國立臺灣師範大學理學院數學系

碩士論文

Department of Mathematics, College of Science
National Taiwan Normal University

Master's Thesis

Iterated Galois Groups over Quadratic Number Field

高智強

Kao, Chih-Chiang

指導教授：夏良忠 博士

Advisor: Hsia, Liang-Chung, Ph.D.

中華民國 109 年 7 月

July 2020

Abstract

Consider the base field K is a real quadratic number field and a polynomial X^2+c where c lies in the ring of integer $\mathcal{O}_K$. We will give some criteria on the iterated polynomial $f^n(X)$ of X^2+c to determine whether the Galois group of $f^n(X)$ over K is isomorphic to the wreath product of cyclic group of order 2. Next, we will focus on the following three cases:

1. $K=\mathbb{Q}(\sqrt{2})$;
2. $K=\mathbb{Q}(\sqrt{2p})$ where p is a prime and $p\equiv 3 \pmod 4$;
3. $K=\mathbb{Q}(\sqrt{p})$ where p is a prime and $p\equiv 1 \pmod 4$.

The class number of $\mathbb{Q}(\sqrt{2})$ is one, for the other two cases, we need to assume $h_K=1$. We will give sufficient conditions on c such that the Galois group of the iterated polynomial over K is isomorphic to the iterated wreath product. In the last part, we will prove some 2-independent property of an integer set over a quadratic number field.

Key word: iterated polynomial, arboreal Galois group, iterated wreath product, 2-independent.

Contents

Abstract **i**

1 Introduction **1**

2 Preliminaries **3**

3 Criteria for $\Omega_n \cong [C_2]^n$ **10**

4 Iteration sequences associated to even integer polynomials **17**

5 Some values of c with $|b_i| \notin K^2$ for all $i \geq 2$ **18**
5.1 Case 1: $K = \mathbb{Q}(\sqrt{2})$ 18
5.2 Case 2: $K = \mathbb{Q}(\sqrt{2p})$ and $p \equiv 3 \pmod 4$ 21
5.3 Case 3: $K = \mathbb{Q}(\sqrt{p})$ and $p \equiv 1 \pmod 4$ 23

6 $\Omega_n \cong [C_2]^n$ for $K = \mathbb{Q}(\sqrt{2})$ **27**

7 2-independent property of integers over quadratic number field **31**

References **39**

1 Introduction

Let K be a field of characteristic zero, we consider a sequence of polynomials

$$f_1(X), f_2(X), \cdots \in K[X]$$

where $\deg f_i \geq 2$ for all $i \in \mathbb{N}$. Define

$$F_1(X) = f_1(X) \text{ and } F_{n+1}(X) = F_n(f_{n+1}(X)) \text{ for } n \geq 2,$$

such $F_n(X)$ is called the iterated polynomial of $f_n(X)$. Let K_n be the field obtained by adjoining the roots of $F_n(X)$ to K and denoted the Galois group of K_n over K by Ω_n, called the iterated Galois group. We want to know how large the Galois group can be?

This type of problem is first considered by R. W. K. Odoni [1], he focuses on a function field $K(X,T)$ where X and T are algebraically independent over K. Moreover, we regard X as a variable and T as a parameter. The polynomials which we care about being $f_n(X,T) = X^{k_n} + T$ where k_n are positive integer greater than 1. The main result is the following:

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

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

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

In this case, we called such kind of wreath product the iterated wreath product. If all k_i are equal, namely $C_{k_i} = C_m$ for some m then we denote it by $[C_m]^n$ where n means n times wreath product and called it the n-th iterated wreath product of C_m. There is more detail about iterated wreath product in [8, Section 4].

Note that T can be regarded as a parameter, we can restrict T to any given set. In particular, the first case is to consider $k_i = 2$ for all i, and T varies among integers. The question has been investigated by M. Stoll [2], and in his paper, the basic field is the field of the rational number. The polynomial which we consider is $f(X) = X^2 + c$ where c varies in the set of $\mathbb{Z}$. In this case, we denote the n-th iterated polynomial of $f(X)$ by $f^n(X)$.

By Lemma 1.1 in Odoni's paper [1], we can show that the iterated Galois group of $f^n(X)$ over $\mathbb{Q}$ can be embedded into $[C_2]^n$. The key point is that for $n \geq 2$,

$$\Omega_n \hookrightarrow C_2 \wr_{U_{n-1}} \Omega_{n-1} \hookrightarrow [C_2]^n,$$

by induction. Moreover, he gives some sufficient conditions on c to determine whether the iterated Galois group is isomorphic to the n-th iterated wreath product of C_2.

Theorem (M. Stoll. [2, Theorem]). *If $c \in \mathbb{Z}$ has one of the following properties:*

1. *$c > 0$, and $c \equiv 1 \pmod 4$;*

2. $c > 0$, *and* $c \equiv 2 \pmod 4$*;*

3. $c < 0$, $c \equiv 0 \pmod 4$ *and* $-c$ *is not square in* $\mathbb{Z}$.

then $\Omega_n \cong [C_2]^n$ *for all* $n \geq 1$.

In the conclusion of Odoni and Stoll, they both prove that the iterated Galois group is isomorphic to an iterated wreath product under some condition. On the other hand, there is a relation between tree automorphism group and iterated wreath product of some symmetric groups. Hence, in the next section, we will give an exposition to connect among the three of them.

Stoll's results give us some sufficient conditions to guarantee that the iterated Galois group in our question is the largest possible group, namely the n-th iterated Galois group of a cyclic group C_2. Naturally, we can restrict the parameter T on a set other than integers. Hence, throughout this paper, we assume our basic field to be a real quadratic number field K, and still focus on $X^2 + c$ but c here is a quadratic algebraic integer. We want to know that the largest Galois group of $f^n(X)$ over K and find a sufficient condition on c such that the Galois group as large as possible.

In Odoni's [1] and Stoll's paper [2], a sufficient and necessary condition to determine whether Ω_n is isomorphic to $[C_2]^n$ or not is to consider the constant term of $f^(X)$, called c_n. They prove $\{c_1, \cdots, c_n\}$ is linearly independent over $\mathbb{F}_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ if and only if $\Omega_n \cong [C_2]^n$. However, it is hard to decide whether $\{c_1, \cdots, c_n\}$ is linearly independent over $\mathbb{F}_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ or not, so we use the Möbius inversion formula on c_n to get b_n. Then all b_n are pairwise coprime and $\{b_1, \cdots, b_n\}$ is linearly independent over $\mathbb{F}_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ if and only if $\Omega_n \cong [C_2]^n$. Hence it is enough to show that, for every b_i, there exists a prime element that divides b_i with odd power. In the three cases of Stoll's paper, $|b_i|$ is not a square in $\mathbb{Q}$ for $i \geq 2$ which means b_i appears a new prime element with odd power for $i \geq 2$ and $b_1 = -c \notin \mathcal{O}_K^2$. So $\{b_1, \cdots, b_n\}$ is linearly independent over $\mathbb{F}_2$ in $\mathbb{Q}/\mathbb{Q}^2$ for all n.

Nevertheless, in the case of a real quadratic number field, the unit group of the ring of integer is infinite, so the condition $|b_i|$ is not square in K for $i \geq 2$ which is not enough to guarantee $\{b_1, \cdots, b_n\}$ is linearly independent over $\mathbb{F}_2$ in $K^*/(K^*)^2$ where K is the base field. If we assume $|N_{K/\mathbb{Q}}(b_i)|$ is not square in $\mathbb{Q}$ for $i \geq 2$ then we can deduce that $\Omega_n \cong [C_2]^n$ for $n \geq 1$. But it is hard to prove $|N_{K/\mathbb{Q}}(b_i)|$ is not square in $\mathbb{Q}$ for $i \geq 2$. However, for $K = \mathbb{Q}(\sqrt{2})$, we can use another method to prove that b_i can be divided by some prime element with odd power for $i \geq 3$, and we can show that $\{b_1, b_2\}$ is linearly independent over $\mathbb{F}_2$ in $K^*/(K^*)^2$ by direct computation. Hence $\Omega_n \cong [C_2]^n$ for all $n \geq 1$ as $K = \mathbb{Q}(\sqrt{2})$.

In my thesis, we will follow Odoni and Stoll's method. Due to technical reasons, we assume that the ring of integer of K is a unique factorization domain. First, we will show that the iterated Galois group of $f^n(X)$ also can be embedded into $[C_2]^n$ so the largest possible Galois group is isomorphic to $[C_2]^n$. Next, we will focus on some real quadratic number fields and give sufficient conditions on c such that $|b_i| \notin \mathcal{O}_K^2$ for $i \geq 2$. Moreover, for $K = \mathbb{Q}(\sqrt{2})$, such kind of c will imply $\Omega_n \cong [C_2]^n$. The main theorem in my thesis is the following:

Theorem. *Assume that K is a real quadratic number field of class number one. Consider $f(X) = X^2 + c \in \mathcal{O}_K[X]$ with $N_{K/\mathbb{Q}}(c) > 0$ where $\mathcal{O}_K$ is the ring of integer of K, for the following three cases:*

1. *$K = \mathbb{Q}(\sqrt{2})$, and $c = u + v\sqrt{2}$ where u, v are positive odd integer.*
2. *$K = \mathbb{Q}(\sqrt{2p})$ where p is a prime and $p \equiv 3 \pmod 4$, and $c = u + v\sqrt{2p}$ where u, v are positive integer and $u \equiv -1 \pmod{2p}$, $v \equiv 1 \pmod 2$.*
3. *$K = \mathbb{Q}(\sqrt{p})$ where p is a prime and $p \equiv 1 \pmod 4$, and $c = u + v\left(\frac{1+\sqrt{p}}{2}\right)$ where u, v are positive integer and $u \equiv -1 \pmod{4p}$, $v \equiv 2p \pmod{4p}$.*

$|b_i|$ is not a square in $\mathcal{O}_K$ for $i \geq 2$. Moreover, if c satisfies case 1, then $\Omega_n \cong [C_2]^n$.

In the next section, we will give some preliminary knowledge that contains wreath product, tree automorphism, and some results in algebraic number theory. In the third section, we will give some criteria to determine an iterated Galois group whether is isomorphic to the n-th iterated wreath product of C_2 or not. In the fourth section, we extend the condition of Lemma 2.1 in Stoll's paper [2] from integer into quadratic algebraic integer. The fifth section, let c satisfies the conditions in Section 5, we give some sufficient conditions on c such that $|b_i|$ is not square in $\mathcal{O}_K$ for $i \geq 2$. In the sixth section, we will prove $\Omega_n \cong [C_2]^n$ as $K = \mathbb{Q}(\sqrt{2})$. In the last section, we get back to consider c is an integer, and determine whether the set $\{b_1, b_2, \cdots\}$ is 2-independent over quadratic number field or not. Moreover, we will give some sufficient conditions on c to prove $\mathrm{Gal}(f^n(X)/K) \cong [C_2]^n$ for $K = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ as $n \geq 1$.

2 Preliminaries

First, we will introduce the wreath product and tree automorphism. The main reference is from J. Rotman's book [4, Chapter 7, p.167 − p.177].

Definition. A group G is a *semidirect product* of K by Q, denoted by $G = K \rtimes Q$, if $K \trianglelefteq G$ and there exists a subgroup Q' of G where $Q' \cong Q$ such that $K \cap Q' = \{e\}$ and $KQ' = G$.

Definition. Let D and Q be groups, Λ be a finite Q-set, and $K = \prod_{\lambda \in \Lambda} D_\lambda$, where $D_\lambda \cong D$ for all $\lambda \in \Lambda$. Then the *wreath product* of D by Q, denoted by $D \wr_\Lambda Q$, is the semidirect product of K by Q, where Q acts on K by $q \cdot (d_\lambda) = (d_{q\lambda})$ for $q \in Q$ and $(d_\lambda) \in \prod_{\lambda \in \Lambda} D_\lambda$.

Definition. A *graph* Γ is a nonempty set V, called *vertices*, together with an *adjacency* relation on V, denoted by $v \sim u$, that is symmetric ($v \sim u$ implies $u \sim v$ for all $u, v \in V$) and irreflexive ($v \not\sim v$ for all $v \in V$).

Definition. A *tree* is a graph Γ which is connected and there does not exist a loop in Γ, which means there does not exist $\{v_1, \cdots, v_k\} \subset V$ such $v_i \sim v_{i+1}$ for $i = 1, \cdots, k-1$ and $v_k \sim v_1$.

We say a graph is a *rooted tree* if Γ is a tree in which a special vertex is singled out and called *root* which is always denoted by 0. We define a partial order on Γ by considering the root which is a minimal element and it is the only vertex of level zero. If $v \sim 0$ then $v \in V$ is level one, all level one vertices are denoted by L_1. The set of level n vertices denoted by L_n. For $v \in V \backslash L_{n-2}$, if $v \sim v'$ for some $v' \in L_{n-1}$ then $v \in L_n$. Here if $v' \in L_{n-1}$, $v \in L_n$ and $v' \sim v$ then we say v' is a *parent* and v is a *child*. If there exists the largest level k in Γ then we call the level of Γ is k. In the figure of Γ, the root will be drawn in the bottom.

A *rooted binary tree* is a rooted tree in which every vertex has at most two children. A rooted binary tree of level k which has exactly $2^k - 1$ vertices is called a *rooted full binary tree* of level k.

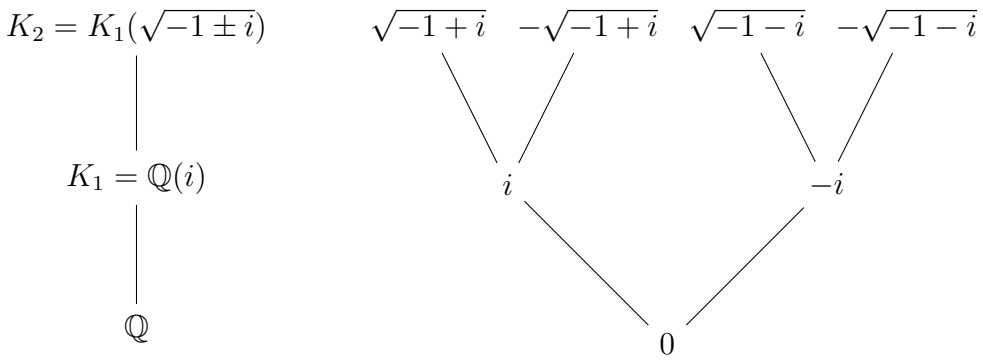
Definition. A *tree automorphism* for a rooted tree T with vertices V is a bijection $\varphi : V \to V$ such that $u, v \in V$ are adjacent if and only if $\varphi(u)$ and $\varphi(v)$ are adjacent, thus φ will preserve the order of vertices. Here, the root 0 is the fixed point of any automorphism. It is plain that the set of all tree automorphism of a tree T detonated by $\mathrm{Aut}_0(T)$, is a group under composition.

Here, we show an example first to understand the operation of tree automatism. Give a rooted tree, T as follows:

If $\varphi \in \mathrm{Aut}_0(T)$, then φ fixes 0 since it is the only vertex adjacent to 4 vertices, $\widetilde{\varphi}$ permutes on $\Gamma = \{1, 2, 3, 4\}$, and for each $i \in \Gamma$, φ induces a bijective map from $\{a_i, b_i\}$ to $\{a_{\widetilde{\varphi}(i)}, b_{\widetilde{\varphi}(i)}\}$. Clearly, S_4 can act on Γ and S_2 can act on $\Lambda = \{a, b\}$. We can identify $\{a_i, b_i : i \in S\}$ with $\Gamma \times \Lambda$ by writing a_i as (a, i) and b_i as (b, i). Hence, we have $\mathrm{Aut}_0(T) \cong S_2 \wr_\Gamma S_4$.

Now, we will explain the relation between the iterated Galois group of $X^2 + c$ and the tree automorphism group. Let $V_n = \bigcup_{i=0}^{n} \{f^{-i}(0)\}$, we consider a tree T_n with vertices, V_n. If $v, v' \in V_n$ and $v' = f(v)$ then $v \sim v'$ where v' is parent and v is child. Note that since our basic field is characteristic zero if $f^n(X)$ has multiple roots then it must be 0. Assume none of $f^{-n}(0)$ is equal, V_n has $2^{n+1} - 1$ elements and so T_n is a rooted fully binary tree.

Here, we consider an example for the Galois group of $f^2(X)$ over $\mathbb{Q}$ where $f(X) = X^2+1$.



The left-hand side is the tower of field extension of $f^2(X)$ where $f(X) = X^2 + 1$. On the other hand, on the right-hand side, we have a 2-level rooted full binary tree, T_2. The root is zero, the first level is roots of $f(X)$ and the second level is roots of $f^2(X)$. For any $\varphi \in \mathrm{Gal}(K_2/\mathbb{Q})$, we can verify it as a tree automorphism on T_2 by permuting the vertices. Hence we can embed $\mathrm{Gal}(K_2/\mathbb{Q})$ into $\mathrm{Aut}_0(T_2)$ by Galois theory. Moreover, we have a fact that if T_n is a rooted full binary tree then $\mathrm{Aut}_0(T_n) \cong [C_2]^n$. Therefore, Stoll tells us under some conditions of c, the iterated Galois group is isomorphic to $\mathrm{Aut}_0(T_n)$. According to this relation, we know that the largest Galois group is isomorphic to n-th iterated wreath product of C_2. The results of Stoll shows that for c satisfy those conditions, then $\mathrm{Gal}(K_n/\mathbb{Q})$ is as large as possible.

Next, we will give some preliminary about algebraic number theory, the following topic can be found in most books about algebraic number theory. The main textbooks I use are M. Rosen [3, Chapter 6,12,13] and J. Neukirch [5, Chapter 4]. There is also some knowledge about commutative algebra which refers to M. F. Atiyah [7, Chapter 5].

Definition. A *Kummer extension* is an extension of a field k of characteristic $p \geq 0$, of the type

$$K = k(a_1^{1/n}, \cdots, a_t^{1/n})$$

where $a_1, \ldots, a_t \in k$, n is some natural number, and it is assumed that k contains the n-th root of unities (in particular, if $p \neq 0$ then n is prime to p)

Definition. The *exponent* of a group G is the least natural number n such that for all $g \in G, g^n = e$. If L/K is an abelian extension and the exponent of $\mathrm{Gal}(L/K)$ is n then we say that the abelian extensions L over K of exponent n.

Theorem. *Let n be a natural number which is relatively prime to characteristic of the field k, and assume that k contains all n-th roots of unity.*

Then the abelian extensions K over k of exponent n correspond one-to-one to the finite subgroups $\triangle$ of $k^*/(k^*)^n$, via the rules

$$\triangle \mapsto K = k(\sqrt[n]{\triangle}) \text{ where } \sqrt[n]{\Delta} = \{a^{\frac{1}{n}} : a \in k^*, a \cdot (k^*)^n \in \Delta\}$$

and

$$K \mapsto (k^* \cap (K^*)^n)/(k^*)^n.$$

Moreover, we have

$$\mathrm{Gal}(K/k) \cong \mathrm{Hom}(\triangle, \mu_n)$$

where μ_n is the group of n-th roots of unity.

Remark. By Kummer theory, we define K/k to be a 2-Kummer extension if $\mathrm{char}\, k \neq 2$ and $K = k(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_n})$ for some $a_1, a_2, \cdots, a_n \in k, n \in \mathbb{N}$.

Definition. Let L be a finite field extension of degree n over K. Suppose $\alpha_1, \cdots, \alpha_n$ is a basis for L/K and $\alpha \in L$. Then

$$\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \text{ for } i = 1, \cdots n \text{ where } a_{ij} \in K.$$

The *norm* of α for L to K is defined to be

$$N_{L/K}(\alpha) = \det(a_{ij}),$$

and the *trace* of α is

$$T_{L/K}(\alpha) = a_{11} + \cdots + a_{nn}.$$

Definition. If $\alpha_1, \cdots, \alpha_n$ is an n-tuple of elements of L, the *discriminant* $\Delta(\alpha_1, \cdots, \alpha_n)$ is defined to be $\det(T_{L/K}(\alpha_i\alpha_j))$.

Definition. A subfield K of the complex numbers is called an *(algebraic) number field* if $[K : \mathbb{Q}] < \infty$. We call an algebraic number field K a *quadratic number field* if $[K : \mathbb{Q}] = 2$.

Definition. Let B be a ring and A be a subring of B. An element $\alpha \in B$ is said to be *integral* over A if there exists a nonzero monic polynomial $f(x) \in A[x]$ such that α is a root of $f(x)$. Here, α is called an *algebraic integer* if α is integral over $\mathbb{Z}$.

If K is an algebraic number field, the subset of K consisting of algebraic integers called the *ring of (algebraic) integers* of K, denoted by $\mathcal{O}_K$.

Theorem. *The ring of integer, $\mathcal{O}_K$, of K forms a ring.*

Proof. It is sufficient to show that if $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. First, we claim that $\mathbb{Z}[\alpha]$ is a finitely-generated $\mathbb{Z}$-module if and only if α is integral over $\mathbb{Z}$.

Suppose α is an algebraic integer, then there exists a nonzero monic polynomial $f(x) \in \mathbb{Z}[x]$ such that

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \text{ where } a_i \in \mathbb{Z}, n \in \mathbb{N}.$$

For any $\alpha^{n+r} \in \mathbb{Z}[\alpha]$ where $r \geq 0$, we have

$$\alpha^{n+r} = -(a_{n_1}\alpha^{n-1+r} + \cdots + a_1\alpha^{r+1} + a_0\alpha^r),$$

and by induction, all positive powers of α lie in $\mathbb{Z}[\alpha]$ which are generated by $1, \alpha, \cdots, \alpha^{n-1}$. Hence $\mathbb{Z}[\alpha]$ is finitely-generated.

Conversely, suppose $\mathbb{Z}[\alpha]$ is a finitely-generated $\mathbb{Z}$-module and the generators of $\mathbb{Z}[\alpha]$ are $\alpha_1, \cdots, \alpha_n$, we consider that

$$\alpha\alpha_i = \sum_{i=1}^{n} a_{ij}\alpha_j \text{ where } a_{ij} \in \mathbb{Z}.$$

Set a $n \times n$ matrix $A = (a_{ij})$, then α is an eigenvalue of A. Hence α is a root of the characteristic polynomial of A which is a monic integer-valued polynomial and so α is an algebraic integer.

Suppose α, β are algebraic integers, then $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ are both finitely-generated and denoted their generators by $\{1, \alpha, \cdots, \alpha^m\}$ and $\{1, \beta, \cdots, \beta^n\}$, respectively. Then $\{\alpha^i\beta^j : 0 \leq i \leq m, 0 \leq j \leq n\}$ are generators of $\mathbb{Z}[\alpha, \beta]$. By Hilbert's basis theorem, $\mathbb{Z}[\alpha, \beta]$ is Noetherian $\mathbb{Z}$-module. Hence $\mathbb{Z}[\alpha + \beta]$ and $\mathbb{Z}[\alpha\beta]$ are finitely-generated submodules of $\mathbb{Z}[\alpha, \beta]$. Hence $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

Definition. An integral domain R, that is not a field, is called a *Dedekind domain* if R is Noetherian, integrally closed and every nontrivial prime ideal is a maximal ideal of R.

Proposition. *The ring of integers of a number field, $\mathcal{O}_K$ is a Dedekind domain.*

A basic fact is that every nonzero proper ideal in a Dedekind domain, R, can be uniquely factored into a product of prime ideals up to the order of the product. Moreover, if A, B are two ideals in R and $A \subset B$ then there exists $C \trianglelefteq R$ such that $B = AC$.

Definition. A set $\{\alpha_1, \cdots, \alpha_n\} \subset \mathcal{O}_K$ is called an *integral basis* of $\mathcal{O}_K$ if

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Definition. Let K be a number field, a *fractional ideal* of K is a finitely generated nonzero $\mathcal{O}_K$-submodule of K. Note that the fractional ideals form an abelian group, called the *ideal group* J_K of K.

The fractional principal ideal $(a) = a\mathcal{O}_K, a \in K^*$, form a subgroup of the group of ideals J_K, which will be denoted P_K. The quotient group

$$\mathrm{Cl}_K = J_K/P_k$$

is called the *ideal class group*. Note that Cl_K is finite, and its order

$$h_K = (J_K : P_K)$$

is called the *class number* of K.

Proposition. *Let K be a number field, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a unique factorization domain.*

Proof. If $h_K = 1$ then every ideal is principal ideal, thus $\mathcal{O}_K$ is a principal ideal domain and so a unique factorization domain.

Conversely, we want to show that if $\mathcal{O}_K$ is a unique factorization domain then $h_K = 1$. Let $\mathfrak{p}$ be a nonzero proper prime ideal of R and choose $0 \neq x \in \mathfrak{p}$. Since $\mathfrak{p}$ is a proper ideal so x is not a unit. Since $\mathcal{O}_K$ is UFD so we can write x as $p_1^{a_1} \cdots p_k^{a_k}$ where p_i are distinct prime in $\mathcal{O}_K$, $a_i \in \mathbb{N}$ and $k \geq 1$. Since $x \in \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal so one of $p_i \in \mathfrak{p}$, say p_1. Then $(p_1) \subset \mathfrak{p}$. Note that since p_1 is prime so (p_1) is a prime ideal and $\mathcal{O}_K$ is a Dedekind domain so (p_1) is maximal. However $\mathfrak{p}$ is a proper ideal of $\mathcal{O}_K$ which contains (p_1), thus $\mathfrak{p} = (p_1)$ and so every prime ideal in $\mathcal{O}_K$ is principal. Since every ideal in $\mathcal{O}_K$ can be uniquely factored into a product of prime ideals. Hence every ideal is principle. □

Let K be a number field, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal in $\mathbb{Z}$. Hence, it is natural to consider for any nonzero prime ideal in $\mathbb{Z}$, how can it be decomposed in $\mathcal{O}_K$.

Definition. Let (p) be a prime ideal of $\mathbb{Z}$ and $\mathfrak{p}_i$ be prime ideals of $\mathcal{O}_K$ contains $p\mathcal{O}_K$, then

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \text{ where } e_i \geq 1.$$

The number e_i is called the ramification index of $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is maximal ideal for all i so $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field which contains $\mathbb{Z}/p\mathbb{Z}$. Thus the degree of $\mathcal{O}_K/\mathfrak{p}_i$ over $\mathbb{Z}/p\mathbb{Z}$ is called the degree of $\mathfrak{p}_i$.

Theorem. *For any prime ideal (p) in $\mathbb{Z}$, if $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ with degree of $\mathcal{O}_K/\mathfrak{p}_i$ over $\mathbb{Z}/p\mathbb{Z}$, f_i. Then*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Proof. First, we claim that if $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$, e is the ramification index of $\mathfrak{p}$ and f is the degree of $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{Z}/p\mathbb{Z}$ then the number of elements in $\mathcal{O}_K/\mathfrak{p}^e$ is p^{ef}.

Since its degree is f, so the number elements in $\mathcal{O}_K/\mathfrak{p}$ is p^f. This statement is true for $e = 1$. Since $\mathfrak{p}^{e-1}/\mathfrak{p}^e$ is a subgroup of $\mathcal{O}_K/\mathfrak{p}^e$, by the second law of isomorphism,

$$(\mathcal{O}_K/\mathfrak{p}^e)/(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \cong \mathcal{O}_k/\mathfrak{p}^{e-1}.$$

It is enough to show that $\mathfrak{p}^{e-1}/\mathfrak{p}^e$ has p^f elements, then we get the result by induction.

Since $\mathfrak{p}^e \subsetneq \mathfrak{p}^{e-1}$ so there exists $\alpha \in \mathfrak{p}^{e-1} \backslash \mathfrak{p}^e$. We want to show that $(\alpha) + \mathfrak{p}^e = \mathfrak{p}^{e-1}$. Note that, we have

$$\mathfrak{p}^e \subsetneq (\alpha) + \mathfrak{p}^e \subseteq \mathfrak{p}^{e-1},$$

so there exists $A, B \trianglelefteq \mathcal{O}_K$ where A is nontrivial such that $((\alpha) + \mathfrak{p}^e)A = \mathfrak{p}^e$ and $B\mathfrak{p}^{e-1} = (\alpha) + \mathfrak{p}^e$. By the unique factorization property in Dedekind domain, $AB = \mathfrak{p}$, thus $A = \mathfrak{p}$ and so $(\alpha) + \mathfrak{p}^e = \mathfrak{p}^{e-1}$.

Consider a map from $\mathcal{O}_K$ to $\mathfrak{p}^{e-1}/\mathfrak{p}^e$ by $\gamma \mapsto \gamma\alpha + \mathfrak{p}^e$. It is easy to show that it is a homomorphism and surjective. γ is in the kernel if and only if $\gamma\alpha \in \mathfrak{p}^e$ if and only if $v_\mathfrak{p}(\gamma\alpha) \geq e$. Since

$$v_\mathfrak{p}(\gamma\alpha) = v_\mathfrak{p}(\gamma) + v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\gamma) + e - 1,$$

so γ is in the kernel if and only if $v_{\mathfrak{p}}(\gamma) \geq 1$ which equivalent to saying $\gamma \in \mathfrak{p}$. Hence $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{e-1}/\mathfrak{p}^e$ and so the latter group has p^f elements. □

Theorem. *Suppose $K/\mathbb{Q}$ is a Galois extension. Let (p) be a prime ideal in $\mathbb{Z}$ and*

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

Then $e_1 = \cdots = e_g$ and $f_1 = \cdots = f_g$. If e and f denote these common values, then $efg = n$.

Proof. Note that if $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ and $A \trianglelefteq \mathcal{O}_K$ then φA also is an ideal in $\mathcal{O}_K$. Also $\varphi\mathcal{O}_K = \mathcal{O}_K$. Thus $\mathcal{O}_K/\varphi A = \varphi\mathcal{O}_K/\varphi A \cong \mathcal{O}_K/A$. In particular, if P is a prime ideal in $\mathcal{O}_K$ then φP also is a prime ideal in $\mathcal{O}_K$. Moreover, we have a fact that if $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ then there exists $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\varphi\mathfrak{p}_i = \mathfrak{p}_j$ for any $i \neq j$.

Hence, for a given index i there exists $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\varphi\mathfrak{p}_1 = \mathfrak{p}_i$. Since $\mathcal{O}_k/\mathfrak{p}_1 \cong \mathcal{O}_k/\varphi\mathfrak{p}_1 = \mathcal{O}_k/\mathfrak{p}_i$ so $f_1 = f_i$ for all i. Thus, all f_i are equal.

Apply φ to both sides of $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. Since $p \in \mathbb{Z}$ it is clear that $\varphi(p) = p$. Thus

$$(p) = (\varphi\mathfrak{p}_1)^{e_1} \cdots (\varphi\mathfrak{p}_g)^{e_g}.$$

In this product, we see the exponent of $\mathfrak{p}_i = \varphi\mathfrak{p}_1$ is e_1. However, in the original expression, the exponent of $\mathfrak{p}_i$ is e_i. By the uniqueness of prime factorization, we must have $e_1 = e_i$ for all i.

Finally, since $\sum_{i=1}^{g} e_i f_i = n$ we see that $efg = n$. □

Now, we focus on the quadratic number field. The following useful results are well-known in algebraic number theory. We skip the proof and it can be found in M. Rosen's book [3, Chapter 13, p.188 − p.191].

Proposition. *If K is a quadratic number field, then $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and d is square-free. Moreover,*

$$\mathcal{O}_K = \mathbb{Z} + \omega_d\mathbb{Z}$$

where

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Proposition. *Let δ_K denote the discriminant of $K = \mathbb{Q}(\sqrt{d})$. Then*

$$\delta_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod 4, \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Since $n = 2$ so $efg = n = 2$ by previous Theorem, and we have three cases; $e = 2, f = g = 1$, or $g = 2, e = f = 1$, or $f = 2, e = g = 1$. We say, respectively, that p ramifies, splits, or is inertial. Moreover, we have a method to determine which kind of a prime ideal in $\mathbb{Z}$ can be factored in $\mathcal{O}_K$.

Proposition. *Consider $K = \mathbb{Q}(\sqrt{d})$, suppose p is an odd prime.*

1. *If $p \nmid \delta_K$ and $(\frac{d}{p}) = 1$ then (p) is split.*
2. *If $p \nmid \delta_K$ and $(\frac{d}{p}) = -1$ then (p) is inertial.*
3. *If $p \mid \delta_K$ then (p) is ramified.*

Proposition. *Consider $K = \mathbb{Q}(\sqrt{d})$.*

1. *If $2 \nmid \delta_K$ and $d \equiv 1 \pmod 8$ then (2) is split.*
2. *If $2 \nmid \delta_K$ and $d \equiv 5 \pmod 8$ then (2) is inertial.*
3. *If $2 \mid \delta_K$ then (2) is ramified.*

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

We follow the idea from M. Stoll [2] to study a similar question for c in real quadratic number field of class number one. Here we denote the real quadratic number field by K and the ring of integer of K is $\mathcal{O}_K$ which we assume to be a unique factorization domain. The following theorems mainly follow from M. Stoll's paper [2]. As we consider parameter c ranges over a real quadratic number field which is different from Stoll's case, for the reader's convenience, we will give a detailed proof if necessary.

Throughout this paper, c is a quadratic integer such that $-c$ is not a square in $\mathcal{O}_K$. We take

$$f(X) \coloneqq X^2+c \in \mathcal{O}_K[X], f^0(X) \coloneqq X, \text{ and } f^{n+1}(X) \coloneqq f(f^n(X)) = (f^n(X))^2+c \text{ for all } n \geq 0,$$

which is the iterate polynomial of $f(X)$ as the composition $\underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$ of polynomials, also we have $f^{n+1}(X) = f^n(f(X)) = f^n(X^2 + c)$. Let

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

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

$$\Omega_n \coloneqq \mathrm{Gal}(f^n(X)/K) = \mathrm{Gal}(K_n/K)$$

its Galois group over K. First, we have the following proposition:

Proposition (c.f. [2, Fact 1.0])**.**

1. *$f^n(X)$ has degree 2^n.*
2. *For $n \geq 0$, $K_{n+1} = K_n(\sqrt{\alpha - c} \mid \alpha$ are roots of $f^n)$ where $K_0 = K$.*

3. $[K_{n+1} : K_n] \leq 2^{2^n}$.

Proof. These facts are stated in M. Stoll's paper, for the sake of completeness we give a brief proof below.

1. This can be proved by induction.

2. Note that if γ is a root of $f^{n+1}(X)$ then

$$0 = f^{n+1}(\gamma) = f^n(\gamma^2 + c).$$

Hence $\gamma^2 + c = \alpha$ for some root α of f^n, and so $\gamma = \pm\sqrt{\alpha - c}$.
Since K_n is the splitting field of f^n over K so

$$K_{n+1} = K(\gamma \mid \gamma \text{ are roots of } f^{n+1}) = K(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n).$$

On the other hand, since

$$K_n = K(\alpha \mid \alpha \text{ are roots of } f^n)$$

so

$$K_n \subset K(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n),$$

and

$$K_n(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n) \subset K(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n).$$

Because $K \subset K_n$,

$$K_n(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n) = K(\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n) = K_{n+1}.$$

Moreover, by Kummer theory, K_{n+1}/K_n is a 2-Kummer extension.

3. Here $\sqrt{\alpha - c}$ is a fixed root of $x^2 = \alpha - c$, then

$$\#\{\sqrt{\alpha - c} \mid \alpha \text{ are roots of } f^n\} = 2^n.$$

Let $\langle\overline{\alpha_1 - c}, \ldots, \overline{\alpha_{2^n} - c}\rangle$ be the subgroup of $K_n^*/(K_n^*)^2$ generated by $\alpha_1 - c. \cdots, \alpha_{2^n} - c$. Since K_{n+1}/K_n is a 2-Kummer extension, by Kummer theory,

$$\mathrm{Gal}(K_{n+1}/K_n) \cong \langle\overline{\alpha_1 - c}, \ldots, \overline{\alpha_{2^n} - c}\rangle$$

which is isomorphic to a subgroup of $(C_2)^n$.

□

Lemma 3.1 (c.f. [1, Lemma 4.4] and [2, Lemma 1.1])**.**

1. *If* $c \notin (-2, 0)$ *then* $c_n \neq 0$ *for all* $n \in \mathbb{N}$. *Moreover, if* $K = \mathbb{Q}(\sqrt{d})$ *where* $d \equiv 2, 3 \pmod 4$ *and* $c \in \mathcal{O}_K$ *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 :*
   For all $n \geq 1$, $c_n = \prod_{d|n} b_d$, *and* b_n *are pairwise coprime.*

Proof.

1. First, we assume that $c \notin (-2, 0)$. We want to show that $c_n \geq |c|$ for $n \geq 2$. For $n = 2$,
$$c_2 = c^2 + c = c(c+1) \geq |c| \geq 0.$$
Suppose for $n = k-1$, $c_{k-1} \geq |c|$ then consider $n = k$, we have
$$c_k = c_{k-1}^2 + c \geq c^2 + c \geq |c| > 0.$$
By induction, $c_n \geq |c| > 0$ for all $n \geq 2$ and $c \neq 0$ so $c_n \neq 0$ for all $n \in \mathbb{N}$.
Next, we deal with $c \in \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{d})$ and $d \equiv 2, 3 \pmod 4$ then $c = u + v\sqrt{d}$ where $u, v \in \mathbb{Z}$ for all $c \in \mathcal{O}_K$. We denoted $c_n = u_n + v_n\sqrt{d}$, since $c_n = c_{n-1}^2 + c$, so
$$c_n = u_n + v_n\sqrt{d} = (u_{n-1}^2 + dv_{n-1}^2 + u) + (2u_{n-1}v_{n-1} + v)\sqrt{d}.$$
We claim that $|v_n| \geq |v|$ for all n. We only need to consider $c \in \mathcal{O}_k \backslash \mathbb{Z}$ so $v \neq 0$ and clearly $v_1 = -v$. Moreover,
$$|v_2| = |2uv + v| = |v| \cdot |2u + 1| \geq |v| \text{ since } u \in \mathbb{Z}.$$
Now, we assume that for $n = k-1$, $|v_{k-1}| \geq |v|$ then consider $n = k$, we have
$$|v_k| = |2u_{k-1}v_{k-1} + v| \geq ||2u_{k-1}v_{k-1}| - |v||.$$
If $u_{k-1} = 0$ then $|v_k| \geq |v|$. If not, then
$$|v_k| \geq ||2u_{k-1}v_{k-1}| - |v|| \geq ||2v_{k-1}| - |v|| \geq ||2v| - |v|| = |v|.$$
Hence $|v_n| \geq |v| > 0$ for all $n \in \mathbb{N}$ and so $c_n \neq 0$ for all $n \in \mathbb{N}$.

2. Since $c_n \neq 0$, we can define
$$b_n \coloneqq \prod_{d|n} c_d^{\mu(n/d)} \in K$$
where μ is the Möbius function, and have to show that $b_n \in \mathcal{O}_K$.
Let π be a prime element in $\mathcal{O}_K$ which divides at least one of c_n. Let
$$m = \min\{n \geq 1 : \pi \mid c_n\} \text{ and } e = v_\pi(c_m).$$
First, we claim that if $m \mid n$ then $v_\pi(c_n) = e$ and $v_\pi(c_n) = 0$ if $m \nmid n$.

Note that $\pi \nmid c_i$ for $i = 1, \cdots, m-1$ and $v_\pi(c_m) = e$. Since $c_m = f^m(0)$ so we denote $f^m(x)$ by $g(x)$, thus

$$f^m(x) = g(x) = g(0) + g'(0)x + \frac{g''(0)}{2}x^2 + \cdots .$$

Moreover, since $g'(x) = f'(f^{n-1}(x)) \cdot \cdots \cdot f'(f(x)) \cdot f'(x)$ so $g'(0) = 0$.

First, we prove that if $m \mid n$ then $v_\pi(c_n) = e$, by induction. Let $n = km$ and suppose $v_\pi(c_{(k-1)m}) = v_\pi(g^{k-1}(0)) = e$. Then

$$c_n = g^n(0) = g(0) + (g^{k-1}(0))^2 h(0) \text{ where } h(X) \in \mathcal{O}_K[X].$$

Hence

$$v_\pi(c_n) = v_\pi(g^n(0)) = \min\{v_\pi(g(0)), v_\pi((g^{k-1}(0))^2 h(0))\} = e,$$

since $v_\pi((g^{k-1}(0))^2 h(0)) \geq 2e$.

For any $n \geq 2$, let $n = km + r$ where $r = 1, \cdots, m-1$. Then

$$c_n = f^r(f^{km}(0)) = f^r(c_{km}) \equiv f^r(0) \pmod{\pi},$$

and $f(0) = -c_1, f^r(0) = c_r$ for $r = 2, \cdots, n-1$. Hence $v_\pi(c_n) = 0$ if $m \nmid n$. So, $v_\pi(c_n) = e$ if $m \mid n$, and 0 otherwise. Thus

$$v_\pi(b_n) = \sum_{d|n} v_\pi(c_d) \cdot \mu(n/d) = e, \text{ if } n = m.$$

For otherwise case, if $m \nmid n$ then $v_\pi(c_d) = 0$ for all d. Thus, we only need to consider $m \mid n$ as following:

$$v_\pi(b_n) = \sum_{d|n} v_\pi(c_d) \cdot \mu(n/d) = e \cdot \sum_{lm|n} \mu(n/lm) = e \cdot \sum_{l|\frac{n}{m}} \mu\left(\frac{n/m}{l}\right) = 0.$$

Hence, for any prime element π, $v_\pi(b_n) \geq 0$ for all $n \in \mathbb{N}$, and so $b_n \in \mathcal{O}_K$. Moreover, for fixed π, $v_\pi(b_m) = e$ and $v_\pi(b_n) = 0$ for $n \neq m$. That means b_n are pairwise coprime. Clearly, use Möbius inversion formula, we get $c_n = \prod_{d|n} b_d$.

□

Remark. In the previous proposition and lemma, we don't need to assume $\mathcal{O}_K$ is a unique factorization domain. However, to prove the following lemma, we need the hypothesis of class number one in K.

Lemma 3.2 (c.f. [2, Lemma 1.2])**.** *If none of $c_1, c_2, \cdots, c_n$ is a square in $\mathcal{O}_K$, then $f^n(X)$ is irreducible in $\mathcal{O}_K[X]$.*

Proof. Assume $f^n(X)$ is reducible, let $m \coloneqq \min\{k : f^k(X) \text{ is reducible}\}$, then $1 < m \leq n$. We have $f^{m-1}(X)$ is irreducible, and $f^m(X) = f^{m-1}(X^2 + c)$ is reducible. We claim that if $h(X)$ is an even polynomial and $h(X) \mid f^m(X)$ then $h(X)$ is a constant. By our hypothesis, $f^m(X) = h(X)g(X)$ for some $g(X) \in \mathcal{O}_K[X]$. Since both $f^m(X)$ and $h(X)$ are even, we can deduce that $g(X)$ is an even polynomial via

$$h(X)g(X) = f^m(X) = f^m(-X) = h(-X)g(-X) = h(X)g(-X).$$

Thus we can change the variable X^2 into y, then $f^{m-1}(y + a) = \hat{h}(y)\hat{g}(y)$. Hence $f^{m-1}(X)$ is reducible which contradicts the hypothesis.

Since $f^m(X)$ is an even polynomial, if $h(X)$ is a nontrivial divisor of $f^m(X)$, then so is $h(-X)$. Suppose $g(X) = \gcd(h(X), h(-X)) \in K[X]$ then we can find $q(X), r(X) \in \mathcal{O}_K[X]$ such that

$$\begin{cases} h(X) = g(X)q(X) \\ h(-X) = g(X)r(X) \end{cases} \Rightarrow \begin{cases} h(-X) = g(-X)q(-X) \\ h(X) = g(-X)r(-X) \end{cases}$$

where we use the hypothesis of $\mathcal{O}_K$ is a unique factorization domain. Since $g(X)$ is the greatest common divisor of $h(X), h(-X)$ and $g(-X)$ is a common divisor of $h(X), h(-X)$, thus $g(-X) \mid g(X)$. Hence $g(X) = \pm g(-X)$ by comparing their leading coefficients.

If $g(X) = -g(-X)$, that means the degree of $g(X)$ is odd and so $X \mid g(X)$. However $g(X) \mid h(X)$ and $h(X) \mid f^m(X)$ so $X \mid f^m(X)$ but $f^m(0) = c_m \neq 0$ for all $m \geq 1$ which is absurd.

Hence $g(X) = g(-X)$, that means $g(X)$ is an even polynomial. But we have shown that $f^m(X)$ has no nontrivial even degree divisor, so $g(X)$ must be a constant. Since the leading coefficient of $f^m(X)$ is 1, and $g(X) \mid f^m(X)$ so $g(X) \mid 1$. Hence $g(X)$ is a unit and $h(X)$ and $h(-X)$ are coprime. Thus, $f^m(X)$ being reducible, and there exists a polynomial $k(X)$ with $f^m(X) = k(X) \cdot k(-X)$. In particular, $c_m = f^m(0) = k(0)^2$ is a square in $\mathcal{O}_K$. □

Lemma 3.3 ([2, Lemma 1.4])**.** *For all $n \in \mathbb{N}$, we have $\Omega_n \hookrightarrow [C_2]^n$. In particular, if $[K_{n+1} : K_n] = 2^{2^n}$ then*

$$\Omega_{n+1} \cong [C_2]^{n+1} \Leftrightarrow \Omega_n \cong [C_2]^n.$$

Proof. See Lemma 1.4 in Stoll's paper [2]. □

Definition. For nonzero numbers $a_1, \cdots, a_n$ 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.

Lemma 3.4 (c.f. [2, Lemma 1.5])**.** *If $\Omega_n \cong [C_2]^n$ and $c_1, c_2, \cdots, c_n$ are 2-independent over K, then for all $\gamma \in K^*$:*

$$\gamma \notin (K_n^*)^2 \Leftrightarrow c_1, c_2, \cdots, c_n, \gamma \text{ are 2-independent over } K.$$

Proof. Note that we have the following fact which is proved by induction : for a transitive permutation group G, one has

$$(H \wr G)^{ab} \cong G^{ab} \times H^{ab}$$

where G^{ab} is the largest abelian factor group of G which means G/G' where G' is the commutator subgroup of G.

According to this fact, we have $([C_2]^n)^{ab} \cong (C_2)^n$. Thus the largest 2-Kummer extension of $\mathbb{Q}(\sqrt{d})$ within K_n has degree 2^n. Consider the natural map $\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^2 \to K_n^*/(K_n^*)^2$, the kernel of this map is

$$(\mathbb{Q}(\sqrt{d})^* \cap (K_n^*)^2)/(\mathbb{Q}(\sqrt{d})^*)^2 \cong \mathrm{Hom}(\mathrm{Gal}(K_n/\mathbb{Q}(\sqrt{d}), \{\pm 1\}) \cong \mathrm{Hom}((C_2)^n, \{\pm 1\}).$$

Since $|\mathrm{Hom}((C_2)^n, \{\pm 1\})| = 2^n$ so it has $\mathbb{F}_2$-dimension n.

Denoting the set of zeros of f^m by U_m, since f^m is even so $\alpha \in U_m$ implies $-\alpha \in U_m$. We have

$$c_m = f^m(0) = f^{m-1}(-c) = \prod_{\alpha \in U_{m-1}} (-c - \alpha) = \prod_{\alpha \in U_{m-1}} (-c + \alpha) \text{ for } m > 1$$

which is a square in K_m because for $\alpha \in U_{m-1}$, $\alpha - c$ is a square in K_m. Thus, all of $c_1, \cdots, c_n$ are squares in K_n. Since $c_1, \cdots, c_n$ are 2-independent over K, the above kernel must be generated by the residue classes of $c_1, \cdots, c_n$. Hence $c \in (K_n^*)^2$ if and only if the residue class of c in $(\mathbb{Q}(\sqrt{d})^* \cap (K_n^*)^2)/(\mathbb{Q}(\sqrt{d})^*)^2$ can be generated by $c_1, \cdots, c_n$ if and only if $c_1, \cdots, c_n, c$ are not 2-independent over K. □

Lemma 3.5 ([2, Lemma 1.6])**.** *For all n: $[K_{n+1} : K_n] = 2^{2^n} \Leftrightarrow c_{n+1}$ is not a square in K_n.*

Proof. The proof follows from M. Stoll's paper [2, Lemma 1.6]. □

In the following theorem, we denote the norm of K over $\mathbb{Q}$ by $N(\cdot)$ if no confusion will arise.

Theorem 1 (c.f. [2, Theorem])**.**

1. *For all n, the following statements are equivalent:*
   - *(a) $\Omega_n \cong [C_2]^n$*
   - *(b) $c_1, c_2, \cdots, c_n$ are 2-independent over K;*
   - *(c) $b_1, b_2, \cdots, b_n$ are 2-independent over K.*
2. *If none of $|N(b_2)|, |N(b_3)|, \cdots, |N(b_n)|$ is a square in $\mathbb{Q}$, then $\Omega_n \cong [C_2]^n$.*

Proof.

1. We use induction to prove this statement. For $k = 1$ is trivial, so suppose these statements hold for $k = n - 1$

   "(a) $\Longleftrightarrow$ (b)": By Lemma 3.3, we have

   $$\Omega_n \cong [C_2]^n \text{ if and only if } \Omega_{n-1} \cong [C_2]^{n-1} \text{ and } [K_n : K_{n-1}] = 2^{2^{n-1}}.$$

Use the induction hypothesis, we apply Lemma 3.5, then

$$\Omega_n \cong [C_2]^n \text{ if and only if } c_n \notin (K_{n-1}^*)^2.$$

By our induction hypothesis and Lemma 3.4, $c_n \notin (K_{n-1}^*)^2$ if and only if $c_1, \cdots, c_{n-1}, c_n$ are 2-independent over K if and only if $\Omega_n \cong [C_2]^n$.

"(b) $\iff$ (c)": Since $c_n = \prod_{d|n} b_d$, suppose $c_1, \cdots, c_n$ are not 2-independent over K then there exists $\{c_{i_1}, \cdots, c_{i_m}\} \subset \{c_1, \cdots, c_n\}$ where i_m is the largest index such that

$$c_{i_1} \cdots c_{i_m} = \kappa^2 \text{ where } \kappa \in K.$$

We can write the left-hand side as a product of $\{b_1, \cdots, b_n\}$. Because $b_{i_m} \mid \kappa^2$ and $b_{i_m}^2 \nmid c_{i_1} \cdots c_{i_m}$, thus such subset $\{b_1, \cdots, b_n\}$ which contains b_{i_m} is not 2-independent over K.

On the other hand, suppose $c_1, \cdots, c_n$ are 2-independent over K. Note that the residue class of c_i is equal to c_i^{-1} in $K^*/(K^*)^2$. Since $b_m = \prod_{d|m} c_d^{\mu(m/d)}$ so the residue class of b_m is equal to $\prod_{d|m} c_d$. But $\prod_{d|m} c_d \notin (K^*)^2$ by the hypothesis and $b_1, \cdots, b_n$ are pairwise coprime. Hence $\{b_1, \cdots, b_n\}$ is 2-independent over K.

2. Since $b_1, \cdots, b_n$ are pairwise coprime by Lemma 3.1, thus 1.(c) is equivalent to the following conditions:

$$\begin{cases} 1. \text{ None of } b_i \text{ is square in } K. \\ 2. \text{ There is at most one of } b_i \text{ multiply } \pm u \text{ is square in } K. \end{cases}$$

where u is a fundamental unit in $\mathcal{O}_K$. Note that

$$|N(b_i)| = |N(-b_i)| = |N(ub_i)| = |N(-ub_i)|.$$

Since none of $|N(b_i)|$ is a square in $\mathbb{Q}$ for $i = 2, \cdots, n$, so $\pm b_i$ and $\pm ub_i$ are not square in K for $i \geq 2$. Hence there must appear a new prime with odd power in b_i for $i \geq 2$. Moreover, we assume $b_1 = -c$ is not a square, thus $\{b_1, \cdots, b_n\}$ is 2-independent over K.

□

Remark. The second part of Theorem 3.1 is different from M. Stoll's Theorem [2, Theorem]. That's because the unit group in $\mathbb{Z}$ is $\{\pm 1\}$ but there are infinitely many units in a quadratic ring of integer. Hence, b_i and b_j might be both forms of square times a unit with odd power. Then b_i and b_j are coprime but $b_i b_j \in K^2$. Therefore, $|b_i| \notin K^2$ is not enough to show that $\{b_1, \cdots, b_n\}$ is 2-independent over K.

4 Iteration sequences associated to even integer polynomials

Let $g(X) \in \mathcal{O}_K[X^2]$ be an even polynomial whose constant term is ± 1. Put $\gamma_1 := g(0) = \pm 1$, and $\gamma_{n+1} := g(\gamma_n)$ for $n \geq 1$. Assume that all $\gamma_n \neq 0$ then set $\delta_n := \prod_{d|n} \gamma_d^{\mu(n/d)}$ for $n \geq 1$. We have

Lemma 4.1 (c.f [2, Lemma 2.1]). *Suppose that for all $n \geq 1$, there is a $m \in \mathcal{O}_K$, such that $m \mid \gamma_n + \gamma_{2n}$, m is prime to γ_n, and -1 is not a square mod m. Then for all $i \geq 2$, δ_i is not a square in K.*

Proof. For $n \geq 2$, $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where $r \geq 1$ and all $e_j \geq 1$. Set $n' := p_1 p_2 \cdots p_r > 1$ and $k := n/n'$. Put $\alpha := \gamma_{2k}$ and let $m \in \mathcal{O}_K$ such that $m \mid \gamma_k + \gamma_{2k}$, m is prime to γ_k and -1 is not a square mod m. We have m is prime to γ_{2k}, if not, then there exists a prime p such that $p \mid m$ and $p \mid \gamma_{2k}$. Since $\gamma_k + \gamma_{2k} = mx$ for some $x \in \mathcal{O}_K$ so $p \mid \gamma_k$, which is a contradiction.

Thus, $\alpha = \gamma_{2k} \equiv -\gamma_k \pmod{m}$ implies

$$\gamma_{3k} = g^k(\gamma_{2k}) \equiv g^k(-\gamma_k) = g^k(\gamma_k) = \gamma_{2k} = \alpha \pmod{m},$$

and by induction, $\gamma_{lk} \equiv \alpha \pmod{m}$ for all $l \geq 2$. Note that $\mu(kn'/d) \neq 0$ if and only if d is a multiple of k. Hence

$$\begin{aligned}\delta_n = \prod_{d|n} \gamma_d^{\mu(n/d)} &= \prod_{kt|kn'} \gamma_{kt}^{\mu(kn'/kt)} = \prod_{t|n'} \gamma_{kt}^{\mu(n'/t)} \\ &\equiv (-1)^{\mu(n')} \cdot \prod_{t|n'} \alpha^{\mu(n'/t)} \equiv (-1)^{\mu(n')} \alpha^{\sum_{t|n'} \mu(n'/t)} \equiv -1 \pmod{m}.\end{aligned}$$

Since -1 is not a square mod m, δ_n cannot be a square in K. □

Lemma 4.2. *Take $m = \gamma_k + \gamma_{k+1}$ in Lemma 4.1, then $m \mid \gamma_k + \gamma_{2k}$ and m is prime to γ_k for $k \geq 1$.*

Proof. Since $-\gamma_k \equiv \gamma_{k+1} \pmod{m}$ so

$$\gamma_{k+2} = g(\gamma_{k+1}) \equiv g(-\gamma_k) \equiv g(\gamma_k) = \gamma_{k+1} \pmod{m}.$$

Use induction on k, $\gamma_{2k} \equiv \gamma_{k+1} \equiv -\gamma_k \pmod{m}$. Hence $\gamma_k + \gamma_{2k} \equiv \gamma_k - \gamma_k \equiv 0 \pmod{m}$.

Since $\gamma_{k+1} = g(\gamma_k) \equiv g(0) = \pm 1 \pmod{\gamma_k}$ so γ_k is prime to γ_{k+1}. Hence m is prime to γ_k for all $k \geq 1$. □

5 Some values of c with $|b_i| \notin K^2$ for all $i \geq 2$

In this section, we deal with the following 3 cases,

1. $K = \mathbb{Q}(\sqrt{2})$;
2. $K = \mathbb{Q}(\sqrt{2p})$ where p is a prime and $p \equiv 3 \pmod 4$;
3. $K = \mathbb{Q}(\sqrt{p})$ where p is a prime and $p \equiv 1 \pmod 4$.

We have a fact that the class number of $\mathbb{Q}(\sqrt{2})$ is one. For the other two cases, we also need to assume $h_K = 1$.

Let $g(X) = |c|X^2 + \mathrm{sgn}(c)$ then $\gamma_1 = g(0) = \pm 1$. In addition, since $c_n = |c| \cdot \gamma_n$ for $n \geq 2$ and $c_n \neq 0$ so $\gamma_n \neq 0$ for all n. Hence we can define $\delta_n = \prod_{d|n} \gamma^{\mu(n/d)}$, moreover, $\delta_n = |b_n|$ for $n \geq 2$.

Remark. In H. Hasse's paper [9], he proved that if $K = \mathbb{Q}(\sqrt{d})$ is real and $h_K = 1$ then $d = p, 2q$ or qr, where p, q, r are primes and $q \equiv r \equiv 3 \pmod 4$. However, for the technical reason, we cannot apply a similar method on $K = \mathbb{Q}(\sqrt{p})$ where p is a prime and $p \equiv 3 \pmod 4$. The case which $d = qr$ where q, r are primes and $q \equiv r \equiv 3 \pmod 4$ is harder than the other two cases. Hence, we only deal with the above three cases.

5.1 Case 1: $K = \mathbb{Q}(\sqrt{2})$

In this subsection, since $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ so we write $c_n \in \mathcal{O}_K$ by $u_n + v_n\sqrt{2}$ and $\gamma_n \in \mathcal{O}_K$ by $\alpha_n + \beta_n\sqrt{2}$. Because K is fixed, we denote the norm of K over $\mathbb{Q}$ by $N(\cdot)$. Let $c = u + v\sqrt{2}$ with $N(c) > 0$ where u, v are odd positive integers. We have the following lemmas.

Lemma 5.1. *None of $c_1, \cdots, c_n$ is square in $\mathcal{O}_K$*

Proof. If $x + y\sqrt{2}$ is a square in $\mathcal{O}_K$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that

$$x + y\sqrt{2} = (\alpha + \beta\sqrt{2})^2 = (\alpha^2 + 2\beta^2) + 2\alpha\beta\sqrt{2},$$

thus y must be even.

Since $c_1 = -c = -u - v\sqrt{2} < 0$ so c_1 is not a square. For $n \geq 2$, we have

$$\begin{aligned} c_n &= c_{n-1}^2 + c \\ &= (u_{n-1} + v_{n-1}\sqrt{2})^2 + (u + v\sqrt{2}) \\ &= (u_{n-1}^2 + 2v_{n-1}^2 + u) + (2u_{n-1}v_{n-1} + v)\sqrt{2}. \end{aligned}$$

Since v is odd, so $2u_{n-1}v_{n-1} + v$ is odd, it follows that c_n is not a square in $\mathcal{O}_K$. □

Corollary. *All $f^n(X)$ are irreducible over $\mathcal{O}_K$.*

Proof. Apply Lemma 3.2 and 5.1, we get the result. □

Lemma 5.2. *For any $\gamma = \alpha + \beta\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,*

$$N(\gamma) = \alpha^2 - 2\beta^2 \equiv 7 \pmod 8 \Leftrightarrow \alpha, \beta \text{ are odd.}$$

Proof. Suppose α, β are odd then $\alpha^2 \equiv \beta^2 \equiv 1 \pmod 8$ and so $\alpha^2 - 2\beta^2 \equiv 7 \pmod 8$. Conversely, for any integer $n \in \mathbb{Z}$, $n^2 \equiv 0, 1, 4 \pmod 8$. Because we assume that $\alpha^2 - 2\beta^2 \equiv 7 \pmod 8$, the only possible of α, β are both odd. □

Lemma 5.3. *$N(\gamma_n + \gamma_{n+1}) > 0$ for all $n \in \mathbb{N}$.*

Proof. Note that for $n \geq 1$, we have

$$\begin{aligned}
\gamma_{n+1} &= c \cdot \gamma_n^2 + 1 \\
&= (u + v\sqrt{2})(\alpha_n + \beta_n\sqrt{2})^2 + 1 \\
&= (u + v\sqrt{2})(\Sigma_n + \Lambda_n\sqrt{2}) + 1 \text{ where } \Sigma_n = \alpha_n^2 + 2\beta_n^2 \quad \Lambda_n = 2\alpha_n\beta_n \\
&= (u\Sigma_n + 2v\Lambda_n + 1) + (u\Lambda_n + v\Sigma_n)\sqrt{2}.
\end{aligned}$$

Hence

$$\begin{cases} \alpha_{n+1} = u\Sigma_n + 2v\Lambda_n + 1, \\ \beta_{n+1} = u\Lambda_n + v\Sigma_n. \end{cases}$$

Since we assume u, v are positive, so it can deduce that α_n, β_n are both positive for all $n \geq 1$.

First, we will prove $N(\gamma_n) > 0$ for all $n \in \mathbb{N}$ by induction. Clearly, $N(\gamma_1) = 1 > 0$. Suppose $N(\gamma_n) > 0$, then

$$\begin{aligned}
N(\gamma_{n+1}) &= \alpha_{n+1}^2 - 2\beta_{n+1}^2 \\
&= (u\Sigma_n + 2v\Lambda_n + 1)^2 - 2(u\Lambda_n + v\Sigma_n)^2 \\
&= 2u\Sigma_n + 4v\Lambda_n + N(c)(\Sigma_n^2 - 2\Lambda_n^2) + 1 \\
&= 2u\Sigma_n + 4v\Lambda_n + N(c)(\alpha_n^2 - 2\beta_n^2)^2 + 1 \\
&= 2u\Sigma_n + 4v\Lambda_n + N(c)N(\gamma_n)^2 + 1 > 0,
\end{aligned}$$

since $u, v > 0$, so $\alpha_n, \beta_n > 0$ and $\Sigma_n, \Lambda_n \geq 0$ for all $n \in \mathbb{N}$.

Now, for any $n \in \mathbb{N}$,

$$\begin{aligned}
N(\gamma_n + \gamma_{n+1}) &= (\alpha_n + \alpha_{n+1})^2 - 2(\beta_n + \beta_{n+1})^2 \\
&= (\alpha_n^2 - 2\beta_n^2) + (\alpha_{n+1}^2 - 2\beta_{n+1}^2) + (2\alpha_n\alpha_{n+1} - 4\beta_n\beta_{n+1}) \\
&= N(\gamma_n) + N(\gamma_{n+1}) + (2\alpha_n\alpha_{n+1} - 4\beta_n\beta_{n+1}) > 0
\end{aligned}$$

The last term is nonnegative because we have proved that $N(\gamma_n) = \alpha_n^2 - 2\beta_n^2 > 0$ and $\alpha_n, \beta_n > 0$. Thus $\alpha_n > \sqrt{2}\beta_n$ for all $n \in \mathbb{N}$. □

Lemma 5.4. *If $c = u + v\sqrt{2}$ where u, v are odd, then $N(\gamma_n + \gamma_{n+1}) \equiv 7 \pmod 8$ for all $n \in \mathbb{N}$.*

Proof. For $n = 1$, we have

$$N(\gamma_1 + \gamma_2) = N(c + 2) = (u + 2)^2 - 2v^2 \equiv 7 \pmod 8.$$

If $n \geq 1$, then

$$\begin{cases} \alpha_{n+1} = u(\alpha_n^2 + 2\beta_n^2) + 4\alpha_n\beta_n v + 1 \equiv \alpha_n + 1 \pmod 2, \\ \beta_{n+1} = 2\alpha_n\beta_n u + v(\alpha_n^2 + 2\beta_n^2) \equiv \alpha_n \pmod 2. \end{cases}$$

Therefore, for $n \geq 2$, we have

$$\begin{cases} \alpha_n + \alpha_{n+1} \equiv \alpha_n + (\alpha_n + 1) \equiv 1 \pmod 2, \\ \beta_n + \beta_{n+1} \equiv \alpha_{n-1} + \alpha_n \equiv 1 \pmod 2. \end{cases}$$

Since $\gamma_n + \gamma_{n+1} = (\alpha_n + \alpha_{n+1}) + (\beta_n + \beta_{n+1})\sqrt{2}$, we have $N(\gamma_n + \gamma_{n+1}) \equiv 7 \pmod 8$, by Lemma 5.2. □

Theorem 2. *Let $m \in \mathbb{Z}[\sqrt{2}]$ satisfy $N(m) \equiv 7 \pmod 8$, and $N(m) > 0$, then -1 is not a square modulo m in $\mathbb{Z}[\sqrt{2}]$.*

Proof. Note that the only ramified prime in $\mathbb{Z}[\sqrt{2}]$ is 2. If p is an odd prime in $\mathbb{Z}$ and $p \equiv 3, 5 \pmod 8$ then p is inertial, so $N(p) = p^2 \equiv 1 \pmod 8$. Hence, if $m \in \mathbb{Z}[\sqrt{2}]$ with $N(m) \equiv 7 \pmod 8$ then there exists a split prime $\pi \in \mathbb{Z}[\sqrt{2}]$ such that $\pi \mid m$, $N(\pi)$ is a prime in $\mathbb{Z}$ and $N(\pi) \equiv 7 \pmod 8$.

Suppose -1 is a quadratic residue modulo m in $\mathbb{Z}[\sqrt{2}]$ then -1 also is a square in $\mathbb{Z}[\sqrt{2}]/(\pi)$ where (π) is the ideal in $\mathbb{Z}[\sqrt{2}]$ generated by π. Consider the natural map $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]/(\pi)$ which induces a map $\tilde{\varphi} : \mathbb{Z} \to \mathbb{Z}[\sqrt{2}]/(\pi)$. Thus, the kernel of $\tilde{\varphi}$ is $\mathbb{Z} \cap (\pi) = (N(\pi))$ which is the ideal in $\mathbb{Z}$ generated by $N(\pi)$. Hence we have

$$\mathbb{Z}[\sqrt{2}]/(\pi) \cong \mathbb{Z}/(N(\pi)) \cong \mathbb{F}_{N(\pi)}.$$

However, -1 is not a square in $\mathbb{F}_{N(\pi)}$ since $N(\pi) \equiv 3 \pmod 4$, which is absurd. Therefore -1 is not a square modulo m in $\mathbb{Z}[\sqrt{2}]$. □

Corollary. *If u, v are odd positive integers and $N(c) > 0$ then δ_n is not a square in $\mathbb{Q}(\sqrt{2})$ for $n \geq 2$.*

Proof. We can take $m = \gamma_n + \gamma_{n+1}$ in Lemma 4.1, then -1 is not a square modulo m. Hence by Lemma 4.1, δ_n is not a square in $\mathbb{Q}(\sqrt{2})$ for $n \geq 2$. □

5.2 Case 2: $K = \mathbb{Q}(\sqrt{2p})$ and $p \equiv 3 \pmod 4$

In this subsection, since $\mathcal{O}_K = \mathbb{Z}[\sqrt{2p}]$ so we write $c_n \in \mathcal{O}_K$ by $u_n + v_n\sqrt{2p}$ and $\gamma_n \in \mathcal{O}_K$ by $\alpha_n + \beta_n\sqrt{2p}$. Because K is fixed, we denote the norm of K over $\mathbb{Q}$ by $N(\cdot)$. Let $c = u + v\sqrt{2p}$ with $N(c) > 0$ where u, v are positive integers, $u \equiv -1 \pmod{2p}$ and $v \equiv 1 \pmod 2$. We have the following lemmas.

Lemma 5.5. *None of $c_1, \cdots, c_n$ is a square in $\mathcal{O}_K$*

Proof. If $x + y\sqrt{2p}$ is a square in $\mathcal{O}_K$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that

$$x + y\sqrt{2p} = (\alpha + \beta\sqrt{2p})^2 = (\alpha^2 + 2p\beta^2) + 2\alpha\beta\sqrt{2p},$$

thus y must be even.

Since $c_1 = -c = -u - v\sqrt{2p}$ and v is odd so c_1 is not a square. For $n \geq 2$, we have

$$\begin{aligned} c_n &= c_{n-1}^2 + c \\ &= (u_{n-1}^2 + 2pv_{n-1}^2 + u) + (2u_{n-1}v_{n-1} + v)\sqrt{2p} \end{aligned}$$

since v is odd so $2u_{n-1}v_{n-1} + v$ is odd and c_n is not a square in $\mathcal{O}_K$. □

Corollary. *All $f^n(X)$ are irreducible over $\mathcal{O}_K$.*

Proof. By Lemma 3.2 and 5.5, we get the result. □

Lemma 5.6. *For any $\gamma = \alpha + \beta\sqrt{2p} \in \mathbb{Z}[\sqrt{2p}]$, If $\alpha \equiv \pm 1 \pmod{2p}$ and $\beta \equiv 1 \pmod 2$ then $N(\gamma) \equiv 6p + 1 \pmod{8p}$.*

Proof. Suppose $\alpha = 2pk \pm 1$ and $\beta = 2l + 1$ where $k, l \in \mathbb{Z}$ then

$$\begin{aligned} N(\gamma) &= \alpha^2 - 2p\beta^2 \\ &= (4p^2k^2 \pm 4pk + 1) - 2p(4l^2 + 4l + 1) \\ &\equiv 4pk(pk \pm 1) + 1 - 2p \pmod{8p} \\ &\equiv 1 - 2p \pmod{8p} \quad \text{since one of } pk, pk \pm 1 \text{ is even.} \\ &\equiv 6p + 1 \pmod{8p} \end{aligned}$$

□

Lemma 5.7. *$N(\gamma_n + \gamma_{n+1}) > 0$ for all $n \in \mathbb{N}$.*

Proof. Note that for $n \geq 1$, if $\gamma_n = \alpha_n + \beta_n\sqrt{2p}$ then

$$\begin{aligned} \gamma_{n+1} &= c \cdot \gamma_n^2 + 1 \\ &= (u + v\sqrt{2p})(\alpha_n + \beta_n\sqrt{2p})^2 + 1 \\ &= (u + v\sqrt{2p})(\Sigma_n + \Lambda_n\sqrt{2p}) + 1 \text{ where } \Sigma_n = \alpha_n^2 + 2p\beta_n^2 \quad \Lambda_n = 2\alpha_n\beta_n \\ &= (u\Sigma_n + 2pv\Lambda_n + 1) + (u\Lambda_n + v\Sigma_n)\sqrt{2p}. \end{aligned}$$

Hence

$$\begin{cases} \alpha_{n+1} = u\Sigma_n + 2pv\Lambda_n + 1, \\ \beta_{n+1} = u\Lambda_n + v\Sigma_n. \end{cases}$$

Clearly, since $u, v > 0$, so $\alpha_n, \beta_n > 0$ and $\Sigma_n, \Lambda_n \geq 0$ for all $n \in \mathbb{N}$.

First, we will prove $N(\gamma_n) > 0$ for all $n \in \mathbb{N}$ by induction. Clearly, $N(\gamma_1) = 1 > 0$. Suppose $N(\gamma_n) > 0$, then

$$\begin{aligned} N(\gamma_{n+1}) &= \alpha_{n+1}^2 - 2p\beta_{n+1}^2 \\ &= (u\Sigma_n + 2pv\Lambda_n + 1)^2 - 2p(u\Lambda_n + v\Sigma_n)^2 \\ &= 2u\Sigma_n + 4pv\Lambda_n + N(c)(\Sigma_n^2 - 2p\Lambda_n^2) + 1 \\ &= 2u\Sigma_n + 4pv\Lambda_n + N(c)(\alpha_n^2 - 2p\beta_n^2)^2 + 1 \\ &= 2u\Sigma_n + 4pv\Lambda_n + N(c)N(\gamma_n)^2 + 1 > 0 \end{aligned}$$

Now, for any $n \in \mathbb{N}$,

$$\begin{aligned} N(\gamma_n + \gamma_{n+1}) &= (\alpha_n + \alpha_{n+1})^2 - 2p(\beta_n + \beta_{n+1})^2 \\ &= (\alpha_n^2 - 2p\beta_n^2) + (\alpha_{n+1}^2 - 2p\beta_{n+1}^2) + (2\alpha_n\alpha_{n+1} - 4p\beta_n\beta_{n+1}) \\ &= N(\gamma_n) + N(\gamma_{n+1}) + (2\alpha_n\alpha_{n+1} - 4p\beta_n\beta_{n+1}) > 0 \end{aligned}$$

The last term is nonnegative because $\alpha_n \geq \sqrt{2p}\beta_n$ for all $n \in \mathbb{N}$. □

Lemma 5.8. *If $c = u + v\sqrt{2p}$ where $u \equiv -1 \pmod{2p}$, and $v \equiv 1 \pmod 2$ then $N(\gamma_n + \gamma_{n+1}) \equiv 6p + 1 \pmod{8p}$.*

Proof. Note that, for $n \geq 1$

$$\begin{cases} \alpha_{n+1} = u(\alpha_n^2 + 2p\beta_n^2) + 4vp\alpha_n\beta_n + 1 \equiv -\alpha_n^2 + 1 \pmod{2p} \\ \beta_{n+1} = 2u\alpha_n\beta_n + v(\alpha_n^2 + 2p\beta_n^2) \equiv \alpha_n \pmod 2. \end{cases}$$

Since $\gamma_1 = g(0) = 1$ so

$$\alpha_1 \equiv 1 \pmod{2p} \text{ and } \beta_1 \equiv 0 \pmod 2.$$

For $n = 2$, we have

$$\alpha_2 \equiv -\alpha_1^2 + 1 \equiv 0 \pmod{2p} \text{ and } \beta_2 \equiv \alpha_1 \equiv 1 \pmod 2.$$

As $n = 3$,

$$\alpha_3 \equiv -\alpha_2^2 + 1 \equiv 1 \equiv \alpha_1 \pmod{2p} \text{ and } \beta_3 \equiv \alpha_2 \equiv 0 \equiv \alpha_1 \pmod 2.$$

Thus

$$\begin{cases} \alpha_n \equiv 1 \pmod{2p} \\ \beta_n \equiv 0 \pmod 2 \end{cases} \text{ for } n \text{ is odd, and } \begin{cases} \alpha_n \equiv 0 \pmod{2p} \\ \beta_n \equiv 1 \pmod 2 \end{cases} \text{ for } n \text{ is even.}$$

Hence $\alpha_n + \alpha_{n+1} \equiv 1 \pmod{2p}$ and $\beta_n + \beta_{n+1} \equiv 1 \pmod 2$ for any $n \in \mathbb{N}$. Therefore, $N(\gamma_n + \gamma_{n+1}) \equiv 6p + 1 \pmod{8p}$ by Lemma 5.6. □

Theorem 3. *Let $m \in \mathbb{Z}[\sqrt{2p}]$ satisfy $N(m) \equiv 6p+1 \pmod{8p}$, and $N(m) \geq 0$, then -1 is not quadratic residue modulo m in $\mathbb{Z}[\sqrt{2p}]$.*

Proof. Note that the discriminant of $\mathbb{Z}[\sqrt{2p}]$ is $8p$ so the only ramified primes are $2, p$. But $N(m) \equiv 6p+1 \pmod{8p}$ thus $p \nmid N(m)$ and $2 \nmid N(m)$. Thus, all prime factors of m are split or inertial. Since our $\mathbb{Z}[\sqrt{2p}]$ is a unique factorization domain, so for any $m \in \mathbb{Z}[\sqrt{2p}]$ we can factor m in some primes $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k} \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_l^{b_l}$ where $\mathfrak{p}_i$ are inertial and $\mathfrak{q}_j$ are split. Note that $N(\mathfrak{p}_i)$ is a square of prime, so $N(\mathfrak{p}_i) \equiv 1 \pmod{4}$. Hence, if all prime factors of m are inertial then $N(m) \equiv 1 \pmod{4}$ which is a contradiction. So $l \geq 2$, that means there exists a split prime $\mathfrak{q}_1$ divides m such that $N(\mathfrak{q}_1) \equiv 3 \pmod{4}$.

Suppose -1 is a quadratic residue modulo m in $\mathcal{O}_K$ then -1 also is a square in $\mathbb{Z}[\sqrt{2p}]/(\mathfrak{q}_j)$ where $(\mathfrak{q}_j)$ is the ideal in $\mathbb{Z}[\sqrt{2p}]$ which generated by $\mathfrak{q}_j$. Consider the natural map $\varphi : \mathbb{Z}[\sqrt{2p}] \to \mathbb{Z}[\sqrt{2p}]/(\mathfrak{q}_j)$ which induces a map $\tilde{\varphi} : \mathbb{Z} \to \mathbb{Z}[\sqrt{2p}]/(\mathfrak{q}_j)$. Thus, the kernel of $\tilde{\varphi}$ is $\mathbb{Z} \cap (\mathfrak{q}_j) = (N(\mathfrak{q}_j))$ which is the ideal in $\mathbb{Z}$ generated by $N(\mathfrak{q}_j)$. Hence we have

$$\mathbb{Z}[\sqrt{2p}]/(\mathfrak{q}_j) \cong \mathbb{Z}/(N(\mathfrak{q}_j)) \cong \mathbb{F}_{N(\mathfrak{q}_j)}.$$

However, -1 is not a square in $\mathbb{F}_{N(\mathfrak{q}_j)}$ since $N(\mathfrak{q}_j) \equiv 3 \pmod{4}$, which is absurd. Therefore -1 is not a square modulo m in $\mathbb{Z}[\sqrt{2p}]$. □

Corollary. *If $u \equiv 1 \pmod{2p}$, and $v \equiv 1 \pmod{2}$ and $N(c) > 0$ then δ_n is not a square in $\mathbb{Q}(\sqrt{2p})$ for $n \geq 2$.*

Proof. We can take $m = \gamma_k + \gamma_{k+1}$ in Lemma 4.1, then -1 is not a square modulo m. Hence by Lemma 4.1, δ_n is not a square in $\mathbb{Q}(\sqrt{2p})$ for $n \geq 2$. □

5.3 Case 3: $K = \mathbb{Q}(\sqrt{p})$ and $p \equiv 1 \pmod{4}$

In this subsection, since $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$ so we write $c_n \in \mathcal{O}_K$ by $u_n + v_n\left(\frac{1+\sqrt{p}}{2}\right)$ and $\gamma_n \in \mathcal{O}_K$ by $\alpha_n + \beta_n\left(\frac{1+\sqrt{p}}{2}\right)$. Because K is fixed, we denote the norm function of K over $\mathbb{Q}$ by $N(\cdot)$. Let $c = u + v\left(\frac{1+\sqrt{p}}{2}\right)$ with $N(c) > 0$ where u, v are positive integers, $u \equiv -1 \pmod{4p}$ and $v \equiv 2p \pmod{4p}$. Note that since $p \equiv 1 \pmod{4}$ so $p = 4k+1$ for some $k \in \mathbb{Z}$. We have the following lemmas.

Lemma 5.9. *None of $c_1, \cdots, c_n$ is square in $\mathcal{O}_K$*

Proof. If $x + y\left(\frac{1+\sqrt{p}}{2}\right)$ is a square in $\mathcal{O}_K$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that

$$x + y\left(\frac{1+\sqrt{p}}{2}\right) = \left(\alpha + \beta\left(\frac{1+\sqrt{p}}{2}\right)\right)^2 = (\alpha^2 + k\beta^2) + (2\alpha\beta + \beta^2)\left(\frac{1+\sqrt{p}}{2}\right).$$

If β is even then $2\alpha\beta + \beta^2 \equiv 0 \pmod{4}$, if β is odd then $2\alpha\beta + \beta^2 \equiv 1$ or $3 \pmod{4}$.

Since $c_1 = -c = -u - v\left(\frac{1+\sqrt{p}}{2}\right)$ and $v \equiv 2p \pmod{4p}$ so $v \equiv 2 \pmod 4$ and so c_1 is not a square. For $n \geq 2$, suppose $v_{n-1} \equiv 2 \pmod 4$ and use induction, we have

$$\begin{aligned} c_n &= c_{n-1}^2 + c \\ &= \left(u_{n-1} + v_{n-1}\left(\frac{1+\sqrt{p}}{2}\right)\right)^2 + \left(u + v\left(\frac{1+\sqrt{p}}{2}\right)\right) \\ &= (u_{n-1}^2 + kv_{n-1}^2 + u) + (2u_{n-1}v_{n-1} + v_{n-1}^2 + v)\left(\frac{1+\sqrt{p}}{2}\right) \end{aligned}$$

and $2u_{n-1}v_{n-1} + v_{n-1}^2 + v \equiv 2 \pmod 4$ so c_n is not a square in $\mathcal{O}_K$. □

Corollary. *All $f^n(X)$ are irreducible over $\mathcal{O}_K$.*

Proof. By Lemma 3.2 and Lemma 5.9, we get the result. □

Lemma 5.10. *Let $c = u + v\left(\frac{1+\sqrt{p}}{2}\right)$ where $u, v \in \mathbb{Z}$. If $u \equiv \pm 1 \pmod{4p}$ and $v \equiv 2p \pmod{4p}$ then $N(c) \equiv 2p + 1 \pmod{4p}$.*

Proof. Note that

$$\begin{aligned} N(c) &= \left(u + v\left(\frac{1+\sqrt{p}}{2}\right)\right)\left(u + v\left(\frac{1-\sqrt{p}}{2}\right)\right) \\ &= \left(u + \frac{v}{2}\right)^2 - \frac{v^2 p}{4} \\ &= u^2 + uv + \frac{v^2}{4} - \frac{v^2 p}{4} \\ &= u^2 + uv - kv^2 \end{aligned}$$

Suppose $u = 4pm \pm 1$ and $v = 4pn + 2p$ where $m, n \in \mathbb{Z}$ then

$$\begin{aligned} N(c) &= u^2 + uv - kv^2 \\ &= (4pm \pm 1)^2 + (4pm \pm 1)(4pn + 2p) - k(4pn + 2p)^2 \\ &\equiv 1 + 2p \pmod{4p} \end{aligned}$$

□

Lemma 5.11. *Let $c = u + v\left(\frac{1+\sqrt{p}}{2}\right)$ where $u, v \in \mathbb{Z}$. If $u \equiv -1 \pmod{4p}$ and $v \equiv 2p \pmod{4p}$ then $N(\gamma_n + \gamma_{n+1}) \equiv 2p + 1 \pmod{4p}$.*

Proof. Note that for $n \geq 1$, if $\gamma_n = \alpha_n + \beta_n \left(\frac{1+\sqrt{p}}{2}\right)$ then

$$\begin{aligned}
\gamma_{n+1} &= c \cdot \gamma_n^2 + 1 \\
&= \left(u + v\left(\frac{1+\sqrt{p}}{2}\right)\right)\left(\alpha_n + \beta_n\left(\frac{1+\sqrt{p}}{2}\right)\right)^2 + 1 \\
&= \left(u + v\left(\frac{1+\sqrt{p}}{2}\right)\right)\left(\Sigma_n + \Lambda_n\left(\frac{1+\sqrt{p}}{2}\right)\right) + 1 \\
&= (u\Sigma_n + vk\Lambda_n + 1) + (u\Lambda_n + v\Sigma_n + v\Lambda_n)\left(\frac{1+\sqrt{p}}{2}\right),
\end{aligned}$$

where $\Sigma_n = \alpha_n^2 + k\beta_n^2$ and $\Lambda_n = 2\alpha_n\beta_n + \beta_n^2$. Thus

$$\begin{cases} \alpha_{n+1} = u(\alpha_n^2 + k\beta_n^2) + vk(2\alpha_n\beta_n + \beta_n^2) + 1 \\ \beta_{n+1} = (u+v)(2\alpha_n\beta_n + \beta_n^2) + v(\alpha_n^2 + k\beta_n^2). \end{cases}$$

Since $\gamma_1 = g(0) = 1$, so

$$\alpha_1 \equiv 1 \pmod{4p} \text{ and } \beta_1 \equiv 0 \pmod{4p}.$$

For $n = 2$, we have $\gamma_2 = (u+1) + v\left(\frac{1+\sqrt{p}}{2}\right) = \alpha_2 + \beta_2\left(\frac{1+\sqrt{p}}{2}\right)$, so

$$\begin{cases} \alpha_2 = u(\alpha_1^2 + k\beta_1^2) + vk(2\alpha_1\beta_1 + \beta_1^2) + 1 \equiv u + 1 \equiv 0 \pmod{4p} \\ \beta_2 = (u+v)(2\alpha_1\beta_1 + \beta_1^2) + v(\alpha_1^2 + k\beta_1^2) \equiv v \equiv 2p \pmod{4p}. \end{cases}$$

For $n = 3$, we have

$$\begin{cases} \alpha_3 = u(\alpha_2^2 + k\beta_2^2) + vk(2\alpha_2\beta_2 + \beta_2^2) + 1 \equiv 1 \equiv \alpha_1 \pmod{4p} \\ \beta_3 = (u+v)(2\alpha_2\beta_2 + \beta_2^2) + v(\alpha_2^2 + k\beta_2^2) \equiv 0 \equiv \beta_1 \pmod{4p}. \end{cases}$$

Thus

$$\begin{cases} \alpha_n \equiv 1 \pmod{4p} \\ \beta_n \equiv 0 \pmod{4p} \end{cases} \text{ for } n \text{ is odd, and } \begin{cases} \alpha_n \equiv 0 \pmod{4p} \\ \beta_n \equiv 2p \pmod{4p} \end{cases} \text{ for } n \text{ is even.}$$

Hence $\alpha_n + \alpha_{n+1} \equiv 1 \pmod{4p}$ and $\beta_n + \beta_{n+1} \equiv 2p \pmod{4p}$ for any $n \in \mathbb{N}$. Therefore, $N(\gamma_n + \gamma_{n+1}) \equiv 2p + 1 \pmod{4p}$ by Lemma 5.10. □

Lemma 5.12. *If $u, v > 0$ then $\alpha_n, \beta_n \geq 0$ for all $n \geq 1$.*

Proof. Since $\gamma_1 = 1$ so $\alpha_1 \geq 0$ and $\beta_1 \geq 0$. Assume it is hold for $n = m$, then consider $n = m + 1$, we have

$$\begin{cases} \alpha_{m+1} = u(\alpha_m^2 + k\beta_m^2) + vk(2\alpha_m\beta_m + \beta_m^2) + 1 \\ \beta_{m+1} = (u+v)(2\alpha_m\beta_m + \beta_m^2) + v(\alpha_m^2 + k\beta_m^2). \end{cases}$$

Since $k = (p-1)/4$ so k is bigger than 0 and $\alpha_m, \beta_m \geq 0$. By induction, we have $\alpha_n, \beta_n \geq 0$ for all $n \in \mathbb{N}$. □

Lemma 5.13. *If $N(c) > 0, u, v > 0$, then $N(\gamma_n + \gamma_{n+1}) > 0$ for all $n \in \mathbb{N}$.*

Proof. We will prove $N(\gamma_n) > 0$ for all $n \in \mathbb{Z}$ by induction. Note that since $u, v \geq 0$ so $\alpha_n, \beta_n \geq 0$ for all $n \in \mathbb{N}$, thus $\Sigma_n, \Lambda_n \geq 0$ for all $n \geq 1$.

$$\begin{aligned}\Sigma_n^2 + \Sigma_n\Lambda_n - k\Lambda_n^2 &= (\alpha_n^2 + k\beta_n^2)^2 + (\alpha_n^2 + k\beta_n^2)(2\alpha_n\beta_n + \beta_n^2) - k(2\alpha_n\beta_n + \beta_n^2)^2 \\ &= \alpha_n^4 - 2k\alpha_n^2\beta_n^2 + k^2\beta_n^4 + 2\alpha_n^3\beta_n + \alpha_n^2\beta_n^2 - 2k\alpha_n\beta_n^3 \\ &= (\alpha_n^2 + \alpha_n\beta_n - k\beta_n^2)^2 = N(\gamma_n)^2.\end{aligned}$$

$N(\gamma_1) = N(1) > 0$ and Suppose $N(\gamma_n) > 0$, then

$$\begin{aligned}N(\gamma_{n+1}) &= \alpha_{n+1}^2 + \alpha_{n+1}\beta_{n+1} - k\beta_{n+1}^2 \\ &= (u\Sigma_n + vk\Lambda_n + 1)^2 + (u\Sigma_n + vk\Lambda_n + 1)(u\Lambda_n + v\Sigma_n + v\Lambda_n) - k(u\Lambda_n + v\Sigma_n + v\Lambda_n)^2 \\ &= (\Sigma_n^2 + \Sigma_n\Lambda_n - k\Lambda_n^2)N(c) + 2u\Sigma_n + v\Sigma_n + u\Lambda_n + v\Lambda_n + 2vk\Lambda_n + 1 \\ &= N(\gamma_n)^2N(c) + 2u\Sigma_n + v\Sigma_n + u\Lambda_n + v\Lambda_n + 2vk\Lambda_n + 1 > 0.\end{aligned}$$

By induction, $N(\gamma_{n+1}) > 0$ for all $n \in \mathbb{N}$.

Because

$$\begin{aligned}N(\gamma_n + \gamma_{n+1}) &= (\alpha_n + \alpha_{n+1})^2 + (\alpha_n + \alpha_{n+1})(\beta_n + \beta_{n+1}) - k(\beta_n + \beta_{n+1})^2 \\ &= N(\gamma_n) + N(\gamma_{n+1}) + \alpha_n\beta_{n+1} + \alpha_{n+1}\beta_n + 2\alpha_n\alpha_{n+1} - 2k\beta_n\beta_{n+1},\end{aligned}$$

if we can prove $\alpha_n\beta_{n+1} + \alpha_{n+1}\beta_n + 2\alpha_n\alpha_{n+1} - 2k\beta_n\beta_{n+1} \geq 0$ then $N(\gamma_n + \gamma_{n+1}) > 0$. Note that $N(\gamma_n) > 0$ so we have

$$N(\gamma_n) = \alpha_n^2 + \alpha_n\beta_n - k\beta_n^2 > 0,$$

thus $\alpha_n(\alpha_n + \beta_n) > k\beta_n^2$ for all $n \in \mathbb{N}$. Since $\alpha_n, \beta_n \geq 0$ for all n so

$$\begin{aligned}\alpha_n\beta_{n+1} + \alpha_{n+1}\beta_n + 2\alpha_n\alpha_{n+1} &= \alpha_n(\alpha_{n+1} + \beta_{n+1}) + \alpha_{n+1}(\alpha_n + \beta_n) \\ &\geq 2\sqrt{\alpha_n\alpha_{n+1}(\alpha_n + \beta_n)(\alpha_{n+1} + \beta_{n+1})} \\ &> 2\sqrt{k^2\beta_n^2\beta_{n+1}^2} \\ &= 2k\beta_n\beta_{n+1}\end{aligned}$$

Hence $N(\gamma_n + \gamma_{n+1}) \geq 0$ for all $n > 1$. □

Theorem 4. *Let $m \in \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right] = \mathcal{O}_K$ satisfy $N(m) \equiv 2p + 1 \pmod{4p}$, and $N(m) > 0$, then -1 is not quadratic residue modulo m in $\mathcal{O}_K$.*

Proof. Note that the discriminant of $\mathcal{O}_K$ is p so the only ramified primes are p. But $N(m) \equiv 2p + 1 \pmod{4p}$ thus $p \nmid N(m)$, moreover, $N(m) \equiv 3 \pmod 4$. Hence all prime factors of m is split or inertial. Moreover, if $\mathfrak{p}$ is inertial then $N(\mathfrak{p})$ is a square of a rational prime and $N(\mathfrak{p}) \equiv 1 \pmod 4$. Hence if all prime factor of m are inertial then $N(m) \equiv 1 \pmod 4$ which is a contradiction. so there exists a split prime divides m.

Since our $\mathcal{O}_K$ is a unique factorization domain so for any $m \in \mathcal{O}_K$ we can factor m in some primes $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k} \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_l^{b_l}$ where $\mathfrak{p}_i$ are inertial and $\mathfrak{q}_j$ are split. Note that $N(\mathfrak{p}_i)$ is a square of prime, so $N(\mathfrak{p}_i) \equiv 1 \pmod 4$. Hence there exists at least one $\mathfrak{q}_j$ such that $N(\mathfrak{q}_j) \equiv 3 \pmod 4$ where $N(\mathfrak{q}_j)$ is a rational prime.

Suppose -1 is a quadratic residue modulo m in $\mathcal{O}_K$ then -1 also is a square in $\mathcal{O}_K/(\mathfrak{q}_\mathfrak{j})$ where $(\mathfrak{q}_\mathfrak{j})$ is the ideal in $\mathcal{O}_K$ which generated by $\mathfrak{q}_\mathfrak{j}$. Consider the natural map $\varphi : \mathcal{O}_K \to \mathcal{O}_K/(\mathfrak{q}_\mathfrak{j})$ which induces a map $\tilde{\varphi} : \mathbb{Z} \to \mathcal{O}_K/(\mathfrak{q}_\mathfrak{j})$. Thus, the kernel of $\tilde{\varphi}$ is $\mathbb{Z} \cap (\mathfrak{q}_\mathfrak{j}) = (N(\mathfrak{q}_\mathfrak{j}))$ which is the ideal in $\mathbb{Z}$ generated by $N(\mathfrak{q}_\mathfrak{j})$. Hence we have

$$\mathcal{O}_K/(\mathfrak{q}_\mathfrak{j}) \cong \mathbb{Z}/(N(\mathfrak{q}_\mathfrak{j})) \cong \mathbb{F}_{N(\mathfrak{q}_\mathfrak{j})}.$$

However, -1 is not a square in $\mathbb{F}_{N(\mathfrak{q}_\mathfrak{j})}$ since $N(\mathfrak{q}_\mathfrak{j}) \equiv 3 \pmod 4$, which is absurd. Therefore -1 is not a square modulo m in $\mathcal{O}_K$. □

Corollary. *If $u \equiv -1 \pmod{4p}$, and $v \equiv 2p \pmod{4p}$ and $N(c) > 0$ then δ_n is not a square in $\mathbb{Q}(\sqrt{p})$ for $n \geq 2$.*

Proof. We can take $m = \gamma_k + \gamma_{k+1}$ in Lemma 4.1, then -1 is not a square modulo m. Hence by Lemma 4.1, δ_n is not a square in $\mathbb{Q}(\sqrt{p})$ for $n \geq 2$. □

6 $\Omega_n \cong [C_2]^n$ for $K = \mathbb{Q}(\sqrt{2})$

Note that if $c = u + v\sqrt{2}$ is a square in $\mathbb{Z}[\sqrt{2}]$ then v must be even. However, we consider $c = u + v\sqrt{2}$ where u, v are odd positive integers, so none of

$$b_1 = -c, \quad b_2 = -(c+1), \quad b_1 b_2 = c^2 + c$$

is a square. In this section, we will prove that there must appear a new prime with odd power in b_i for $i > 2$, thus $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}(\sqrt{2})$.

Since $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain, b_i can be unique factored into products of units and primes as following:

$$b_i = \pm u^e p_1^{r_1} \cdots p_k^{r_k}$$

where $u = 1 + \sqrt{2}$ is a fundamental unit in $\mathbb{Z}[\sqrt{2}]$.

By the corollary to Theorem 5.1, at least one of $e, r_1, \cdots, r_k$ must be odd. We will prove, for $i \geq 3$, there does not exist the case which e is odd and $r_1, \cdots, r_k$ are even, that means $b_i = \pm u (b_i')^2$ where $b_i' \in \mathbb{Z}[\sqrt{2}]$. Hence, there appears a new prime with odd power in b_i for $i \geq 3$ and so $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}(\sqrt{2})$ for $n \geq 1$.

We define some notations as follows: for $\gamma = \alpha + \beta\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, let $[\gamma]_2$ be the residue class of γ in $\mathbb{Z}[\sqrt{2}]/(2)$ and $[\gamma]_4$ be the residue class of γ in $\mathbb{Z}[\sqrt{2}]/(4)$. Moreover, we also denote

$$[\gamma]_2 \coloneqq [\alpha \bmod 2, \beta \bmod 2]_2 \text{ and } [\gamma]_4 \coloneqq [\alpha \bmod 4, \beta \bmod 4]_4.$$

For example, if $\gamma = 10 + 23\sqrt{2}$ then $[\gamma]_2 = [0,1]_2$ and $[\gamma]_4 = [2,3]$.

For any $\gamma = \alpha + \beta\sqrt{2}, \gamma' = \alpha' + \beta'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, we define

$$[\gamma]_4 * [\gamma']_4 \coloneqq [\gamma\gamma']_4 = [\alpha\alpha' + 2\beta\beta' \bmod 4, \alpha\beta' + \alpha'\beta \bmod 4]_4$$

and

$$[\gamma]_2 * [\gamma']_2 \coloneqq [\gamma\gamma']_2 = [\alpha\alpha' \bmod 2, \alpha\beta' + \alpha'\beta \bmod 2]_2.$$

First, we observe the following result:

Lemma 6.1. *If $\gamma = \pm u(\gamma')^2$ where $\gamma' \in \mathbb{Z}[\sqrt{2}]$ then $[\gamma]_4 \in \{[0,0]_4, [2,2]_4, \pm[1,1]_4, \pm[3,1]_4\}$.*

Proof. Suppose $\gamma' = x + y\sqrt{2}$ then

$$\begin{aligned}\gamma &= \pm(1+\sqrt{2})(x+y\sqrt{2})^2 \\ &= \pm(1+\sqrt{2})(x^2+2y^2+2xy\sqrt{2}) \\ &= \pm((x^2+2y^2+4xy) + (x^2+2y^2+2xy)\sqrt{2}).\end{aligned}$$

Hence

$$[\gamma]_4 = \begin{cases} [0,0]_4 & \text{if } x, y \text{ are even,} \\ \pm[3,1]_4 & \text{if } x, y \text{ are odd,} \\ [2,2]_4 & \text{if } x \text{ is even and } y \text{ is odd,} \\ \pm[1,1]_4 & \text{if } x \text{ is odd and } y \text{ is even.} \end{cases}$$

□

Next, since $c = u+v\sqrt{2}$ where u, v are odd positive integers, so $[c]_4 \in \{[1.1]_4, [1,3]_4, [3,1]_4, [3,3]_4\}$, and we want to compute $[c_n]_4$ for all $n \geq 1$.

Proposition. *If $[c]_4 = [a,b]_4 \in \{[1.1]_4, [1,3]_4, [3,1]_4, [3,3]_4\}$ then $[c_1]_4 = [-a,-b]_4$. Moreover,*

$$[c_n]_4 = \begin{cases} [a+3, b+2]_4 & \textit{if } n \textit{ is even,} \\ [a+2, b]_4 & \textit{if } n \textit{ is odd and } n \geq 3. \end{cases}$$

Proof. Obviously, since $c_1 = -c$ so $[c_1]_4 = [-a,-b]_4$. Note that a, b are odd so

$$a^2 \equiv b^2 \equiv 1 \pmod 4 \text{ and } 2ab \equiv 2 \pmod 4.$$

Since $[c_1]_4 = [-a,-b]_4$ and $c_n = c_{n-1}^2 + c$ for $n \geq 2$ so

$$\begin{aligned}[c_2]_4 &= [-a,-b]_4 * [-a,-b]_4 + [a,b]_4 \\ &= [a^2+2b^2, 2ab]_4 + [a,b]_4 \\ &= [a^2+2b^2+a, 2ab+b]_4 \\ &= [a+3, b+2]_4,\end{aligned}$$

and

$$\begin{aligned}[c_3]_4 &= [a+3, b+2]_4 * [a+3, b+2]_4 + [a, b]_4 \\ &= [(a+3)^2 + 2(b+2)^2 + a, 2(a+3)(b+2) + b]_4 \\ &= [2(b+2)^2 + a, b]_4 \\ &= [a+2, b]_4\end{aligned}$$

because $a+3$ is even and $b+2$ is odd. Moreover, since

$$\begin{aligned}[c_4]_4 &= [a+2, b]_4 * [a+2, b]_4 + [a, b]_4 \\ &= [(a+2)^2 + 2b^2 + a, 2(a+2)b + b]_4 \\ &= [a+3, b+2]_4 \\ &= [c_2]_4,\end{aligned}$$

thus $[c_n]_4 = [a+2, b]_4$ for any odd integer $n \geq 3$, and $[c_n]_4 = [a+3, b+2]_4$ for all even n. □

By Lemma 6.1, if we can prove that $[b_i]_4 \notin \{[0,0]_4, [2,2]_4, \pm[1,1]_4, \pm[3,1]_4\}$ for $i \geq 3$, then there must appear a new prime with odd power in b_i. Since $b_1 = -c$ and $b_2 = -(c+1)$ so $[b_1]_2 = [1,1]_2$ and $[b_2]_2 = [0,1]_2$ for any case of c. Moreover, we have

Lemma 6.2. *$[b_i]_2 \neq [0,0]_2, [0,1]_2$ for $i \geq 3$.*

Proof. Note that, for any $[a,b]_2$ where $a, b \in \{0,1\}$, $[a,b]_2 * [0,0]_2 = [0,0]_2$ and $[a,b]_2 * [0,1]_2 = [0,0]_2$ or $[0,1]_2$. Suppose $[b_n]_2 = [0,0]_2$ or $[0,1]_2$ for some $n \geq 3$, note that

$$c_n = \prod_{d|n} b_d.$$

If $n \geq 3$ is odd, then $[c_n]_2 = [b_1]_2 * \cdots * [b_n]_2 = [0,0]_2$ or $[0,1]_2$. However, $[c_n]_2 = [1,1]_2$, by previous Proposition, which is absurd. On the other hand, if $n \geq 3$ is even then

$$[0,1]_2 = [c_n]_2 = [b_1]_2 * [b_2]_2 * \cdots * [b_n]_2.$$

However, $[b_1]_2 * [b_2]_2 * [b_n]_2 = [1,1]_2 * [0,1]_2 * [b_n]_2 = [0,1]_2 * [b_n]_2 = [0,0]_2$ whenever $[b_n]_2 = [0,0]_2$ or $[0,1]_2$. Hence the right-hand side of above equation is $[0,0]_2$ which is absurd. □

Theorem 5. *For $n \geq 3$, $[b_n]_4 \notin \{[1,1]_4, [1,3]_4, [3,1]_4, [3,3]_4\}$.*

Proof. Note that, we have the following multiplication table:

$*$	$[1,0]_4$	$[3,0]_4$	$[1,2]_4$	$[3,2]_4$
$[1,0]_4$	$[1,0]_4$	$[3,0]_4$	$[1,2]_4$	$[3,2]_4$
$[3,0]_4$	$[3,0]_4$	$[1,0]_4$	$[3,2]_4$	$[1,2]_4$
$[1,2]_4$	$[1,2]_4$	$[3,2]_4$	$[1,0]_4$	$[3,0]_4$
$[3,2]_4$	$[3,2]_4$	$[1,2]_4$	$[3,0]_4$	$[1,0]_4$

Hence $\{[1,0]_4, [3,0]_4, [1,2]_4, [3,2]_4\}$ is closed under multiplication.

By Lemma 6.2, we know that $[b_n]_4 \in \{[1,1]_4, [1,3]_4, [3,1]_4, [3,3]_4, [1,0]_4, [3,0]_4, [1,2]_4, [3,2]_4\}$ for $n \geq 3$. Now, suppose there exists n such that $[b_n]_4 \in \{[1,1]_4, [1,3]_4, [3,1]_4, [3,3]_4\}$ and such n is minimal. Since n is the least number greater than 2 such that $[b_n]_4 \notin \{[1,0]_4, [3,0]_4, [1,2]_4, [3,2]_4\}$ so $[b_i]_2 = [1,0]_2$ for all $3 \leq i < n$. If n is odd then

$$[1,1]_2 = [c_n]_2 = [b_1]_2 * \cdots * [b_n]_2 = [1,1]_2 * \cdots * [1,1]_2 = [1,0]_2$$

which is absurd.

On the other hand, we consider n is even. Since n is the first number such that $[b_n]_4 \notin \{[1,0]_4, [3,0]_4, [1,2]_4, [3,2]_4\}$ so

$$\prod_{\substack{d|n \\ 2<d<n}} [b_d]_4 \in \{[1,0]_4, [3,0]_4, [1,2]_4, [3,2]_4\},$$

since they are closed under multiplication.

Hence we need to consider the following cases:

1. For $[c]_4 = [1,1]_4$, we have $[c_n]_4 = [0,3]_4$ for n is even. Note that $[b_1]_4 * [b_2]_4 = [3,3]_4 * [2,3]_4 = [0,3]_4$ so

   $$[b_1]_4 * [b_2]_4 * [b_n]_4 = [2,1]_4 \text{ or } [2,3]_4.$$

   Moreover,

   $$[c_n]_4 = [b_1]_4 * [b_2]_4 * \cdots * [b_n]_4 = [2,1]_4 \text{ or } [2,3]_4,$$

   which is a contradiction since $[c_n]_4 = [0,3]_4$.

2. For $[c]_4 = [1,3]_4$, we have $[c_n]_4 = [0,1]_4$ for n is even. Note that $[b_1]_4 * [b_2]_4 = [3,1]_4 * [2,1]_4 = [0,1]_4$ so

   $$[b_1]_4 * [b_2]_4 * [b_n]_4 = [2,1]_4 \text{ or } [2,3]_4.$$

   Moreover,

   $$[c_n]_4 = [b_1]_4 * [b_2]_4 * \cdots * [b_n]_4 = [2,1]_4 \text{ or } [2,3]_4,$$

   which is a contradiction since $[c_n]_4 = [0,1]_4$.

3. For $[c]_4 = [3,1]_4$, we have $[c_n]_4 = [2,3]_4$ for n is even. Note that $[b_1]_4 * [b_2]_4 = [1,3]_4 * [0,3]_4 = [2,3]_4$ so

   $$[b_1]_4 * [b_2]_4 * [b_n]_4 = [0,1]_4 \text{ or } [0,3]_4.$$

   Moreover,

   $$[c_n]_4 = [b_1]_4 * [b_2]_4 * \cdots * [b_n]_4 = [0,1]_4 \text{ or } [0,3]_4,$$

   which is a contradiction since $[c_n]_4 = [2,3]_4$.

4. For $[c]_4 = [3,3]_4$, we have $[c_n]_4 = [2,1]_4$ for n is even. Note that $[b_1]_4 * [b_2]_4 = [1,1]_4 * [0,1]_4 = [2,1]_4$ so

$$[b_1]_4 * [b_2]_4 * [b_n]_4 = [0,1]_4 \text{ or } [0,3]_4.$$

Moreover,

$$[c_n]_4 = [b_1]_4 * [b_2]_4 * \cdots * [b_n]_4 = [0,1]_4 \text{ or } [0,3]_4,$$

which is a contradiction since $[c_n]_4 = [2,1]_4$.

□

Corollary. *If $c = u + v\sqrt{2}$ where u, v are odd positive integers, then $\Omega_n \cong [C_2]^n$ for any $n \geq 1$.*

Proof. By Lemma 6.1 and Theorem 5, we show that b_i will appear a new prime with odd power for $i \geq 3$. Hence $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}(\sqrt{2})$ for any $n \in \mathbb{Z}$ and so $\Omega_n \cong [C_2]^n$ by Theorem 1. □

7 2-independent property of integers over quadratic number field

We split this section into two parts, first, for $f(X) = X^2 + c \in \mathbb{Z}[X]$, we will find some sufficient conditions such that the Galois group of $f^n(X)$ over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$ is isomorphic to $[C_2]^n$. Next, we will prove some properties of 2-independent over a quadratic number field.

we denote $d \in \mathbb{Z}$ where d is square-free. Give $c \in \mathbb{Z}$, we define

$$c_1 = -c \text{ and } c_n = c_{n-1}^2 + c \text{ for } n \geq 2.$$

Let

$$b_n = \prod_{d|n} c_d^{\mu(n/d)},$$

then $b_n \in \mathbb{Z}$ for all n and b_n are pairwise coprime (by [2, Lemma 1.1]). Note that $b_1 = -c$, and we define that

$$B_c = \{b_n : n \in \mathbb{N} \text{ and } b_1 = -c\}.$$

Definition. A subset S in a field K is called 2-*independent* over K if their residue classes in the $\mathbb{F}_2$-vector space $K^*/(K^*)^2$ are linearly independent. If S is not 2-independent over K, then we say that S is 2-*dependent* over K.

M. Stoll [2, Theorem] shows that:

Theorem. *If $c \in \mathbb{Z}$ has one of the following properties:*

1. *$c > 0$, and $c \equiv 1 \pmod 4$;*

2. $c > 0$, *and* $c \equiv 2 \pmod 4$;

3. $c < 0$, $c \equiv 0 \pmod 4$ *and* $-c$ *is not a square in* $\mathbb{Z}$.

then none of $|b_2|, \cdots, |b_n|$ *is a square in* $\mathbb{Q}$.

Corollary. *If* c *satisfies one of the properties in the previous theorem, then* B_c *is 2-independent over* $\mathbb{Q}$. *Moreover,* $\Omega_n \cong [C_2]^n$ *for all* $n \in \mathbb{N}$.

Proof. Since $(b_i, b_j) = 1$ for $i \neq j$, so B_c is 2-independent over $\mathbb{Q}$ which is equivalent to for any subset $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$, none of b_{i_j} is square and at most one of $-b_{i_j}$ is a square in $\mathbb{Q}$. Moreover, since $b_1 = -c$ is not a square in $\mathbb{Q}$ for all cases. Hence none of $|b_2|, \cdots, |b_n|$ is a square in $\mathbb{Q}$ implies B_c is 2-independent over $\mathbb{Q}$.

By Theorem in [2], since $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}$ for all n, so $\Omega_n \cong [C_2]^n$ for all $n \in \mathbb{N}$. □

It is natural to consider whether B_c is 2-independent over another field or not. The easiest case is to consider the basic field is a quadratic number field. For convenience, if $S \subset K = \mathbb{Q}(\sqrt{a})$ then we denoted,

$$\left\{\frac{a}{S}\right\} = \begin{cases} -1 & \text{if } S \text{ is 2-independent over } \mathbb{Q}(\sqrt{a}), \\ 1 & \text{if } S \text{ is 2-dependent over } \mathbb{Q}(\sqrt{a}). \end{cases}$$

Moreover, we take $a = 1$ if $K = \mathbb{Q}$ and only consider the case $\{\frac{1}{B_c}\} = -1$ in the following statements. To study this problem, we need to investigate all prime numbers in which divides some elements in B_c.

Definition. We denote the set of all prime numbers by $\mathcal{P}$. Consider $S \subset \mathbb{Z}$, we define the set of prime divisors of S by

$$P(S) = \{p \in \mathcal{P} : p \text{ divides } s \text{ for some } s \in S \text{ with } s \neq 0\}.$$

Moreover, if we have $B \subset A \subset \mathbb{Z}$ then we can define the density of B in A by

$$d_A(B) = \lim_{n\to\infty} \frac{\#\{b \in B : b \leq n\}}{\#\{a \in A : a \leq n\}}$$

By the property of b_n, we have:

Proposition 1. *If* c *satisfies one of the properties in Stoll's theorem. Then, for any* b_i *where* $i \geq 2$, *there exists a prime* p_i *such that* $v_{p_i}(b_i)$ *is odd where* $v_{p_i}(\cdot)$ *is the valuation.*

Proof. If $v_p(b)$ is even for all prime p, then $|b|$ is a square. Since none of $|b_i|$ is square for $i \geq 2$ so there exists prime number p_i such that $v_{p_i}(b_i)$ is odd. □

Moreover, since b_i are pairwise coprime so $p_i \neq p_j$ if $i \neq j$ in previous proof. Hence $P(B_c)$ is an infinite set. However, in R. Jones' paper [10, Theorem 1.2], he shows that

Theorem. *$d_{\mathcal{P}}(P(B_c)) = 0$ for $c \in \mathbb{Z}\backslash\{-1\}$.*

Hence, there also exist infinitely many prime numbers that do not divide any one of b_n. Actually, it is far more than the number of primes which can divide some b_n. To deal with this problem, for arbitrary a, we have $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{d})$ where d is the radical of a. Hence it is enough to consider $\mathbb{Q}(\sqrt{d})$ where d is square-free. Here, we prove a useful lemma first.

Lemma 7.1. *$\{\frac{d}{B_c}\} = 1$ for some square-free integer d if and only if there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that*

$$b_{i_1} \cdots b_{i_k} = dn^2 \text{ where } n \in \mathbb{Z}.$$

Proof. Suppose B_c is not 2-independent over $\mathbb{Q}(\sqrt{d})$ then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ and $s, t \in \mathbb{Q}$ such that

$$b_{i_1} \cdots b_{i_k} = (s + t\sqrt{d})^2 = (s^2 + dt^2) + 2st\sqrt{d}.$$

Since the left-hand side is an integer so $s = 0$ or $t = 0$.

If $t = 0$ then $b_{i_1} \cdots b_{i_k} = s^2$. However, B_c is 2-independent over $\mathbb{Q}$ which makes a contradiction. Hence $s = 0$ and we have

$$b_{i_1} \cdots b_{i_k} = dt^2.$$

If t is not an integer then so is dt^2. But the left-hand side is an integer which makes a contradiction, thus $t \in \mathbb{Z}$.

On the other hand, if there exist some elements in B_c such that

$$b_{i_1} \cdots b_{i_k} = dn^2 = (0 + n\sqrt{d})^2 \text{ where } n \in \mathbb{Z}.$$

Then B_c is not 2-independent over $\mathbb{Q}(\sqrt{d})$. □

The easiest case is to consider d is a prime. Here we give a sufficient and necessary condition to determine the value of $\{\frac{p}{B_c}\}$ where p is a prime.

Theorem 6. *Let p be a prime number, $\{\frac{p}{B_c}\} = 1$ if and only if $b_n = pt^2$ or $b_n = -pt^2$ and $c \in \mathbb{Q}^2$ where $t \in \mathbb{Z}$ and $n \in \mathbb{N}$.*

Proof. If $b_n = pt^2$ then $b_n = (0 + t\sqrt{p})^2$. For the other case, if $b_n = -pt^2$ and $c = -b_1 = s^2$ where $s \in \mathbb{Q}$ then $b_1 b_n = (0 + st\sqrt{p})^2$. Hence, for above two cases, $\{\frac{p}{B_c}\} = 1$.

Conversely, if $\{\frac{p}{B_c}\} = 1$, by Lemma 1, there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = pt^2 \text{ where } t \in \mathbb{Z}.$$

Without loss of generality, let $p \mid b_n$, then for any $i > 1$ and $i \neq n$, there exists a prime $p_i \neq p$ such that $v_{p_i}(b_i)$ is odd by Proposition 1. Hence $b_i \notin \{b_{i_1}, \cdots, b_{i_k}\}$, otherwise, $v_{p_i}(b_{i_1} \cdots b_{i_k})$ is odd but $v_{p_i}(pt^2)$ is even which is absurd. Hence $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_n\}$ or $\{b_1, b_n\}$.

If $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_n\}$ then $b_n = pt^2$. For the second case, we can assume $n \neq 1$, otherwise, it can be reduced to the first case. Thus, we have $b_1 b_n = pt^2$. Since $v_p(b_1) = 0$ so b_1 must be $-s^2$ for some $s \in \mathbb{Z}$ and $s \mid t$. Hence $c = -b_1 \in \mathbb{Q}^2$ and $b_n = p \cdot (t/s)^2$ where $t/s \in \mathbb{Z}$. □

Because $\mathcal{P}\backslash P(B_c)$ is an infinitely set, by Theorem 6, it is obviously that $\{\frac{\pm p}{B_c}\} = -1$ for any $p \notin P(B_c)$. Hence, there exists infinitely many quadratic number field such that B_c is 2-independent over it. In fact, we can describe more precisely about primes, not in $P(B_c)$.

Proposition 2. *If* $(\frac{-c}{p}) = -1$ *then* $p \notin P(B_c)$ *where* $(\frac{\cdot}{\cdot})$ *is the Legendre symbol, thus* $\{\frac{\pm p}{B_c}\} = -1$.

Proof. Note that $(\frac{-c}{p}) = -1$ so $p \nmid c_1$. If $p \mid c_n$ for some n then

$$c_n = c_{n-1}^2 + c \equiv 0 \pmod{p}.$$

Thus $(\frac{-c}{p}) = 1$ which is a contradiction. Hence $p \nmid c_n$ and so $p \nmid b_n$ for all $n \in \mathbb{N}$. □

Hence, if b_1 is not a quadratic residue modulo p then B_c is 2-independent over $\mathbb{Q}(\sqrt{\pm p})$. However, all such prime numbers do not lie in $P(B_c)$. In Theorem 6, we have a sufficient and necessary condition to determine whether $\{\frac{p}{B_c}\} = 1$ or not. Later, we will show that there is infinitely many such primes exist under some conditions.

Obviously, since one of b_1 or b_2 is even, so we can give a sufficient and necessary condition to determine whether or not B_n is 2-independent over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. In the following two results, since we assume $\{\frac{1}{B_c}\} = -1$ so we only consider $c \in \mathbb{Z}$ which satisfies one of the following properties:

1. $c > 0$, $c \equiv 1 \pmod 4$;
2. $c > 0$, $c \equiv 2 \pmod 4$;
3. $c < 0$, $c \equiv 0 \pmod 4$ and $-c$ is not a square in $\mathbb{Z}$.

Definition. An NSW(Newman-Shanks-Williams) number is an integer m such that the Diophantine equation

$$2x^2 = m^2 + 1$$

can be solved in integers.

Theorem 7. $\{\frac{2}{B_c}\} = 1$ *if and only if* $\sqrt{c}$ *is an NSW number in case* 1 *or* $v_2(c)$ *is odd and* $v_p(c)$ *is even for all odd prime* p *in case* 3.

Proof. Note that, by Theorem 6.3, $\{\frac{2}{B_c}\} = 1$ if and only if $b_n = 2t^2$ or $b_n = -2t^2$ and $c \in \mathbb{Q}^2$. Moreover, since one of b_1 or b_2 is even so $n = 1$ or 2.

Suppose $\sqrt{c}$ is an NSW number in case 1 then c is a square and $2x^2 = c + 1$ has an integer solution, called t. Hence $b_2 = -(c+1) = -2t^2$ and so $\{\frac{2}{B_c}\} = 1$.

For another case, since $c < 0$, $v_2(c)$ is odd and $v_p(c)$ is even for all odd prime p so $c = -2t^2$ where $t \in \mathbb{Z}$. Again, by Theorem 6.3, $b_1 = -c = 2t^2$ implies $\{\frac{2}{B_c}\} = 1$.

Conversely, suppose $\{\frac{2}{B_c}\} = 1$ then B_c must satisfy one of the following case:

1. $b_1 = 2t^2$;

2. $b_2 = 2t^2$;

3. $-b_1 = c \in \mathbb{Q}^2$ and $b_2 = -2t^2$

where $t \in \mathbb{Z}$.

In the first case, $b_1 = -c = 2t^2$ then $c < 0$, $v_2(c)$ is odd and $v_p(c)$ is even for all prime p. The second case is absurd since $b_2 = -(c+1) = 2t^2$ imply $c < 0$. However, we assume that if $c < 0$ then $4 \mid c = -1 - 2t^2$. For the last case, since $c \in \mathbb{Q}^2$ so we can write c as $(c')^2$ where $c' \in \mathbb{Q}$. Then $b_2 = -(c+1) = -2t^2$ which means $2x^2 = c + 1$ has an integer solution and so $\sqrt{c} = c'$ is an NSW number. □

Corollary. *If $c \in \mathbb{Z}$ has one of the following properties:*

1. *$c > 0$, and $c \equiv 1 \pmod 4$ and $\sqrt{c}$ is not an NSW number;*

2. *$c > 0$, and $c \equiv 2 \pmod 4$;*

3. *$c < 0$, $c \equiv 0 \pmod 4$ and $-c$ is not square in $\mathbb{Z}$. Moreover, $v_2(c)$ is even or $v_p(c)$ is odd for some odd prime p.*

then $\mathrm{Gal}(f^n(X)/\mathbb{Q}(\sqrt{2})) \cong [C_2]^n$ *for all $n \geq 1$ where $f(X) = X^2 + c$.*

Proof. By Theorem 7, if c satisfies one of properties in hypothesis then $\{\frac{2}{B_c}\} = -1$. Hence $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}(\sqrt{2})$ for all n which is equivalent to $\mathrm{Gal}(f^n(X)/\mathbb{Q}(\sqrt{2})) \cong [C_2]^n$, by Theorem 1. □

Theorem 8. $\{\frac{-2}{B_c}\} = 1$ *if and only if $\sqrt{c}$ is an NSW number in case* 1 *or $c/2$ is a square in case* 2.

Proof. For case 1, Suppose B_c is not 2-independent over $\mathbb{Q}(\sqrt{-2})$ then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = -2t^2 \text{ where } t \in \mathbb{Z}.$$

Since c is odd and $b_2 = -(c+1)$ so b_2 is the only even integer in B_c then $b_2 \in \{b_{i_1}, \cdots, b_{i_k}\}$. If there exists $b_i \in \{b_{i_1}, \cdots, b_{i_k}\}$ where $i \geq 3$ then there exists an odd prime p_i such that $v_{p_i}(b_{i_1} \cdots b_{i_k})$ is odd, but $v_{p_i}(-2t^2)$ is even for any odd prime p_i, which is a contradiction. Hence $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_1, b_2\}$ or $\{b_2\}$.

If $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_2\}$ then

$$b_2 = -(c+1) = -2t^2.$$

That means t is a solution of $2x^2 = c+1$ which is a contradiction since we assume $\sqrt{c}$ is not an NSW number.

If $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_1, b_2\}$ then

$$-2t^2 = b_1 b_2 = c(c+1) \geq 0$$

which is a contradiction. Hence B_c is 2-independent over $\mathbb{Q}(\sqrt{-2})$.

For case 2, Suppose B_c is not 2-independent over $\mathbb{Q}(\sqrt{-2})$ then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_n$ such that

$$b_{i_1} \cdots b_{i_k} = -2t^2 \text{ where } t \in \mathbb{Z}.$$

Since $b_1 = -c$ is the only even number in B_n so $b_1 \in \{b_{i_1}, \cdots, b_{i_k}\}$. If there exists $b_i \in \{b_{i_1}, \cdots, b_{i_k}\}$ where $i \geq 2$ then there exists an odd prime p_i such that $v_{p_i}(b_{i_1} \cdots b_{i_k})$ is odd, but $v_{p_i}(-2t^2)$ is even for any odd prime p_i, which is a contradiction. So $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_1\}$. Hence $b_1 = -c = -2t^2$,i.e., $c/2 = t^2$, but we assume that $c/2 \in \mathbb{Q}^2$ which is a contradiction. Hence B_c is 2-independent over $\mathbb{Q}(\sqrt{-2})$.

For case 3, Suppose B_c is not 2-independent over $\mathbb{Q}(\sqrt{-2})$ then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = -2t^2 \text{ where } t \in \mathbb{Z}.$$

Since $b_1 = -c$ is the only even number in B_c so $b_1 \in \{b_{i_1}, \cdots, b_{i_k}\}$. If there exists $b_i \in \{b_{i_1}, \cdots, b_{i_k}\}$ where $i \geq 2$ then there exists an odd prime p_i such that $v_{p_i}(b_{i_1} \cdots b_{i_k})$ is odd, but $v_{p_i}(2n^2)$ is even for any odd prime p_i, which is a contradiction. Hence $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_1\}$ and we have

$$b_1 = -2t^2.$$

But $b_1 = -c > 0$, hence such $\{b_{i_1}, \cdots, b_{i_k}\}$ does not exist. Hence B_c is 2-independent over $\mathbb{Q}(\sqrt{-2})$.

Conversely, consider $c > 0$, $c \equiv 1 \pmod 4$ and $\sqrt{c}$ is an NSW number then $2x^2 = c + 1$ has solution. Hence

$$b_2 = -(c+1) = -2x^2,$$

which means B_c is not 2-independent over $\mathbb{Q}(\sqrt{-2})$.

If $c > 0$, $c \equiv 2 \pmod 4$ and $c/2 \in \mathbb{Q}^2$ that means $c = 2t^2$ where t is an odd integer, then B_c is not 2-independent over $\mathbb{Q}(\sqrt{-2})$ since

$$b_1 = -c = -2t^2.$$

□

Corollary. *If $c \in \mathbb{Z}$ has one of the following properties:*

1. *$c > 0$, $c \equiv 1 \pmod 4$ and c is not an NSW number;*
2. *$c > 0$, $c \equiv 2 \pmod 4$ and $c/2 \notin \mathbb{Q}^2$;*
3. *$c < 0$, $c \equiv 0 \pmod 4$ and $-c$ is not a square in $\mathbb{Z}$.*

then $\mathrm{Gal}(f^n(X)/\mathbb{Q}(\sqrt{-2})) \cong [C_2]^n$ *for all $n \geq 1$ where $f(X) = X^2 + c$.*

Proof. By Theorem 8, if c satisfies one of properties in hypothesis then $\{\frac{-2}{B_c}\} = -1$. Hence $\{b_1, \cdots, b_n\}$ is 2-independent over $\mathbb{Q}(\sqrt{-2})$ for all n which is equivalent to $\mathrm{Gal}(f^n(X)/\mathbb{Q}(\sqrt{-2})) \cong [C_2]^n$, by Theorem 1. □

Now, we want to know whether there exists infinitely many primes, $p \in P(B_c)$ such that B_n is not 2-independent over $\mathbb{Q}(\sqrt{p})$ or not.

Theorem 9. *there exists infinitely many d such B_c is 2-independent over $\mathbb{Q}(\sqrt{d})$ if c has one of the following property:*

1. *$c > 0$, $c \equiv 1 \pmod 4$ and c is not a square;*
2. *$c > 0$, $c \equiv 2 \pmod 4$;*
3. *$c < 0$, $c \equiv 0 \pmod 4$ and $-c$ is not a square in $\mathbb{Z}$.*

Proof. We have shown that for all $i \geq 3$ there is an odd prime p_i such that $v_{p_i}(b_i)$ is odd. We claim that if $d_i = -\operatorname{sgn}(b_i)p_i$ then B_c is 2-independent over $\mathbb{Q}(\sqrt{d_i})$ for all i.

Suppose B_c is not 2-independent over $\mathbb{Q}(\sqrt{d_i})$ for some i then there exists a subset $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = d_i t^2 \text{ for some } t \in \mathbb{Q}.$$

Since $v_{p_i}(d_i t^2)$ is odd so $b_i \in \{b_{i_1}, \cdots, b_{i_k}\}$ and $v_p(d_i t^2)$ is even for another prime so $b_k \notin \{b_{i_1}, \cdots, b_{i_k}\}$ for $k \geq 2$ and $k \neq i$.

Hence $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_i\}$ or $\{b_1, b_i\}$. If $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_i\}$ then

$$b_i = d_i t^2 \text{ for some } t \in \mathbb{Z},$$

thus

$$\operatorname{sgn}(b_i) = \operatorname{sgn}(d_i t^2) = \operatorname{sgn}(d_i) = -\operatorname{sgn}(b_i)$$

which is a contradiction.

If $b_i \in \{b_{i_1}, \cdots, b_{i_k}\} = \{b_1, b_i\}$ then

$$b_1 b_i = d_i t^2 \text{ for some } t \in \mathbb{Z},$$

and so $|b_1|$ must be a square. However, we have assumed that $|b_1| = |c|$ is not a square for all case.

Hence B_c is 2-independent over $\mathbb{Q}(\sqrt{d_i})$ for all i. □

Remark. By Theorem 9, we know that for the above three cases, there exists infinite many quadratic number field such that $\operatorname{Gal}(f^n(X)/\mathbb{Q}(\sqrt{d})) \cong [C_2]^n$. However, it is hard to find all elements in $P(B_c)$ for given $c \in \mathbb{Z}$. Hence, we cannot give a criterion for p, c to determine whether $\operatorname{Gal}(f^n(X)/\mathbb{Q}(\sqrt{p})) \cong [C_2]^n$ or not.

In the second part, we have some property about 2-independent over quadratic number field.

Proposition. $\{\frac{-1}{B_c}\} = 1$ *if and only if* $c \in \mathbb{Q}^2$.

Proof. If $c \in \mathbb{Q}^2$, let $c = (c')^2$ where $c' \in \mathbb{Q}$, then

$$b_1 = -c = -(c')^2.$$

Hence B_c is 2-dependent over $\mathbb{Q}(\sqrt{-1})$, by Lemma 7.1.

Conversely, if B_c is 2-dependent over $\mathbb{Q}(\sqrt{-1})$, then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = -t^2 \text{ where } t \in \mathbb{Z}.$$

Note that $v_p(-t^2)$ is even for any prime p and none of $|b_i|$ is a square for $i \geq 2$. Hence $\{b_{i_1}, \cdots, b_{i_k}\} = \{b_1\}$ and so $b_1 = -c = -t^2$. Therefore, $c \in \mathbb{Q}^2$. □

Proposition. *If* $\{\frac{1}{B_c}\} = 1$ *then* $\{\frac{a}{B_c}\} = 1$ *for any* $a \in \mathbb{Z}$.

Proof. Suppose B_n is not 2-independent over $\mathbb{Q}$ then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_n$ such that

$$b_{i_1} \cdots b_{i_k} = s^2 = (s + 0 \cdot \sqrt{a})^2 \text{ where } s \in \mathbb{Q}.$$

So B_n is not 2-independent over $\mathbb{Q}(\sqrt{a})$. □

Proposition. *If* $P(\{a\}) \not\subset P(B_c)$ *then* $\{\frac{a}{B_c}\} = \{\frac{-a}{B_c}\} = -1$.

Proof. If $P(\{a\}) \not\subset P(B_c)$ then there exists a prime p such that $p \mid a$ but $p \notin P(B_c)$. Suppose $\{\frac{a}{B_c}\}$ or $\{\frac{-a}{B_c}\} = 1$, then there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = at^2 \text{ or } -at^2 \text{ where } t \in \mathbb{Z}.$$

However, take $v_p(\cdot)$ on both sides, the left-hand side is zero. On the other hand, the right-hand side is nonzero, which is a contradiction. □

Proposition. *Suppose* $\{\frac{d}{B_c}\} = 1$ *then* $\{\frac{-d}{B_c}\} = 1$ *if and only if* $\{\frac{-1}{B_c}\} = 1$.

Proof. It is clear when $d = 1$. Hence we only need to consider $d > 1$. Since $\{\frac{d}{B_c}\} = 1$ so there exists $\{b_{i_1}, \cdots, b_{i_k}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = dt^2 \text{ where } t \in \mathbb{Z}.$$

Suppose $\{\frac{-d}{B_c}\} = 1$ then there exists $\{b_{j_1}, \cdots, b_{j_l}\} \subset B_c$ such that

$$b_{j_1} \cdots b_{j_l} = -ds^2 \text{ where } s \in \mathbb{Z}.$$

Hence we have

$$b_{i_1} \cdots b_{i_k} b_{j_1} \cdots b_{j_l} = -(dst)^2,$$

by Lemma 7.1, $\{\frac{-1}{B_c}\} = 1$.

Conversely, suppose $\{\frac{-1}{B_c}\} = 1$ then $c \in \mathbb{Q}^2$ by Lemma 7.3. Let $c = s^2$ where $s \in \mathbb{Q}$ so $b_1 = -s^2$. Now, we discuss the following two cases:

First, if $b_1 \in \{b_{i_1}, \cdots, b_{i_k}\}$ then without loss of generality, let $b_{i_k} = b_1$. Since $d > 1$ so $\{b_1\} \subsetneq \{b_{i_1}, \cdots, b_{i_k}\}$. Hence

$$b_{i_1} \cdots b_{i_{k-1}} = \frac{dt^2}{b_1} = \frac{dt^2}{-s^2} = -d \cdot (t/s)^2$$

which means $\{\frac{-d}{B_c}\} = 1$.

For the second case, we consider $b_1 \notin \{b_{i_1}, \cdots, b_{i_k}\}$ then

$$b_1 b_{i_1} \cdots b_{i_k} = -s^2 \cdot dt^2 = -d(st)^2.$$

Hence $\{\frac{-d}{B_c}\} = 1$, by Lemma 1. □

Proposition. *For any $a, b \in \mathbb{Z}$, if $\{\frac{a}{B_c}\} = \{\frac{b}{B_c}\} = 1$ then $\{\frac{ab}{B_c}\} = 1$.*

Proof. By Lemma, there exists $\{b_{i_1}, \cdots, b_{i_k}\}$ and $\{b_{j_1}, \cdots, b_{j_l}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = at^2 \text{ and } b_{j_1} \cdots b_{j_l} = bs^2 \text{ where } s, t \in \mathbb{Z}.$$

So

$$b_{i_1} \cdots b_{i_k} \cdot b_{j_1} \cdots b_{j_l} = ab(st)^2.$$

Hence B_c is not 2-independent over $\mathbb{Q}(\sqrt{ab})$. □

Corollary. *Suppose $b_n = pt^2$ or $b_n = -pt^2$ and $c \in \mathbb{Q}^2$ where $t \in \mathbb{Z}$ and $n \in \mathbb{N}$ then $\{\frac{-p}{B_c}\} = 1$ if and only if $\{\frac{-1}{B_c}\} = 1$.*

Proof. By Theorem 6.3, $\{\frac{p}{B_c}\} = 1$. Hence by Lemma 6.3, $\{\frac{-p}{B_c}\} = 1$ if and only if $\{\frac{-1}{B_c}\} = 1$. □

Proposition. *For any $a, b \in \mathbb{Z}$, if $\{\frac{a}{B_c}\}\{\frac{b}{B_c}\} = -1$ then $\{\frac{ab}{B_c}\} = -1$.*

Proof. Without loss of generality, Let $\{\frac{a}{B_c}\} = 1$ and $\{\frac{b}{B_c}\} = -1$, and suppose $\{\frac{ab}{B_c}\} = 1$. By Lemma, there exists $\{b_{i_1}, \cdots, b_{i_k}\}$ and $\{b_{j_1}, \cdots, b_{j_l}\} \subset B_c$ such that

$$b_{i_1} \cdots b_{i_k} = at^2 \text{ and } b_{j_1} \cdots b_{j_l} = abs^2 \text{ where } s, t \in \mathbb{Z}.$$

So

$$b_{i_1} \cdots b_{i_k} \cdot b_{j_1} \cdots b_{j_l} = b(ast)^2$$

which implies $\{\frac{b}{B_c}\} = 1$. However, we assume $\{\frac{b}{B_c}\} = -1$ which is absurd. Hence B_c is 2-independent over $\mathbb{Q}(\sqrt{ab})$. □

References

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

[2] M. Stoll, Galois groups over $\mathbb{Q}$ of some iterated polynomials, Arch. Math. (Basel) 59, 239-244 (1992).

[3] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, second edition, GTM 84, Springer-Verlag, New York, 1982.

[4] J. J. Rotman, An Introduction to the Theory of Groups, forth edition, GTM 148, Springer-Verlag, New York, 1995, ch.7.

[5] J. Neukirch, Algebraic number theory, first edition, Springer-Verlag, Berlin Heidelberg, 1999.

[6] E. Horowitz and S. Sahni, Fundamentals of Computer Algorithms, first edition, Computer Science Press, 1978.

[7] M. F. Atiyah and I. G. Macdonald, Introduction to Commutaive Algebra, Addison-Wesley, 1969.

[8] R. W. K. Odoni, The Galois theory of composites and iterates of polynomials, Proc. London Math. Soc. 51(3), 385-414 (1985).

[9] H. Hasse, Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper. Elem. Math., 20, 49–59 (1965).

[10] R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. 78(2), 523–544 (2008).