{O}_K$ where ϵ_d is the fundamental unit in $\mathcal{O}_K$, and u are any unit in $\mathcal{O}_K$. In Section 5, we will show that $\gamma_n + \gamma_{n+1}$ satisfying the conditions in Lemma 3.1, provided some conditions on c. According to the previous lemma, we can deduce that δ_n are not squares in K.

4 Quadratic residue properties for the fundamental unit of some real quadratic number fields

By [CH88, Corollary 18.4], the class number of $\mathbb{Q}(\sqrt{d})$ is odd if and only if

1. $d = 2, q$ — q is a prime congruent to 1 modulo 4;
2. $d = l, 2l, l_1 l_2$ — l, l_1, l_2 are primes congruent to 3 modulo 4;
3. $d = -1, -2, -l$ — l is a prime congruent to 3 modulo 4.

Let p be an odd rational prime, and suppose p is not inertial in $\mathcal{O}_K$. Then $\langle p \rangle = \mathfrak{p}\bar{\mathfrak{p}}$ or $\mathfrak{p}^2$ for some prime $\mathfrak{p} \subset \mathcal{O}_K$. In this section, we only consider $\mathbb{Q}(\sqrt{d})$ with odd class number, $d > 0$, and $N(\epsilon_d) = 1$, whence $d = l, 2l, l_1 l_2$ by [Rib13, pp 173-175]. We have the following quadratic residue properties for ϵ_d:

Lemma 4.1. *ϵ_d is a square modulo $\mathfrak{p}$ if and only if*

1. $(\frac{2}{p}) = 1$ *if* $d = l, 2l$;
2. $(\frac{l_1}{p}) = (\frac{l_2}{p}) = 1$ *if* $d = l_1 l_2$.

where $(\frac{\cdot}{\cdot})$ is the Legendre symbol.

5 Some sufficient conditions for $\Omega_n \cong [C_2]^n$

In this section, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with odd class number, and $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with $|N(c)|$ is not a square in $\mathbb{Q}$. We want to prove that none of ub_i is a square in $\mathcal{O}_K$, provided some conditions on c hold, and thus $\Omega_n \cong [C_2]^n$ by Theorem 2.1. The main theorem is as follows:

Theorem 5.1. *Suppose $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, and $|N(c)| \notin \mathbb{Q}^2$. Let $f^n(X)$ be the n-th iteration of $f(X) = X^2 + c$. We have*

$$\mathrm{Gal}(f^n(X)/K) \cong [C_2]^n \text{ for all } n \in \mathbb{N}$$

if one of the following conditions holds:

1. *($u < 0, N(c+2) > 0$ or $u > 0, N(c) > 0$), and*

$$\begin{aligned} c &\equiv 1 + \sqrt{d} \pmod 2 && \text{if } d = 2, \\ c &\equiv \sqrt{d} \pmod 2 && \text{if } d = q, \end{aligned}$$

2. *($u \geq 0, N(c+2) < 0$ or $u < 0, N(c) < 0$), and*

$$\begin{aligned} c &\equiv 1 \text{ or } 3 \pmod 4 && \text{if } d = l, \\ c &\equiv 1 \pmod 2 && \text{if } d = 2l, \\ c &\equiv -1 + 2s\sqrt{d} \pmod{2d} \text{ where } s \in \mathbb{Z} && \text{if } d = l_1 l_2, \end{aligned}$$

3.

$$\begin{aligned} c &\equiv 1+\sqrt{d} \pmod 2 && \text{if } d=-2,\\ c &\equiv \sqrt{d} \pmod 2 && \text{if } d=-l, \end{aligned}$$

where q, l, l_1, l_2 *are primes,* $q \equiv 1 \pmod 4$*, and* $l \equiv l_1 \equiv l_2 \equiv 3 \pmod 4$*.*

Before giving the proof of Theorem 5.1, we need some lemmas.

Lemma 5.1. *None of* $c_1, \ldots, c_n$ *is a square in* $\mathcal{O}_K$*. It follows that all* $f^n(X)$ *are irreducible over* K*.*

Lemma 5.2. *Let* $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$*, where* $d > 0$*, for* $n \geq 2$*,*

$$N(\gamma_n) > 0 \text{ if } u > 0, N(c) > 0 \text{ or } u < 0, N(c+2) > 0;$$

on the other hand,

$$N(\gamma_n) < 0 \text{ if } u < 0, N(c) < 0 \text{ or } u \geq 0, N(c+2) < 0.$$

Corollary. *Let* $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ *where* $d > 0$*, for all* $n \geq 1$*,*

$$N(\gamma_n + \gamma_{n+1}) > 0 \text{ if } u > 0, N(c) > 0 \text{ or } u < 0, N(c+2) > 0;$$

on the other hand,

$$N(\gamma_n + \gamma_{n+1}) < 0 \text{ if } u < 0, N(c) < 0 \text{ or } u \geq 0, N(c+2) < 0.$$

Proposition. *Let* $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$*. We have the following results for all* $n \in \mathbb{N}$*:*

1. *If* $d = q$ *and* $c \equiv \sqrt{d} \pmod 2$*, then* $N(\gamma_n \pm \gamma_{n+1}) \equiv 3 \pmod 4$*.*
2. *If* $d = 2$ *and* $c \equiv 1 + \sqrt{d} \pmod 2$*, then* $N(\gamma_n \pm \gamma_{n+1}) \equiv 3 \pmod 4$*.*
3. *If* $d = l$ *and* $c \equiv 1$ *or* $3 \pmod 4$*, then* $N(\gamma_n + \gamma_{n+1}) \equiv 1 \pmod 8$*.*
4. *If* $d = 2l$ *and* $c \equiv 1 \pmod 2$*, then* $N(\gamma_n + \gamma_{n+1}) \equiv 1 \pmod 8$*.*
5. *If* $d = l_1 l_2$ *and* $c \equiv -1 + 2s\sqrt{d} \pmod{2d}$ *for any* $s \in \mathbb{Z}$*, then* $N(\gamma_n + \gamma_{n+1}) \equiv 1 \pmod{4d}$*.*

Lemma 5.3. *Let* $d = l, 2l$*, consider* $m \in \mathcal{O}_K$*. If* $|N(m)| \equiv 7 \pmod 8$*, then* $-\epsilon_d$ *is not a square modulo* m *in* $\mathcal{O}_K$*.*

Lemma 5.4. *Consider* $K = \mathbb{Q}(\sqrt{d})$ *where* $d = l_1 l_2$*. Let* $m \in \mathcal{O}_K$ *satisfy* $|N(m)| \equiv -1 \pmod{4d}$*, then* $-1, -\epsilon_d$ *are not square modulo* m *in* $\mathcal{O}_K$*.*

Sketch of the proof of Theorem 5.1. In Theorem 2.1, We proved that if the class number of K is odd, and none of ub_i is a square in $\mathcal{O}_K$ for $i = 1, \ldots, n$, then $\Omega_n \cong [C_2]^n$ where u are any units in $\mathcal{O}_K$. For $d < 0$, it is enough to show that none of $\pm b_i$ is a square in $\mathcal{O}_K$. On the other hand, for $d > 0$, it is sufficient to show that none of $\pm b_i, \pm\epsilon_d b_i$ is a square in $\mathcal{O}_K$.

In Section 3, we have proved that $\pm b_n = \pm\delta_n \equiv -1 \pmod{\gamma_{n'} \pm \gamma_{n'+1}}$ when $d < 0$. Thus it is enough to prove that -1 (and $-\epsilon_d$ if $d > 0$) is not a square modulo $\gamma_n \pm \gamma_{n+1}$ for all $n \in \mathbb{N}$ in $\mathcal{O}_K$. To apply Lemma 3.1, we need to prove that $m_n = \gamma_n + \gamma_{n+1} \in \mathcal{O}_K \backslash \mathcal{O}_K^*$. By the hypothesis, we can deduce that the norm of m_n is congruent to 3 modulo 4. Hence m_n is not a unit in $\mathcal{O}_K$.

Finally, in each case in Theorem 5.1, we can deduced that $b_1, \ldots, b_n$ are 2-independent over K by previous lemmas. Hence $\Omega_n \cong [C_2]^n$ for all $n \in \mathbb{N}$. □

Remark. In Theorem 5.1, for each d, there exist infinitely many $c \in \mathbb{Z}[\sqrt{d}]$ satisfying the conditions. For example, let $c = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $k \in \mathbb{N}$, and

$$\begin{aligned} &u = 2k+1, v = 1 && \text{if } d = 2, -2, \\ &u = 2dk, \quad v = 1 && \text{if } d = q, -l, \\ &u = -1, \quad v = 4k && \text{if } d = l, 2l, l_1 l_2. \end{aligned}$$

Then $\Omega_n \cong [C_2]^n$ for $n \geq 1$. All cases can be verified by direct calculation.

References

[BIJ+19] Robert Benedetto, Patrick Ingram, Rafe Jones, Michelle Manes, Joseph Silverman, and Thomas Tucker. Current trends and open problems in arithmetic dynamics. *Bulletin of the American Mathematical Society*, 56(4):611–685, 2019.

[BJ19] Robert L Benedetto and Jamie Juul. Odoni's conjecture for number fields. *Bulletin of the London Mathematical Society*, 51(2):237–250, 2019.

[CH88] Pierre E Conner and Jurgen Hurrelbrink. *Class number parity*, volume 8. World Scientific, 1988.

[Kad20] B. Kadets. Large arboreal galois representations. *Journal of Number Theory*, 210:416–430, 2020.

[Li20] Hua-Chieh Li. Arboreal galois representation for a certain type of quadratic polynomials. *Archiv der Mathematik*, 114(3):265–269, 2020.

[Li21] Hua-Chieh Li. On stoll's criterion for the maximality of quadratic arboreal galois representations. *Archiv der Mathematik*, 117(2):133–140, 2021.

[Loo19] Nicole Looper. Dynamical galois groups of trinomials and odoni's conjecture. *Bulletin of the London Mathematical Society*, 51(2):278–292, 2019.

[Odo85a] R. W. K. Odoni. The galois theory of iterates and composites of polynomials. *Proceedings of the London Mathematical Society*, 3(3):385–414, 1985.

[Odo85b] R. W. K. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *Journal of the London Mathematical Society*, 2(1):1–11, 1985.

[Odo88] R. W. K. Odoni. Realising wreath products of cyclic groups as galois groups. *Mathematika*, 35(1):101–113, 1988.

[Rib13] Paulo Ribenboim. *Classical theory of algebraic numbers*. Springer Science & Business Media, 2013.

[Spe18] Joel Specter. Polynomials with surjective arboreal galois representations exist in every degree. *arXiv preprint arXiv:1803.00434*, 2018.

[Sto92] Michael Stoll. Galois groups over $\mathbb{Q}$ of some iterated polynomials. *Archiv der Mathematik*, 59(3):239–244, 1992.