Iterated towers of number fields by a quadratic map defined over the Gaussian rationals

By Yasushi MIZUSAWA[*)] and Kota YAMAMOTO[**)]

(Communicated by Shigefumi MORI, M.J.A., Sept. 14, 2020)

Abstract: An iterated tower of number fields is constructed by adding preimages of a base point by iterations of a rational map. A certain basic quadratic rational map defined over the Gaussian number field yields such a tower of which any two steps are relative bicyclic biquadratic extensions. Regarding such towers as analogues of $\mathbf{Z}_2$-extensions, we examine the parity of 2-ideal class numbers along the towers with some examples.

Key words: Iterated extension; class number parity; Iwasawa theory.

1. Introduction. Let ϕ be a rational map of prime degree p which is defined as the rational function $\phi(x) \in k(x)$ over a number field k. Let $\{b_n\}_{0\leq n\in\mathbf{Z}}$ be a sequence of algebraic numbers such that $\phi(b_{n+1}) = b_n$ for all $n \geq 0$. For a finite extension $K/k(b_0)$, we obtain a sequence

$$K \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup_{n\geq 1} K_n,$$

where $K_n = K(b_n)$ for each $n \geq 1$. The number field K_n is contained in a Galois extension $K(\phi^{-n}(b_0))$ of K. If ϕ is 'post-critically finite', i.e., the orbits $\{\phi^n(c)\}_{0\leq n\in\mathbf{Z}}$ of any critical points c of ϕ are finite, then the number of primes of K ramifying in $K(\phi^{-\infty}(b_0))/K$ is finite ([1,5]), and such iterated extensions have been constructed and studied in various situations (see e.g. [2,3]).

If K_n/K is a cyclic Galois extension of degree p^n for all $n \geq 1$, then K_∞ is a $\mathbf{Z}_p$-extension of K, i.e., $\mathrm{Gal}(K_\infty/K)$ is isomorphic to the additive group $\mathbf{Z}_p$ of p-adic integers. For example, K_∞/K is the cyclotomic $\mathbf{Z}_2$-extension if $\phi(x) = x^2 - 2$ and $b_0 = 0$. The growth of the p-parts of the class numbers along a $\mathbf{Z}_p$-extension K_∞/K is described by Iwasawa's class number formula ([9]), and such a formula has been extended to some non-Galois towers ([4,11] etc.) and p-adic Lie extensions ([6,12,15] etc.). One of the most important conjectures in Iwasawa theory is Greenberg's conjecture ([7]) which states that the p-parts of the class numbers are bounded along the cyclotomic $\mathbf{Z}_p$-extension of a totally real number field. Analogous problems can be also considered for iterated extensions K_∞/K by post-critically finite ϕ, as in [17] where the case of $\phi(x) = x^2 - 2$ has been considered. In particular, it is a basic problem to find many iterated extensions K_∞/K such that the T-ideal class number of K_n is not divisible by p for all sufficiently large n and for a finite set T of primes of K ramifying in K_∞/K. For a finite set T of primes of a subfield of a number field F, the T-ideal class number $|Cl^T(F)|$ of F is the order of the T-ideal class group $Cl^T(F) = Cl(F)/\langle [w]\,;\, w | \prod_{v\in T} v\rangle$, which is the quotient of the ideal class group $Cl(F)$ by the subgroup generated by all classes of prime ideals w lying over T.

In this paper, we consider iterated extensions K_∞/K by a rational finction

$$(1) \qquad \phi(x) = \frac{(ix) + (ix)^{-1}}{2} = \frac{i}{2}\left(x - \frac{1}{x}\right)$$

of degree $p = 2$, which is defined over the Gaussian number field $\mathbf{Q}(i)$, where $i = \sqrt{-1}$. The map ϕ is post-critically finite, and comes from an endomorphism of the elliptic curve $E : y^2 = x^3 + x$ with complex multiplication by Gaussian integers $\mathbf{Z}[i]$ (see Remark 3.3). Then, regarding K_∞/K as an analogue of a $\mathbf{Z}_2$-extension, we examine the parity of $|Cl^T(K_n)|$ along the tower of iterated extensions $\{K_n\}_{1\leq n\in\mathbf{Z}}$. The main result is the following theorem, which can be seen as a partial refinement of [5, §5] in a special case. Put a condition $C(b)$:

2020 Mathematics Subject Classification. Primary 11R11; Secondary 11R29, 11R23.

[*)] Department of Mathematics, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan.

[**)] Division of Mathematics and Mathematical Science, Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan.

doi: 10.3792/pjaa.96.012

$$\{\sqrt{b^2-1}, \sqrt{b(b\pm 1)}, \sqrt{b\pm 1}, \sqrt{b}\} \cap k(b) = \emptyset$$

for each algebraic number b. We denote an abelian 2-group by its type.

Theorem 1.1. *Suppose that $i \in k$ and $\phi(x) = \frac{i}{2}(x - \frac{1}{x})$. Let $b_0 \in k$ be an algebraic integer satisfying $C(b_0)$. Put $k_n = k(b_n)$ for $n \geq 0$. Put $K = k(\sqrt{b_0})$, and put $K_n = k_n(\sqrt{b_0})$ for $n \geq 1$. Let T be a set of primes of k lying over 2. Then the following statements hold true for each $n \geq 1$.*

(a) *k_{n+1}/k_{n-1} is a $[2,2]$-extension.*

(b) *K_{n+3}/K_n is a $[2,4]$-extension unramifid outside 2.*

(c) *If K_{n+2}/K_n is totally ramified at any prime lying over 2 and $2 \nmid |Cl^T(K_{n+2})|$, then $2 \nmid |Cl^T(K_m)|$ for all $m \geq n$.*

In the proof of Theorem 1.1, the notation K_0 denotes either k or K according to whether $\sqrt{b_0(b_0^2-1)} \in k$ or not. Then we will see that the statements (b) and (c) also hold true for $n = 0$ if $\sqrt{b_0(b_0^2-1)} \in k$.

Remark 1.2. For $b_0 \in k$, the conditions $C(b_0)$ and $\sqrt{b_0(b_0^2-1)} \notin k$ are satisfied if and only if $k(\sqrt{b_0}, \sqrt{b_0+1}, \sqrt{b_0-1})/k$ is a $[2,2,2]$-extension. If $\sqrt{b_0(b_0^2-1)} \in k$, then the condition $C(b_0)$ is satisfied if and only if $k(\sqrt{b_0}, \sqrt{b_0+1})/k$ is a $[2,2]$-extension. The point $(b_0, \sqrt{b_0(b_0^2-1)})$ is a $k(\sqrt{b_0(b_0^2-1)})$-rational point of the elliptic curve $E' : y^2 = x^3 - x$.

2. Proof of Theorem 1.1.

2.1. Preliminaries. Suppose that ϕ is defined as (1), and k is a finite extension of $\mathbf{Q}(i)$. For $b \in \overline{\mathbf{Q}}$, we have $\phi(b') = b$ if and only if $b'^2 + 2bib' - 1 = 0$, i.e.,

$$b' = -i(b \pm \sqrt{b^2-1}) = \left(\frac{\sqrt{b-1} \pm \sqrt{b+1}}{1+i}\right)^2.$$

Then $k(b') = k(b, \sqrt{b^2-1})$. Note that $2i = (1+i)^2$.

Lemma 2.1. *Assume that $i \in k$ and that the condition $C(b)$ is satisfied for $b \in \overline{\mathbf{Q}}$. Let b' and b'' be algebraic numbers such that $\phi(b') = b$ and $\phi(b'') = b'$. Then $k(b'')/k(b)$ is a $[2,2]$-extension containing three quadratic subextensions $k(b, \sqrt{b(b\pm 1)})$, $k(b')$. Moreover, the condition $C(b')$ is also satisfied.*

Proof. Let

$$f(x) = x^4 + 4bx^3 + 2x^2 - 4bx + 1 \in k(b)[x]$$

be the numerator of $\phi^2(x) - b = \frac{f(x)}{-4x^3+4x}$. Note that $\phi(-\frac{1}{x}) = \phi(x)$. Since $\phi(b'') = b'$ and $\phi(b') = b$, we can easily see that the four roots of $f(x)$ are

$$(2) \qquad b'', \quad -\frac{1}{b''}, \quad \frac{b''+1}{b''-1}, \quad -\frac{b''-1}{b''+1},$$

and hence $k(b'')/k(b)$ is a Galois extension and $[k(b''):k(b)] \leq 4$. Moreover, one can directly show that

$$\left(b'' + \frac{b''+1}{b''-1} + 2b\right)^2 = 4b(b-1),$$

which implies that $\sqrt{b(b-1)} \in k(b'')$. Since the condition $C(b)$ is satisfied,

$$k(b'') = k(b)(\sqrt{b(b-1)}, \sqrt{b(b+1)})$$

and $\mathrm{Gal}(k(b'')/k(b)) \simeq [2,2]$. Thus we obtain the former statement.

Since $[k(b''):k(b')] = 2$, we have $\sqrt{b'^2-1} \notin k(b')$. Recall that $b'^2 + 2bib' - 1 = 0$. Since $N_{k(b')/k(b)}(b'(b' \pm 1)) = -N_{k(b')/k(b)}(b' \pm 1) = \pm(1+i)^2 b$, and since $\sqrt{b} \notin k(b)$ by the assumption, we have $\sqrt{b'(b' \pm 1)} \notin k(b')$ and $\sqrt{b' \pm 1} \notin k(b')$. Note that $k(b'') = k(b')(\sqrt{b'^2-1}) = k(b')(\sqrt{bb'})$. If $\sqrt{b'} \in k(b')$, then $k(b'') = k(b')(\sqrt{b})$, in particular $k(\sqrt{b})/k(b)$ is a quadratic subextension of the $[2,2]$-extension $k(b'')/k(b)$. This implies that $k(\sqrt{b}) = k(b, \sqrt{b(b-1)})$ or $k(\sqrt{b}) = k(b, \sqrt{b(b+1)})$, i.e., $\sqrt{b-1} \in k(b)$ or $\sqrt{b+1} \in k(b)$. This is a contradiction. Therefore $\sqrt{b'} \notin k(b')$. Thus the latter statement is also obtained. □

Remark 2.2. Since ϕ^2 is defined over $\mathbf{Q}$, $f(x)$ is defined over $\mathbf{Q}(b)$. Put $g(x) = \pm\sqrt{x}$. Then $g^{-1}(x) = x^2$, and a conjugate

$$(g^{-1}\phi g)(x) = -\frac{1}{4}\left(x - 2 + \frac{1}{x}\right)$$

is also defined over $\mathbf{Q}$.

2.2. Field theoretic part. Unless otherwise noted, we may suppose that $b_0 \in k$ is not necessarily an algebraic integer.

Lemma 2.3. *If $C(b_0)$ is satisfied, then for all $n \geq 0$, $C(b_n)$ is satisfied, and k_{n+2}/k_n is a $[2,2]$-extension containing three quadratic subextensions $k_n(\sqrt{b_n(b_n \pm 1)})$, $k_{n+1} = k_n(\sqrt{b_n^2-1})$.*

Proof. We obtain the statement by using Lemma 2.1 inductively. □

Throughout the following, we assume that $C(b_0)$ is satisfied. Recall that $K_n = k_n(\sqrt{b_0})$ for each $n \geq 1$, and put

$$\begin{aligned} N_0 &= \{1 \leq n \in \mathbf{Z} \mid \sqrt{b_0} \in k_n\} \\ &= \{1 \leq n \in \mathbf{Z} \mid K_n = k_n\}. \end{aligned}$$

Note that $n \in N_0$ if $n \geq \min N_0$.

Lemma 2.4. *If $n \geq 1$, then $K_{n+1} = K_n(\sqrt{b_n})$. In particular, $K_n = k_n$ and $k_{n+1} = k_n(\sqrt{b_n})$ for all $n \in N_0$.*

Proof. Recall that $k_{n+1} = k_n(\sqrt{b_{n-1}b_n})$ for all $n \geq 1$. Then $K_{n+1} = K_n(\sqrt{b_{n-1}b_n})$. If $\sqrt{b_{n-1}} \in K_n$ for $n \geq 1$, then $K_{n+1} = K_n(\sqrt{b_n})$ and $\sqrt{b_n} \in K_{n+1}$. Since $\sqrt{b_0} \in K_1$, we obtain the claim by induction. □

Lemma 2.5. *K_{n+3}/k_n is a Galois extension for each $n \geq 0$.*

Proof. Recall that $-\frac{1}{b_{n+1}}$ is the conjugate of b_{n+1} over k_n. Then there exists $\tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/k_n)$ such that $b_{n+1}^\tau = -\frac{1}{b_{n+1}}$. Since k_{n+3}/k_{n+1} is a Galois extension, the conjugate of k_{n+3} over k_n different from k_{n+3} itself is $k_{n+3}^\tau = k(b_{n+3}^\tau)$. Therefore $k_{n+3}^\tau k_{n+3} = k_{n+3}(b_{n+3}^\tau)$ is a Galois extension of k_n. Since $\phi^2(b_{n+2}^\tau) = b_n$, we have $b_{n+2}^\tau \in \{b_{n+2}, -\frac{1}{b_{n+2}}, \frac{b_{n+2}+1}{b_{n+2}-1}, -\frac{b_{n+2}-1}{b_{n+2}+1}\}$ (see (2)). If b_{n+2}^τ is either b_{n+2} or $-\frac{1}{b_{n+2}}$, then $b_{n+1}^\tau = \phi(b_{n+2}^\tau) = b_{n+1}$, which implies a contradiction that $k_{n+1} \subset k_n$. Therefore $b_{n+2}^\tau = \frac{b_{n+2}+1}{b_{n+2}-1}$ or $b_{n+2}^\tau = -\frac{b_{n+2}-1}{b_{n+2}+1}$. Then $(b_{n+2}^\tau)^2 - 1 = \pm\frac{4b_{n+2}}{(b_{n+2}\mp 1)^2}$. Since $b_{n+3}^\tau = -i(b_{n+2}^\tau \pm \sqrt{(b_{n+2}^\tau)^2 - 1})$, $k_{n+3}^\tau k_{n+3} = k_{n+3}(\sqrt{b_{n+2}}) \subset K_{n+3}$ by Lemma 2.4. Since $[K_{n+3} : k_{n+3}] \leq 2$, we have $K_{n+3} = k_{n+3}^\tau k_{n+3}$ if $\sqrt{b_{n+2}} \notin k_{n+3}$. Suppose that $\sqrt{b_{n+2}} \in k_{n+3}$. Since $k_j(\sqrt{b_{j-1}b_j}) = k_{j+1} \subset k_{n+3}$ for any $n+2 \geq j \geq 1$, we have $\sqrt{b_{j-1}} \in k_{n+3}$ if $\sqrt{b_j} \in k_{n+3}$, and hence $\sqrt{b_0} \in k_{n+3}$ by induction. Then $K_{n+3} = k_{n+3} = k_{n+3}^\tau k_{n+3}$. Therefore K_{n+3}/k_n is a Galois extension. □

By Lemma 2.3, $k_{n+1}(\sqrt{b_{n+1}(b_{n+1}+1)})$ is a subextension of k_{n+3}/k_n of degree 4. Since

$$b_{n+1} = \frac{(\sqrt{b_{n+1}(b_{n+1}+1)})^2 - 1}{1 - 2b_n i},$$

one can easily see that the minimal polynomial of $\sqrt{b_{n+1}(b_{n+1}+1)}$ over k_n is

$$(3) \quad \begin{aligned} &x^4 + a_n x^2 + c_n \\ &\quad = x^4 + (4b_n^2 + 2b_n i - 2)x^2 + b_n(1+i)^2. \end{aligned}$$

Then

$$(4) \quad \begin{aligned} c_n(a_n^2 - 4c_n) &= 4b_n(b_n^2 - 1)(1+i)^2(2b_n + i)^2 \\ &\equiv b_n(b_n^2 - 1) \bmod (k_n^\times)^2. \end{aligned}$$

Lemma 2.6. *The following three statements are equivalent:*

(a) *$N_0 \neq \emptyset$.*
(b) *$1 \in N_0$, i.e., N_0 is the set of all positive rational integers.*
(c) *$\sqrt{b_0(b_0^2 - 1)} \in k$.*

Proof. (a) ⇒ (b): Put $n_0 = \min N_0$. Suppose that $n_0 \geq 3$. Then $K_{n_0} = k_{n_0}$ which is a Galois extension of k_{n_0-3} by Lemma 2.5. Since $\sqrt{b_0} \notin k_{n_0-1}$ and $\sqrt{b_0} \in k_{n_0}$, we have $k_{n_0-1} \cap K_{n_0-3} = k_{n_0-3}$ and $k_{n_0} = K_{n_0-1}$. Since k_{n_0-1}/k_{n_0-3} is a $[2,2]$-extension, k_{n_0}/k_{n_0-3} is a $[2,2,2]$-extension. In particular, $k_{n_0-2}(\sqrt{b_{n_0-2}(b_{n_0-2}+1)})/k_{n_0-3}$ is a $[2,2]$-extension. By (3), we have $\sqrt{c_{n_0-3}} \in k_{n_0-3}$ (see e.g. [10, Corollary 2.2.4]), i.e., $\sqrt{b_{n_0-3}} \in k_{n_0-3}$. This contradicts the validity of $C(b_{n_0-3})$ by Lemma 2.3. Therefore $n_0 \leq 2$ if $N_0 \neq \emptyset$. Suppose that $n_0 = 2$. Then $\sqrt{b_0} \in k_2$, and hence $k(\sqrt{b_0})/k$ is a quadratic subextension of the $[2,2]$-extension k_2/k. Since $\sqrt{b_0} \notin k_1$, i.e., $k(\sqrt{b_0}) \neq k_1$, we have either $k(\sqrt{b_0}) = k(\sqrt{b_0(b_0+1)})$ or $k(\sqrt{b_0}) = k(\sqrt{b_0(b_0-1)})$. Then $\sqrt{b_0+1} \in k$ or $\sqrt{b_0-1} \in k$. This contradicts to the condition $C(b_0)$. Thus we have $n_0 = 1 \in N_0$.

(b) ⇔ (c): We have $\sqrt{b_0} \in k_1$ if and only if $k(\sqrt{b_0}) = k(\sqrt{b_0^2 - 1})$, i.e., $\sqrt{b_0(b_0^2 - 1)} \in k$. □

By Lemma 2.6, we have $K_1 = k_1 = k_0(\sqrt{b_0}) \neq k_0$ if $N_0 \neq \emptyset$. Put

$$K_0 = \begin{cases} k_0 & \text{if } N_0 \neq \emptyset, \\ k_0(\sqrt{b_0}) & \text{if } N_0 = \emptyset. \end{cases}$$

Then $k_m \cap K_n = k_n$ and $K_m = k_m K_n$ for any $m \geq n \geq 0$. By Lemma 2.3, we obtain a diagram

$$\begin{tikzcd}
 & K_n^+ \arrow[dl, dash] \arrow[dr, dash] & K_{n+1}^+ \arrow[dl, dash] \arrow[dr, dash] & \\
K_n \arrow[r, dash] & K_{n+1} \arrow[r, dash] & K_{n+2} \arrow[r, dash] & K_{n+3} \\
 & K_n^- \arrow[ul, dash] \arrow[ur, dash] & K_{n+1}^- \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

for all $n \geq 0$, where $K_n^\pm = K_n(\sqrt{b_n(b_n \pm 1)})$.

Lemma 2.7. *The following two statements hold true:*

- *If $N_0 \neq \emptyset$, then k_{n+3}/k_n is a $[2,4]$-extension for each $n \geq 0$.*
- *If $N_0 = \emptyset$, then K_{n+3}/K_n is a $[2,4]$-extension for each $n \geq 1$, and*

$$K_3 = K_0\Big(\sqrt{b_0(b_0-1)}, \sqrt{(\sqrt{b_0}+1)(\sqrt{b_0}-i)}, \sqrt{(\sqrt{b_0}-1)(\sqrt{b_0}+i)}\Big).$$

Proof. By Lemmas 2.4 and 2.5, K_{n+3}/K_n is a Galois extension of degree 8 for each $n \geq 0$. Since $[K_{n+1}^+ : K_n] = 4$, the polynomial (3) is irreducible over K_n. If $n \geq 1$, $K_n(\sqrt{b_n^2 - 1}) = K_{n+1} = K_n(\sqrt{b_n})$ by Lemma 2.4, which implies that $\sqrt{b_n} \notin K_n$ and

$\sqrt{b_n(b_n^2-1)} \in K_n$. By Lemma 2.6, $\sqrt{b_0} \notin k = K_0$ and $\sqrt{b_0(b_0^2-1)} \in k_0 = K_0$ if $N_0 \neq \emptyset$. Hence $\sqrt{c_n} = (1+i)\sqrt{b_n} \notin K_n$ and $\sqrt{c_n(a_n^2-4c_n)} \in K_n$ for all $n \geq \delta$ (see (4)), where $\delta = 0$ if $N_0 \neq \emptyset$, and $\delta = 1$ if $N_0 = \emptyset$. Therefore K_{n+1}^+/K_n is a cyclic extension of degree 4 (see e.g. [10, Corollary 2.2.4]) if $n \geq \delta$. This implies that K_{n+3}/K_n is a $[2,4]$-extension for all $n \geq \delta$. In particular, we obtain the statement for $N_0 \neq \emptyset$. Suppose that $N_0 = \emptyset$. Then $x^4 + a_0x^2 + c_0$ is also the the minimal polynomial of $\sqrt{b_1(b_1+1)}$ over K_0. Recall that $b_1(b_1+1) = 1 - b_1(2b_0i-1)$. Since $\sqrt{c_0} = (1+i)\sqrt{b_0} \in K_0$, $K_1^+ = K_0(\sqrt{b_1(b_1+1)})$ is a $[2,2]$-extension of K_0 (see e.g. [10, Corollary 2.2.4]). Then the octic Galois extension K_3/K_0 contains two distinct $[2,2]$-extension K_1^+/K_0 and K_2/K_0, and hence $K_3 = K_0^-K_1^+$ is a $[2,2,2]$-extension of K_0. In fact, the four roots of $x^4 + a_0x^2 + c_0$ are

$$\begin{aligned}
&\pm \frac{i}{2}(\sqrt{a_0+2\sqrt{c_0}} \pm \sqrt{a_0-2\sqrt{c_0}}) \\
&\quad = \pm i\Bigg((\sqrt{b_0} + \tfrac{i-1}{2})\sqrt{(\sqrt{b_0}+1)(\sqrt{b_0}-i)} \\
&\qquad \pm (\sqrt{b_0} - \tfrac{i-1}{2})\sqrt{(\sqrt{b_0}-1)(\sqrt{b_0}+i)} \Bigg),
\end{aligned}$$

and hence $K_3 = K_0^-(\sqrt{a_0 \pm 2\sqrt{c_0}})$. Thus we obtain the statement for $N_0 = \emptyset$. □

2.3. Number theoretic part. We shall consider the ramification and the class number parity. We denote by $\mathcal{O}_F$ the ring of integers in a number field F, and by $\mathcal{O}_F^\times$ its unit group.

Lemma 2.8. *If $b_0 \in \mathcal{O}_k$, then;*

- *k_1/k is unramified outside primes dividing $2(b_0^2-1)$.*
- *k_2/k_1 is unramified outside primes dividing $2b_0$.*
- *k_n/k_2 is unramified outside 2 for any $n \geq 3$.*

Proof. Recall that

$$b_n^2 + 2b_{n-1}ib_n - 1 = 0$$

for all $n \geq 1$. Then $b_n \in \mathcal{O}_{k_n}^\times$ if $b_{n-1} \in \mathcal{O}_{k_{n-1}}$. Therefore $b_n \in \mathcal{O}_{k_n}^\times$ for all $n \geq 1$ if $b_0 \in \mathcal{O}_k$. Since

$$k_{n+1} = k_n(\sqrt{b_n^2-1}) = k_n(\sqrt{b_{n-1}b_n}),$$

we obtain the statements. □

Lemma 2.9. *Assume that $b_0 \in \mathcal{O}_k$. Then the following two statements hold true:*

- *If $N_0 \neq \emptyset$, then k_n/k is unramified outside 2 for any $n \geq 0$.*
- *If $N_0 = \emptyset$, then K_n/K_1 is unramified outside 2 for any $n \geq 1$, and K_1/K_0 is unramified outside primes dividing $2(b_0^2-1)$.*

Proof. Since K_4/K_1 is a $[2,4]$-extension by Lemma 2.7, K_2^+/K_1 is a cyclic extension of degree 4, which is unramified outside $2b_0$ by Lemma 2.8. Since K_2^+/K_2 is unramified outside 2 by Lemma 2.8, any prime v not dividing 2 does not ramify in K_2^+/K_1. Hence K_2/K_1 is unramified outside 2. By Lemma 2.8, K_n/K_1 is unramified outside 2 for any $n \geq 1$. If $N_0 = \emptyset$, then $k_1 \cap K_0 = k$ and $K_1 = k_1K_0$. Hence we obtain the statement for $N_0 = \emptyset$. Suppose that $N_0 \neq \emptyset$. Then $k_1 = k(\sqrt{b_0^2-1}) = k(\sqrt{b_0})$ by Lemma 2.6, and hence k_1/k is unramified outside $2(b_0^2-1)$ and unramified outside $2b_0$. Since $\mathcal{O}_k(b_0^2-1) + \mathcal{O}_kb_0 = \mathcal{O}_k$, k_1/k is unramified outside 2. Thus we obtain the statement for $N_0 \neq \emptyset$. □

We need the following result, which is a part of [17, Theorem 2.1] or [13, Proposition 1].

Proposition 2.10. *Let S be a finite set of primes of a subfield of a number field K, and let T be a subset of S. Let K''/K be a cyclic quartic extension, which is unramified outside S and totally ramified at any primes lying over S. Let K'/K be the unique quadratic subextension of K''/K. If $2 \nmid |Cl^T(K')|$, then $2 \nmid |Cl^T(K'')|$.*

Suppose that $b_0 \in \mathcal{O}_k$. By Lemmas 2.7 and 2.9, K_{n+3}/K_n is a $[2,4]$-extension unramified outside 2 for any $n \geq \delta$, where $\delta = 0$ if $N_0 \neq \emptyset$, and $\delta = 1$ if $N_0 = \emptyset$.

Lemma 2.11. *Suppose that $n \geq \delta$. Assume that K_{n+2}/K_n is totally ramified at any primes lying over 2 and $2 \nmid |Cl^T(K_{n+2})|$. Then K_{n+3}/K_{n+1} is totally ramified at any primes lying over 2 and $2 \nmid |Cl^T(K_{n+3})|$.*

Proof. Since K_{n+2}/K_n^+ is ramified at any primes $v|2$, the cyclic quartic extension K_{n+3}/K_n^+ is totally ramified at any $v|2$. Hence K_{n+3}/K_{n+1} is totally ramified at any primes lying over 2. Since $2 \nmid |Cl^T(K_{n+2})|$, we have $2 \nmid |Cl^T(K_{n+3})|$ by Proposition 2.10 for the cyclic quartic extension K_{n+3}/K_n^+. □

Suppose that $n \geq \delta$. By using Lemma 2.11 recursively, we see that $2 \nmid |Cl^T(K_m)|$ for any $m \geq n$ if K_{n+2}/K_n is totally ramified at any primes lying over 2 and $2 \nmid |Cl^T(K_{n+2})|$. By combining Lemmas 2.6, 2.7, 2.9 and this fact, the proof of Theorem 1.1 is completed.

3. Examples. The following result by Iwasawa ([8]) is also useful to find examples.

Proposition 3.1. *Let K'/K be a quadratic extension ramified at only one prime v. Put $T = \emptyset$ or $T = \{v\}$. If $2 \nmid |Cl^T(K)|$, then $2 \nmid |Cl^T(K')|$.*

Suppose that ϕ is defined as (1).

Example 3.2. Put $b_0 = \pm i$, and put $k = \mathbf{Q}(i)$. Since $b_0(b_0^2 - 1) = \pm(1+i)^2$, we have $\sqrt{b_0(b_0^2-1)} \in k$. Then

$$k_2 = \mathbf{Q}(i, b_2) = \mathbf{Q}(i, \sqrt{b_0}, \sqrt{b_0+1}) = \mathbf{Q}(\zeta_8, \sqrt{1+i})$$

is a $[2,2]$-extension of $k = \mathbf{Q}(i)$ which is unramified outside 2 and totally ramified at $1+i$. Hence the condition $C(b_0)$ is satisfied (see Remark 1.2). By Lemma 2.7, k_{n+3}/k_n is a $[2,4]$-extension unramified outside $1+i$ for any $n \geq 0$. By applying Proposition 3.1 for k_n/k_{n-1} recursively, we see that k_∞/k is totally ramified at $1+i$, and that $2 \nmid |Cl(k_n)|$ for any $n \geq 0$.

Remark 3.3. Note that

$$-i\phi(ix) = \frac{i}{2}\left(x + \frac{1}{x}\right) = -(1+i)^{-2}\left(x + \frac{1}{x}\right)$$

is a PGL_2-conjugate of ϕ. Put $\Phi(x) = i\phi(ix)$. Then $\Phi(x)$ is the x-coordinate of the endomorphism $[1+i]$ of the elliptic curve $E : y^2 = x^3 + x$ with complex multiplication by $\mathbf{Z}[i]$ and the j-invariant 1728 (see [16, p. 111, Proposition 2.3.1]). Since

$$\begin{aligned}\Phi^n(x) &= (-1)^n(-\Phi)^n(x) = (-1)^n(-i\phi i)^n(x)\\ &= (-1)^{n+1} i\phi^n(ix),\end{aligned}$$

we have $(-1)^{n+1} i\phi^{-n}(b_0) = \Phi^{-n}(ib_0)$, and hence $k(\phi^{-n}(b_0)) = k(\Phi^{-n}(ib_0))$. Since $\Phi^{-3}(\infty) = \{\pm 1, \pm i\}$ and $\Phi(\pm 1) = \pm i$, we have $\Phi^{-n-3}(\infty) = \Phi^{-n}(\pm 1) \cup \Phi^{-n+1}(\pm 1)$. If $b_0 = \mp i$ as in Example 3.2, then

$$k(\phi^{-n}(b_0)) = k(\Phi^{-n}(\pm 1)) = k(\Phi^{-n-3}(\infty))$$

contains the ray class field $\mathbf{Q}(i)(\xi^2 | \xi \in \Phi^{-n-3}(\infty))$ of $\mathbf{Q}(i)$ modulo $(1+i)^{n+3}$ (see [16, p. 135, Theorem 5.6]).

Example 3.4. Put $b_0 = \pm i$, and put $k = \mathbf{Q}(i, \sqrt{q})$ with an odd prime number q. By Proposition 3.1, the class number of $\mathbf{Q}(\sqrt{q^*})$ is odd, where $q^* = (-1)^{\frac{q-1}{2}} q \equiv 1 \pmod 4$. By Example 3.2, the conditions $\sqrt{b_0(b_0^2-1)} \in k$ and $C(b_0)$ are satisfied (see Remark 1.2), and k_{n+3}/k_n is a $[2,4]$-extension unramified outside 2 and totally ramified at any primes lying over 2 for any $n \geq 0$.

If $q^* \equiv 5 \pmod 8$, then 2 does not split in $k/\mathbf{Q}$. By Proposition 3.1 for $k/\mathbf{Q}(\sqrt{q^*})$, the class number of k is odd. By applying Proposition 3.1 for k_n/k_{n-1} recursively, we see that $2 \nmid |Cl(k_n)|$ for any $n \geq 0$.

Put $T = \{2\}$. By using PARI/GP ([14]), one can see that $2 \nmid |Cl^T(k_2)|$ if $q \equiv 7 \pmod{16}$ and $q < 100$ (i.e., $q \in \{7, 23, 71\}$). Then k has two primes lying over 2. By Lemma 2.11, $2 \nmid |Cl^T(k_n)|$ for any $n \geq 0$.

```
? TClassGroup(bnf)={local(P,g);
print1(bnf.clgp[2]);P=idealprimedec(bnf,2);
for(g=1,matsize(P)[2],
print1([bnfisprincipal(bnf,P[g])[1],
P[g][3], /* ramification index */
P[g][4]  /* residue degree     */ ]))};
? k0=bnfinit(y^4+900,1);
? i=Mod(y^2/(-30),y^4+900);b0=3*i;
? if(bnfcertify(k0)==1,TClassGroup(k0));
[2][[1]~, 2, 1][[1]~, 2, 1]
? phi=(i/2)*(x-1/x);
? f2=numerator(subst(phi,x,phi)-b0);
? k2=rnfinit(k0,lift(f2/polcoeff(f2,4)));
? k2=bnfinit(k2.polabs,1);
? if(bnfcertify(k2)==1,TClassGroup(k2));
[4][[3]~, 8, 1][[3]~, 8, 1]
```

Fig. 1. PARI/GP for Example 3.5.

Example 3.5. Put $b_0 = 3i$ and $k = \mathbf{Q}(i, \sqrt{b_0(b_0^2-1)}) = \mathbf{Q}(\sqrt{-30i}) = \mathbf{Q}(i, \sqrt{15})$. Then we obtain the following results by using PARI/GP ([14]): The condition $C(b_0)$ is satisfied (see Remark 1.2), and the prime $1+i$ of $\mathbf{Q}(i)$ splits in $k/\mathbf{Q}(i)$. Moreover, k_2/k is totally ramified at the two primes of k, and $2 \nmid |Cl^T(k_2)|$ for $T = \{2\}$ (see Figure 1). By Lemma 2.11, $2 \nmid |Cl^T(k_n)|$ for any $n \geq 0$.

On the other hand, suppose that $b_0 = 2 - i$ and $k = \mathbf{Q}(i, \sqrt{b_0(b_0^2-1)}) = \mathbf{Q}(i, \sqrt{5})$. As seen in Example 3.4, the class number of k is odd, and 2 does not split in $k/\mathbf{Q}$. Then $2 \nmid |Cl(k_n)|$ for all $n \geq 0$, by Lemma 2.9 and the recursive use of Proposition 3.1.

Example 3.6. Put $k = \mathbf{Q}(i)$. For $b_0 \in \{3i, 2-i, 1+4i, 6-i, 3+2i\}$, we obtain the following results by using PARI/GP ([14]): The condition $C(b_0)$ is satisfied and $\sqrt{b_0(b_0^2-1)} \notin k$.

If $b_0 = 3i$, $K_0/\mathbf{Q}$ is totally ramified at 2, and the unique prime of K_0 lying over 2 splits in K_1/K_0. Moreover, assuming GRH, K_3/K_1 is totally ramified at any primes lying over 2, and $2 \nmid |Cl^T(K_3)|$ for $T = \{2\}$. By Theorem 1.1, $2 \nmid |Cl^T(K_n)|$ for any $n \geq 1$ under GRH.

If $b_0 \in \{2-i, 1+4i, 6-i\}$, 2 does not split in $K_1/\mathbf{Q}$ and $|Cl(K_1)| = 1$. If $b_0 = 3+2i$, then 2 does not split in $K_2/\mathbf{Q}$, $|Cl(K_1)| = 2$ and $|Cl(K_2)| = 1$. By Lemma 2.9 and the recursive use of Proposition 3.1, we see that the class number of K_n is odd for any $n \geq 2$.

Remark 3.7. We have not yet found any example of b_0 and k such that $2 \nmid |Cl(K_n)|$ and K_n has at least two ramified primes lying over 2 for all sufficiently large $n \geq \delta$.

Acknowledgements. The authors thank the referees for helpful comments for the improvement of this paper. This work was supported by JSPS KAKENHI Grant Number JP17K05167.

References

[1] W. Aitken, F. Hajir and C. Maire, Finitely ramified iterated extensions, Int. Math. Res. Not. **2005**, no. 14, 855–880.

[2] N. Boston and R. Jones, The image of an arboreal Galois representation, Pure Appl. Math. Q. **5** (2009), no. 1, 213–225.

[3] M. R. Bush, W. Hindes and N. R. Looper, Galois groups of iterates of some unicritical polynomials, Acta Arith. **181** (2017), no. 1, 57–73.

[4] L. Caputo and F. A. E. Nuccio Mortarino Majno di Capriglio, On fake $\mathbf{Z}_p$-extensions of number fields, arXiv:0807.1135.

[5] J. Cullinan and F. Hajir, Ramification in iterated towers for rational functions, Manuscripta Math. **137** (2012), no. 3–4, 273–286.

[6] A. A. Cuoco and P. Monsky, Class numbers in $\mathbf{Z}_p^d$-extensions, Math. Ann. **255** (1981), no. 2, 235–258.

[7] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98** (1976), no. 1, 263–284.

[8] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[9] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[10] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials*: *Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, 45, Cambridge University Press, Cambridge, 2002.

[11] T. Kataoka, An Iwasawa theory for non-Galois extension fields, RIMS Kôkyûroku **658** (1988), 34–42 (in Japanese).

[12] A. Lei, Estimating class numbers over metabelian extensions, Acta Arith. **180** (2017), no. 4, 347–364.

[13] Y. Mizusawa and K. Yamamoto, On 2-adic Lie iterated extensions of number fields arising from a Joukowski map. (to appaer in Tokyo J. Math.).

[14] The PARI Group, PARI/GP version 2.7.4, Univ. Bordeaux, 2015. `http://pari.math.u-bordeaux.fr/`

[15] G. Perbet, Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques, Algebra Number Theory **5** (2011), no. 6, 819–848.

[16] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.

[17] K. Yamamoto, On iterated extensions of number fields arising from quadratic polynomial maps, J. Number Theory **209** (2020), 289–311.