J. Korean Soc. Math. Educ. Ser. B: Pure Appl. Math. ISSN 1226-0657
Volume 16, Number 3 (August 2009), Pages 283–296

ON THE GALOIS GROUP OF ITERATE POLYNOMIALS

EUNMI CHOI

ABSTRACT. Let $f(x) = x^n + a$ be a binomial polynomial in $\mathbb{Z}[x]$ and $f_m(x)$ be the m-th iterate of $f(x)$. In this work we study a necessary condition to be the Galois group of $f_m(x)$ is isomorphic to a wreath product group $[C_n]^m$ where C_n is a cyclic group of order n.

1. INTRODUCTION

Let $f(x)$ be a polynomial and $f_m(x)$ be the m-th iterate of $f(x)$, such that

$$f_1(x) = f(x) \text{ and } f_m(x) = f \circ \cdots \circ f(x) = f(f_{m-1}(x)).$$

A study of Galois theory has a long history that usually concerns about the problem of determining Galois group with single polynomial. During last 2 decades the theory has been extended investigating the Galois group with composition and iteration of polynomials (see [1], [2], [4], [6], [7] and [9]). While the Galois group of iterate polynomial is generally embedded into a wreath product of groups, some research papers were devoted to investigating necessary conditions to be the Galois group itself is isomorphic to wreath product. Odoni [7] studied a binomial polynomial $f(x) = x^2 + 1$ to find a standard that the Galois group $\mathrm{Gal}(f_m/\mathbb{Q})$ is isomorphic to the m-fold wreath product $[C_2]^m$ of the cyclic group C_2 of order 2. Stoll [9] dealt with a more general polynomial $f(x) = x^2 - a \in \mathbb{Z}[x]$ where $a \notin \mathbb{Z}^2$, and proved that $\mathrm{Gal}(f_m/\mathbb{Q}) \cong [C_2]^m$ if a satisfies either ($a > 0$ and $a \equiv 1 \pmod 4$), or ($a > 0$ and $a \equiv 2 \pmod 4$), or ($a < 0$ and $a \equiv 0 \pmod 4$).

The purpose of this work is to study the Galois group of iterate of fourth degree binomial polynomial $f(x) = x^4 + a$ over $\mathbb{Q}$. We will investigate situations to be $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_4)) \cong [C_4]^m$, and provide criterions for the integer a.

Received by the editors December 18, 2008. Revised July 1, 2009. Accepted July 9, 2009.
2000 *Mathematics Subject Classification.* 11D09, 12F10, 20B05.
Key words and phrases. iterated polynomial, Galois group, wreath product group.

In this paper, ε_k denotes a primitive k-th root of unity, and C_k the cyclic group of order k. For any domain D, let $D^* = D - \{0\}$ and $D^p = \{d^p \mid d \in D\}$ $(p > 0)$. When $p^e|m$ and $p^{e+1} \not| m$, we write $p^e||m$ and $e = v_p(m)$.

2. INDEPENDENCY IN A FIELD K

Let G and H be permutation groups on nonempty disjoint finite sets A and B respectively. Let H^A be the group of all functions $\{\theta : A \to H\}$ with the canonical multiplication rule. For any $g \in G$ and $\theta \in H^A$, define a map on $A \times B$ by

$$[g,\theta] : A \times B \to A \times B, \quad (a,b) \mapsto (g(a), \theta(a)(b)) \quad \text{for } a \in A,\ b \in B.$$

Then $[g,\theta] \in Sym(A \times B)$, and $[g,\theta]$'s form a subgroup $G[H]$ of $Sym(A \times B)$ under the operation $([g,\theta][g_1,\theta_1])(a,b) = \big(g(g_1(a)),\ \theta(g_1(a))(\theta_1(a)(b))\big)$. This group is called the wreath of G by H of order $|G|\ |H|^{\deg |G|}$.

Proposition 1. *Let $[C_n]^m = [C_n[C_n[\cdots[C_n]\cdots]]]$ be the m-fold wreath product of C_n. Then $|[C_n]^m| = n^{n^{m-1}+n^{m-2}+\cdots+n+1}$ and the maximal abelian subgroup $([C_n]^m)^{\mathrm{ab}}$ of $[C_n]^m$ is equal to C_n^m.*

Proof. When $m = 2$, $\big|[C_n]^2\big| = |C_n[C_n]| = |C_n|\ |C_n|^n = n \cdot n^n = n^{n+1}$. Suppose that $\big|[C_n]^{m-1}\big| = n^{n^{m-2}+n^{m-3}+\cdots+n+1}$. Then

$$\begin{aligned} |[C_n]^m| &= \big|C_n[C_n]^{m-1}\big| = |C_n|\ \big|[C_n]^{m-1}\big|^n \\ &= n \cdot n^{n^{m-1}+n^{m-2}+\cdots+n^2+n} = n^{n^{m-1}+n^{m-2}+\cdots+n^2+n+1}. \end{aligned}$$

And $([C_n]^2)^{\mathrm{ab}} = (C_n[C_n])^{\mathrm{ab}} = C_n^{\mathrm{ab}} \times C_n^{\mathrm{ab}} = C_n \times C_n$. Hence $([C_n]^m)^{\mathrm{ab}} = C_n \times \cdots \times C_n$ follow immediately. □

A relation between the Galois and the wreath product groups is as follows.

Proposition 2. *Let K be a field of characteristic 0 and $n = p^u$ (p prime). If $f(x) = x^n - a \in K(\varepsilon_n)[x]$ and all $f_m(x)$ are irreducible in $K(\varepsilon_n)$ then*

(1) Gal $(f_{m+1}/K(\varepsilon_n)) \cong [C_n]^{m+1}$ *if and only if* $\mathrm{Gal}(f_m/K(\varepsilon_n)) \cong [C_n]^m$ *and* $[E_{m+1} : E_m] = n^{n^m}$ *where E_m is the splitting field of f_m.*

(2) *If* Gal $(f_m/K(\varepsilon_n)) \cong [C_n]^m$ *then the maximal Kummer extension of $K(\varepsilon_n)$ in E_m is of degree n^m.*

Proof. (1) is mostly due to [3], [7] and [9]. If $\mathrm{Gal}(f_m/K(\varepsilon_n)) \cong [C_n]^m$ then $(\mathrm{Gal}(f_m/K(\varepsilon_n)))^{\mathrm{ab}} \cong ([C_n]^m)^{\mathrm{ab}} = C_n^m$ is of order n^m. So (2) is obvious.

In case (1), the order of Galois group can be calculated explicitly that

$$|\mathrm{Gal}(f_{m+1}/K(\varepsilon_n))| = n^{n^m+n^{m-1}+\cdots+n+1} = [E_{m+1} : E_m]\ |\mathrm{Gal}(f_m/K(\varepsilon_n))|.$$

Let $d_1, \cdots, d_r$ be elements in K^* of characteristic 0, and p be a prime. When $\prod_{i=1}^r d_i^{a_i} \in K^{p^u}$ with $a_i > 0$, if p^u divides every a_i $(1 \le i \le r)$ then $d_1, \cdots, d_r$ are said to be p^u-independent in K (see [5, 4.2.2]).

Proposition 3. *Let $d_1, \cdots, d_r \in K^*$. The following are equivalent:*

(1) *$d_1, \cdots, d_r$ are p^u-independent in K.*

(2) *$\prod_{i=1}^r d_i^{a_i} \equiv 0$ in $K^*/(K^*)^{p^u}$ implies $d_i^{a_i} \equiv 0$ in $K^*/(K^*)^{p^u}$ for all i.*

(3) *$d_1, \cdots, d_r$ are independent by mod $(K^*)^{p^u}$.*

(4) *The residue classes of $d_1, \cdots, d_r$ in $K^*/(K^*)^{p^u}$ are linearly independent.*

(5) *$[K^{p^u}(d_1, \cdots, d_r) : K^{p^u}] = (p^u)^r$.*

(6) *$K^{p^u} \subsetneq K^{p^u}(d_1) \subsetneq \cdots \subsetneq K^{p^u}(d_1, \cdots, d_r)$ is a strictly increasing tower.*

(7) *$\prod_{i=1}^r d_i^{a_i}$ $(0 \le a_i < p^u)$ form a vector basis for $K^{p^u}(d_1, \cdots, d_r)$ over K^{p^u}.*

Proof. The equivalence of (1), ..., (5) are obvious.

(5) $\Rightarrow$ (6). Since $d_j^{p^u} \in K^{p^u}$, $[K^{p^u}(d_1, \cdots, d_{j+1}) : K^{p^u}(d_1, \cdots, d_j)] \le p^u$. If (6) is not strictly increasing then $K^{p^u}(d_1, \cdots, d_{j+1}) = K^{p^u}(d_1, \cdots, d_j)$ for some j would yield $[K^{p^u}(d_1, \cdots, d_r) : K^{p^u}] < (p^u)^r$.

(6) $\Rightarrow$ (7). Since $K^{p^u} \subsetneq K^{p^u}(d_1)$ is strictly increasing, $d_1 \notin K^{p^u}$ so $X^{p^u} - d_1 = 0$ is not solvable in K^{p^u}. Thus $1, d_1, d_1^2, \cdots, d_1^{p^u-1}$ is a basis for $K^{p^u}(d_1)$ over K^{p^u}. It is not hard to see that each tower step $K^{p^u} \subsetneq K^{p^u}(d_1) \subsetneq \cdots \subsetneq K^{p^u}(d_1, \cdots, d_r)$ has basis $\{1, d_1, \cdots, d_1^{p^u-1}\}$, $\cdots$, $\{1, d_r, \cdots, d_r^{p^u-1}\}$, respectively. Thus the set $\{d_1^{a_1} \cdots d_r^{a_r} \mid 0 \le a_j \le p^{u-1};\ 1 \le j \le r\}$ of all product elements from each basis forms a K^{p^u}-vector space basis for $K^{p^u}(d_1, \cdots, d_r)$ over K^{p^u}.

(7) $\Rightarrow$ (5). There are $(p^u)^r$ monomial elements $\prod_{i=1}^r d_i^{a_i}$ $(0 \le a_i < p^u)$ in $K^{p^u}(d_1, \cdots, d_r)$, thus the K^{p^u}-vector space basis is of $(p^u)^r$-elements. □

The p-independence can be generalized to any n-independence that, $d_1, \cdots, d_r \in K^*$ are n-independent in K if $\prod_{i=1}^r d_i^{a_i} \in K^n$ implies $n|\ a_i$ for all $i = 1, \cdots, r$.

Proposition 4. *Let $n = p_1^{u_1} \cdots p_k^{u_k}$ and $\varepsilon_n \in K$. The following are equivalent.*

(1) *$d_1, \cdots, d_r$ are n-independent in K.*

(2) *$d_1, \cdots, d_r$ are $p_j^{u_j}$-independent in K for all $j = 1, \cdots, k$.*

(3) *$d_1, \cdots, d_r$ are p_j-independent in K for all $j = 1, \cdots, k$.*

Proof. For (1) $\Leftrightarrow$ (2), write $n = p_j^{u_j} n_j'$ such that $\gcd(p_j, n_j') = 1$ for $1 \le j \le k$. We assume $\prod_{i=1}^{r} d_i^{a_i} \in K^{p_j^{u_j}}$. Then

$$\left(\prod_{i=1}^{r} d_i^{a_i}\right)^{n'_j} \in K^{p_j^{u_j} n'_j} = K^n$$

and it thus follows from (1) that $n|\ a_i n'_j$, i.e., $p_j^{u_j} |\ a_i$ for all $1 \le i \le r$, so $d_1, \cdots, d_r$ are $p_j^{u_j}$-independent for $j = 1, \cdots, k$. On the other hand, suppose that $\prod_{i=1}^{r} d_i^{a_i} \in K^n$. Then there is $\theta \in K$ such that

$$\prod_{i=1}^{r} d_i^{a_i} = \theta^n = (\theta^{n'_j})^{p_j^{u_j}} \in K^{p_j^{u_j}} \text{ for } 1 \le j \le k.$$

From (2) we have $p_j^{u_j}\ |a_i$ for $1 \le i \le r$, $1 \le j \le k$, thus by employing the fact (if $x|a$, $y|a$ and $\gcd(x, y) = 1$ then $xy|a$), it follows $p_1^{u_1} \cdots p_k^{u_k}\ |a_i$, i.e., $n|\ a_i$ for all i.

For (2) $\Leftrightarrow$ (3), if $\prod_{i=1}^{r} d_i^{a_i} \in K^{p_j}$ then $\prod_{i=1}^{r}(d_i)^{a_i p_j{}^{u_j-1}} \in (K^{p_j})^{p_j{}^{u_j-1}} = K^{p_j{}^{u_j}}$. If $d_1, \cdots, d_r$ are $p_j{}^{u_j}$-independent then $p_j{}^{u_j}$ divides every $a_i p_j{}^{u_j-1}$, i.e., $p_j|\ a_i$ for all i. Conversely suppose that $\prod_{i=1}^{r} d_i^{a_i} \in K^{p_j{}^{u_j}}$. Since $K^{p_j{}^{u_j}} \subseteq K^{p_j}$, $\prod_{i=1}^{r} d_i^{a_i}$ belongs to K^{p_j}, thus due to assumption we have $p_j|a_i$, i.e. $a_i = p_j\ \lambda_{1,i}$ for some $\lambda_{1,i} \in \mathbb{Z}$ and for all $1 \le i \le r$. Hence we may write

$$\left(\prod_{i=1}^{r} d_i^{\lambda_{1,i}}\right)^{p_j} = \prod_{i=1}^{r} d_i^{p_j \lambda_{1,i}} = \theta^{p_j{}^{u_j}} = (\theta^{p_j{}^{u_j-1}})^{p_j}$$

for some $\theta \in K$. Since $\varepsilon_{p_j{}^{u_j}} \in K$, we can have a 1-step reduced form that

$$\prod_{i=1}^{r} d_i^{\lambda_{1,i}} = \theta^{p_j{}^{u_j-1}} \in K^{p_j{}^{u_j-1}}$$

Again since $K^{p_j{}^{u_j-1}} \subseteq K^{p_j}$, we have $\prod_{i=1}^{r} d_i^{\lambda_{1,i}} \in K^{p_j}$, so $p_j|\lambda_{1,i}$, i.e. $\lambda_{1,i} = p_j\ \lambda_{2,i}$ for $\lambda_{2,i} \in \mathbb{Z}$, $1 \le i \le r$. Thus

$$\left(\prod_{i=1}^{r} d_i^{\lambda_{2,i}}\right)^{p_j} = \prod_{i=1}^{r} d_i^{p_j \lambda_{2,i}} = \theta^{p_j{}^{u_j-1}} = (\theta^{p_j{}^{u_j-2}})^{p_j},$$

so it follows the 2-step reduced form that

$$\prod_{i=1}^{r} d_i^{\lambda_{2,i}} = \theta^{p_j{}^{u_j-2}} \in K^{p_j{}^{u_j-2}} \subset K^{p_j}.$$

Hence the p_j-independence of $d_1, \cdots, d_r$ implies that $p_j|\lambda_{2,i}$, i.e. $\lambda_{2,i} = p_j\ \lambda_{3,i}$ for $\lambda_{3,i} \in \mathbb{Z}$, $1 \le i \le r$. Continuing this process until we get

$$\prod_{i=1}^{r} d_i^{\lambda_{u_j-1,i}} = \theta^{p_j} \in K^{p_j},$$

so the p_j-independence yields $p_j | \lambda_{u_j-1,i}$, i.e. $\lambda_{u_j-1,i} = p_j \lambda_{u_j,i}$ for $\lambda_{u_j,i} \in \mathbb{Z}$, $1 \le i \le r$. We therefore conclude that ${p_j}^{u_j}$ divides every a_i, because

$$a_i = p_j \cdot \lambda_{1,i} = {p_j}^2 \cdot \lambda_{2,i} = \cdots = {p_j}^{u_j} \cdot \lambda_{u_j,i} \text{ for all } i.$$

□

3. Iterations of Polynomials

For a binomial polynomial $f(x) = x^n + a \in \mathbb{Z}[x]$, let

$$b_1 = f(0) \text{ and } b_m = f(b_{m-1}) \text{ for all } m > 1$$

and, by means of Möbius function μ we let

$$c_m = \prod_{d|m} b_d^{\mu(m/d)} \text{ for all } m > 0.$$

Since $b_1 = f(0)$, $b_2 = f(b_1) = f(f(0)) = f_2(0)$ and $b_m = f(b_m) = f_2(b_{m-2}) = \cdots = f_{m-1}(b_1) = f_m(0)$ for all m, i.e., b_m is the constant term of $f_m(x)$.

In next proposition, we develop an explicit formula of c_m for next use.

Proposition 5. *If $m = q_1^{k_1} \cdots q_t^{k_t}$ $(k_i \ge 1)$ is a prime factorization then*

$$c_m = \frac{(b_m)\ (\prod_{i_1,i_2} b_{m/q_{i_1}q_{i_2}})(\prod_{i_1,i_2,i_3,i_4} b_{m/q_{i_1}q_{i_2}q_{i_3}q_{i_4}})\cdots}{(\prod_{i_1} b_{m/q_{i_1}})\ (\prod_{i_1,i_2,i_3} b_{m/q_{i_1}q_{i_2}q_{i_3}})(\prod_{i_1,i_2,i_3,i_4,i_5} b_{m/q_{i_1}q_{i_2}q_{i_3}q_{i_4}q_{i_5}})\cdots}$$

where each product runs over all different $1 \le i_j \le t$ that q_{i_j} is a prime factor of m. Moreover the number of product terms in nominator of c_m equals that in denominator, which is equal to $(\sum_{i=0}^{t} {}_tC_i)/2$ where ${}_tC_i = t!/i!(t-i)!$.

Proof. Recall that $\mu(n) = 0$ if n has a square divisor. And $\mu(n) = 1$ (or, -1) if n is square free with even (or, odd) number of prime divisors.

(i) If $m = q^k$ $(k \ge 1)$ then $c_m = \frac{b_m}{b_{m/q}} = \frac{b_{q^k}}{b_{q^{k-1}}}$.

(ii) When $m = q_1^{k_1} q_2^{k_2}$, there are $(k_1+1)(k_2+1)$ divisors of m, so

$$c_m = \prod_{d|m} b_d^{\mu(m/d)} = \prod_{i,j} b_{q_1^i q_2^j}^{\mu(q_1^{k_1-i} q_2^{k_2-j})} \quad \text{for} \quad 0 \le i \le k_1,\ 0 \le j \le k_2.$$

If either $k_1 - i \ge 2$ or $k_2 - j \ge 2$ then $\mu(q_1^{k_1-i} q_2^{k_2-j}) = 0$. Hence there are only 4 cases to be considered with nontrivial Möbius value :

(k_1-i, k_2-j)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
(i,j)	(k_1,k_2)	(k_1-1,k_2)	(k_1,k_2-1)	(k_1-1,k_2-1)

Thus

$$c_m = \frac{b_{q_1^{k_1}q_2^{k_2}} \cdot b_{q_1^{k_1-1}q_2^{k_2-1}}}{b_{q_1^{k_1-1}q_2^{k_2}} \cdot b_{q_1^{k_1}q_2^{k_2-1}}} = \frac{b_m \cdot b_{m/q_1q_2}}{b_{m/q_1} \cdot b_{m/q_2}}.$$

(iii) When $m = q_1^{k_1}q_2^{k_2}q_3^{k_3}$ ($k_i \geq 1$), in the form of c_m there are 8 possible (i,j,t)'s having nontrivial Möbius value $\mu(q_1^{k_1-i}q_2^{k_2-j}q_3^{k_3-t})$:

(k_1-i, k_2-j, k_3-t)	(i,j,t)	$b_{q_1^iq_2^jq_3^t}^{\mu(q_1^{k_1-i}q_2^{k_2-j}q_3^{k_3-t})}$
$(0,0,0)$	(k_1,k_2,k_3)	b_m
$(1,0,0)$	(k_1-1,k_2,k_3)	b_{m/q_1}^{-1}
$(0,1,0)$	(k_1,k_2-1,k_3)	b_{m/q_2}^{-1}
$(0,0,1)$	(k_1,k_2,k_3-1)	b_{m/q_3}^{-1}
$(1,1,0)$	(k_1-1,k_2-1,k_3)	b_{m/q_1q_2}
$(1,0,1)$	(k_1-1,k_2,k_3-1)	b_{m/q_1q_3}
$(0,1,1)$	(k_1,k_2-1,k_3-1)	b_{m/q_2q_3}
$(1,1,1)$	(k_1-1,k_2-1,k_3-1)	$b_{m/q_1q_2q_3}^{-1}$

Thus

$$c_m = \frac{b_m \cdot b_{m/q_1q_2} \cdot b_{m/q_1q_3} \cdot b_{m/q_2q_3}}{b_{m/q_1} \cdot b_{m/q_2} \cdot b_{m/q_3} \cdot b_{m/q_1q_2q_3}}.$$

(iv) In general if $m = q_1^{k_1}\cdots q_t^{k_t}$, there are $(k_1+1)\cdots(k_t+1)$ divisors d of m, and the number l of d's having $\mu(d) \neq 0$ is $l = \sum_{s=0}^{t} {}_tC_s$ due to the next table:

$(k_1-i_1,\cdots,k_t-i_t)$	#of the type	$b_{q_1^{k_1}q_2^{k_2}\cdots q_t^{k_t}}^{\mu(q_1^{k_1-i_1}q_2^{k_2-i_2}\cdots q_t^{k_t-i_t})}$
$(0,0,\cdots,0)$	${}_tC_0$	b_m
$(0,\cdots,1,\cdots,0)$	${}_tC_1$	b_{m/q_j}^{-1}
$(1,1,0,\cdots,0)$	${}_tC_2$	b_{m/q_1q_2}
$(1,1,1,0,\cdots,0)$	${}_tC_3$	$b_{m/q_1q_2q_3}^{-1}$
$\cdots$	$\cdots$	$\cdots$
$(1,1,\cdots,1)$	${}_tC_t$	$b_{m/q_1q_2\cdots q_t}^{\pm 1}$

Clearly l is always even, since $l = 2\sum_{s=0}^{(t-1)/2} {}_tC_s$ if t is odd while $l = 2\sum_{s=0}^{(t/2)-1} {}_tC_s + {}_tC_{t/2}$ if t is even. Moreover the number of d such that $\mu(d) = 1$ is exactly half of l. Thus in the expression of c_m, there are same numbers of b_i's in denominator and numerator, such as

$$c_m = \frac{(b_m)\ (b_{m/q_1q_2}\ b_{m/q_1q_3}\ \cdots\ b_{m/q_{t-1}q_t})\cdots}{(b_{m/q_1}\ b_{m/q_2}\ \cdots b_{m/q_t})\ (b_{m/q_1q_2q_3}\ \cdots b_{m/q_{t-2}q_{t-1}q_t})\cdots}$$

$$= \frac{(b_m)\ (\prod_{i_1,i_2} b_{m/q_{i_1}q_{i_2}})(\prod_{i_1,i_2,i_3,i_4} b_{m/q_{i_1}q_{i_2}q_{i_3}q_{i_4}})\cdots}{(\prod_{i_1} b_{m/q_{i_1}})\ (\prod_{i_1,i_2,i_3} b_{m/q_{i_1}q_{i_2}q_{i_3}})(\prod_{i_1,i_2,i_3,i_4,i_5} b_{m/q_{i_1}q_{i_2}q_{i_3}q_{i_4}q_{i_5}})\cdots}$$

where q_{i_j} $(1 \le i_j \le t)$ is a prime factor of m, and the last term in numerator and denominator depends on whether t is even or odd. □

Proposition 6. *Let $f(x) = x^n + a$ $(a \neq 0)$. Then every b_k divides b_{kj} for all $j > 0$. Moreover for a prime p such that $p^e||b_k$ and $n > 1$,*

(1) *if $k|m$ then $p^e||b_m$.*
(2) *the converse of (1) holds if k is the smallest to be $p \mid b_k$.*
(3) *every c_m is a pairwise coprime integer.*

Proof. By induction on j, we will show $b_1|b_j$. $b_2 = f_2(0) = f(a) = a^n + a$ is divisible by $a = b_1$. Assume b_1 divides b_j, say $b_j = b_1\theta$ for some $\theta \in \mathbb{Z}$. Then $b_{j+1} = f(b_j) = (b_j)^n + a = (b_1\theta)^n + b_1$ is a multiple of b_1.

Moreover b_k divides b_{kj} for all $j > 0$ because (by mod b_k)

$$\begin{aligned} b_{kj} &= f_{kj}(0) = f_{k(j-1)}f_k(0) = f_{k(j-1)}(b_k) \equiv f_{k(j-1)}(0) \\ &= f_{k(j-2)}f_k(0) = f_{k(j-2)}(b_k) \equiv \cdots \equiv f_k(b_k) \equiv f_k(0) = b_k \equiv 0. \end{aligned}$$

(1) Let $m = dk$ $(d \in \mathbb{Z})$. Then $p^e||b_k$ implies $p|b_m$ and by mod p^e we have

$$b_m = f_{(d-1)k}f_k(0) = f_{(d-1)k}(b_k) \equiv f_{(d-1)k}(0) = \cdots = f_k(0) = b_k \equiv 0,$$

so $p^e|b_m$. If we let $b_k = p^e b'_k$ with $\gcd(p, b'_k) = 1$ then $b_k^n = p^{en}(b'_k)^n$. Since $n > 1$, $en \ge e+1$ and $b_k^n \equiv 0 \pmod{p^{e+1}}$. Thus by modulo p^{e+1} we have

$$\begin{aligned} b_m &= f_{(d-1)k-1}f_{k+1}(0) = f_{(d-1)k-1}f(b_k) = f_{(d-1)k-1}(b_k^n + a) \\ &\equiv f_{(d-1)k-1}(a) = f_{(d-1)k-1}(b_1) = f_{(d-1)k}(0) = \cdots = f_k(0) = b_k. \end{aligned}$$

Hence $p^{e+1} \nmid b_m$, so $p^e||b_m$.

(2) Let $m = dk + r$ with $0 \le r < k$. Since $b_m \equiv b_k \equiv 0 \pmod{p^e}$, we have

$$\begin{aligned} 0 \equiv b_m &= f_r\left(f_{dk}(0)\right) = f_r\left(f_{(d-1)k}(f_k(0))\right) = f_r\left(f_{(d-1)k}(b_k)\right) \\ &\equiv f_r\left(f_{(d-1)k}(0)\right) \equiv \cdots \equiv f_r\left(f_k(0)\right) = f_r(b_k) \equiv f_r(0) = b_r \pmod{p^e}, \end{aligned}$$

so $p\ |b_r$. But since k is the smallest to be $p\ |b_k$, we have $r = 0$ so $m = kd$.

(3) Let $m = q_1^{k_1} \cdots q_t^{k_t}$. If p is a prime divisor of denominator of c_m, we may assume $p^e \| b_{m/q_{i_1}\cdots q_{i_j}}$ (Proposition 5). Since there are 2^j multiples of $m/q_{i_1}\cdots q_{i_j}$ in c_m having the same $v_p(b_{m/q_{i_1}\cdots q_{i_j}})$, and exactly half of them are placed in numerator and the others are in denominator, $v_p(c_m) = 0$ so any prime divisor of denominator is canceled out in c_m. Moreover if p divides some b_m then p divides only one of c_m, thus all c_m are pairwise coprime integers. (see [7] and [9] for $\deg f(x) = 2$.) □

4. GALOIS GROUP FOR ITERATION POLYNOMIALS

We will discuss the important role of b_m and c_m in determining the Galois group.

Proposition 7. *Let $f(x) = x^n + a \in \mathbb{Z}[x]$ with $n = p^t$ (p a prime). Let $f_m(x)$ be irreducible in $\mathbb{Q}$, and E_m be the splitting field of f_m for all m. Then*

(1) *$[E_{m+1} : E_m] = n^{n^m}$ if and only if $b_{m+1} \notin (E_m)^p$*

(2) *Let $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$ and $b_1, \cdots, b_m$ be n-independent in $\mathbb{Q}(\varepsilon_n)$. For $b \in \mathbb{Q}(\varepsilon_n)$, if $b_1, \cdots, b_m, b$ are n-independent then $b \notin (E_m)^p$.*

Proof. We remark that $E_m \subseteq E_{m+1}$ is an n-Kummer extension such that $[E_{m+1} : E_m] \le n^{n^m}$. The Proposition was proved in [3] if $n = p^t$ (p odd prime), and in [7] (and [9]) if $n = 2$ and $t = 1$. Similar to [7], we can prove this when $n = 2^2$, then it can be generalized to $n = 2^t$ ($t \ge 1$). In fact, if $f(x) = x^4 + a$ then $f_m(x)$ is of degree 4^m. If $\beta_{m,1}, \cdots, \beta_{m,4^m}$ are all roots of $f_m(x)$ in E_m then $f_m(x) = \prod_{j=1}^{4^m}(x - \beta_{m,j}) \in E_m[x]$, and

$$b_{m+1} = f_{m+1}(0) = f_m(f(0)) = f_m(a) = \prod_{j=1}^{4^m}(a - \beta_{m,j}).$$

Suppose that $b_{m+1} \notin (E_m)^2$. In order to show $[E_{m+1} : E_m] = 4^{4^m}$, we will prove that all $a - \beta_{m,1}$, $a - \beta_{m,2}$, $\cdots$, $a - \beta_{m,4^m}$ are 4-independent in E_m, i.e., they are 2-independent, due to Proposition 3 and 4.

Assume that $\prod_{j=1}^{4^m}(a - \beta_{m,j})^{d_j} \in (E_m)^2$. Let

$$V = \left\{ (d_1, \cdots, d_{4^m}) \in Z_2 \times \cdots \times Z_2 \mid \prod_{j=1}^{4^m}(a - \beta_{m,j})^{d_j} \in (E_m)^2 \right\}.$$

Let $\sigma \in G_m = \mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_4))$ be any element. Then $\sigma(\beta_{m,i}) = \beta_{m,j} \overset{\text{let}}{=} \beta_{m,\sigma(i)}$ for $1 \le i, j = \sigma(i) \le 4^m$, and by defining $\sigma \cdot (d_1, \cdots, d_{4^m}) = (d_{\sigma(1)}, \cdots, d_{\sigma(4^m)})$, V is a $Z_2[G_m]$-module. If $V \ne 0$ then it can be seen $V^{G_m} \ne 0$. Hence there is $0 \ne (d_1, \cdots, d_{4^m}) \in V^{G_m}$ satisfying $\prod_{j=1}^{4^m}(a - \beta_{m,j})^{d_j} \in (E_m)^2$, and

$$(d_1, \cdots, d_{4^m}) = \sigma \cdot (d_1, \cdots, d_{4^m}) = (d_{\sigma(1)}, \cdots, d_{\sigma(4^m)}) \text{ for all } \sigma \in G_m.$$

Since σ permutes d_i to $d_{\sigma(i)} = d_j$, we must have $d_i = d_j$ for all i, j. Furthermore since not every d_i are zero, $d_i = d_j = 1$ for all i, j. Hence $\prod_{j=1}^{4^m}(a - \beta_{m,j}) \in (E_m)^2$, i.e., $b_{m+1} \in (E_m)^2$ a contradiction. Therefore it should be $V = 0$, so every $d_i = 0$ in Z_2, i.e., d_i is a multiple of 2.

On the other hand, if $b_{m+1} \in (E_m)^2$ then it is clear that $[E_{m+1} : E_m] < 4^{4^m}$.

(2) By Proposition 2, the maximal Kummer n-extension F in E_m over $\mathbb{Q}(\varepsilon_n)$ is of degree n^m. We claim $F = \mathbb{Q}(\varepsilon_n)(\sqrt[n]{b_1}, \cdots, \sqrt[n]{b_m})$. In fact if S is the set of all roots of f_{k-1} in E_{k-1} then $f_{k-1}(x) = \prod_{s\in S}(x - s)$ and $b_k = f_{k-1}(f(0)) = f_{k-1}(a) = \prod_{s\in S}(a - s)$. Since any root v of f_k belongs to E_k and

$$0 = f_k(v) = f_{k-1}(f(v)) = f_{k-1}(v^n + a),$$

we have $v^n + a \in S$. Thus for any $s \in S$, $a - s = -v^n$, so $b_k = \prod_{s\in S}(a - s) \in (E_k)^n$ for all $1 \le k \le m$. Hence $b_1, \cdots, b_m \in (E_m)^n$, i.e., $\sqrt[n]{b_1}, \cdots, \sqrt[n]{b_m} \in E_m$. Now from $\mathbb{Q}(\varepsilon_n) \subseteq \mathbb{Q}(\varepsilon_n)(\sqrt[n]{b_1}, \cdots, \sqrt[n]{b_m}) \subseteq E_m$, since $b_1, \cdots, b_m$ are n-independent in $\mathbb{Q}(\varepsilon_n)$, the abelian extension $\mathbb{Q}(\varepsilon_n)(\sqrt[n]{b_1}, \cdots, \sqrt[n]{b_m})$ is of degree n^m over $\mathbb{Q}(\varepsilon_n)$, so $\mathbb{Q}(\varepsilon_n)(\sqrt[n]{b_1}, \cdots, \sqrt[n]{b_m})$ is the Kummer n-extension F in E_m. Thus if $b \in (E_m)^p$ then $\sqrt[p]{b} \in E_m$, $\sqrt[p]{b} \in F$, so $b, b_1, \cdots, b_m$ are n-dependent. □

Proposition 8. *Let $f(x) = x^n + a$ ($n = 2^t$, $a \neq 0, -1$) be irreducible over integer ring. Then every b_m is positive for all $m > 1$. When $a > 0$, $c_m > 0$ for every m. When $a < 0$, every c_m is positive if and only if m is not a square free integer.*

Proof. Clearly $b_1 = a$, $b_2 = a(a^{n-1} + 1)$, and $b_3 = a(a^{n-1}(a^{n-1} + 1)^n + 1)$, etc. Thus if $a > 0$ then b_m and c_m are positive.

Suppose that $a < 0$. Then $b_1 < 0$, but $b_2 = a(a^{n-1} + 1) > 0$ for $a^{n-1} + 1 < 0$. Furthermore since $a^{n-1}(a^{n-1} + 1)^n + 1 < a^{n-1} + 1 < 0$, we have

$$b_3 = a(a^{n-1}(a^{n-1} + 1)^n + 1) > a(a^{n-1} + 1) > 0,$$

thus $b_3 > b_2 > 0$. Hence we can have $b_m > 0$ for all $m > 1$.

Let $m = q_1^{k_1} \cdots q_t^{k_t}$. If m is square free then $b_1 = b_{m/\prod_{j=1}^t q_j}$ appears in the formula of c_m in Proposition 5. Thus $c_m < 0$ because b_1 is the only negative among all b_j's. But if m is not square free then at least one of k_i is larger than 1. Since b_1 is not equal to any of $b_{m/\prod q_j}$, it does not show up in c_m, so $c_m > 0$. □

Proposition 9. *The n-independence of $b_1, \cdots, b_m$ and $c_1, \cdots, c_m$ are equivalent.*

Proof. Let $\prod_{i=1}^m b_i^{x_i} \in \mathbb{Q}^n$ $(x_i \in \mathbb{Z})$. Since $c_k = \prod_{d|k} b_d^{\mu(\frac{k}{d})}$, $b_k = \prod_{d|k} c_d$ so

$$c_1^{x_1}(c_1c_2)^{x_2}(c_1c_3)^{x_3}(c_1c_2c_4)^{x_4}\cdots(\prod_{d|m} c_d)^{x_m}$$
$$= c_1^{\sum_{i=1}^{i\le m} x_i} c_2^{\sum_{i=1}^{2i\le m} x_{2i}} c_3^{\sum_{i=1}^{3i\le m} x_{3i}} \cdots c_m^{\sum_{i=1}^{mi\le m} x_{mi}} \in \mathbb{Q}^n.$$

If k is the largest integer $\le \frac{m}{2}$ and $u \ge k+1$ then $ui \le m$ implies $i=1$, so

$$c_1^{\sum_{i=1}^{i\le m} x_i} \cdots c_k^{\sum_{i=1}^{ki\le m} x_{ki}} \cdot c_{k+1}^{x_{k+1}} \cdots c_m^{x_m} \in \mathbb{Q}^n.$$

But since $c_1, \cdots, c_m$ are n-independent, it is clear that $n|x_{k+1}, \cdots, n|x_m$. Furthermore $c_k^{\sum_{i=1}^{ki\le m} x_{ki}} = c_{x_k+x_{2k}}$ and $n|x_k + x_{2k}$ imply $n|x_k$. Continuing this we can conclude that n divides $x_k, \cdots, x_1$, too. Thus $b_1, \cdots, b_m$ are n-independent.

Now suppose that m is the minimal to be $c_1, \cdots, c_m$ are n-dependent. Let $\prod_{i=1}^m c_i^{y_i} = \theta^n \in \mathbb{Q}^n$ for $\theta \in \mathbb{Q}$ $(y_i \in \mathbb{Z})$. If $n|y_m$ then $c_1^{y_1}\cdots c_{m-1}^{y_{m-1}} = \left(\frac{\theta^n}{c_m^{y_m/n}}\right)^n \in \mathbb{Q}^n$. Due to the minimality of m, $c_1, \cdots, c_{m-1}$ are n-independent, so $n|y_1, \cdots, n|y_{m-1}$. Then together with $n|y_m$, it would yield $c_1, \cdots, c_m$ are n-independent. So we must have $n \not| y_m$. Moreover owing to form of c_k's in Proposition 5, we have

$$\theta^n = b_1^{y_1}\left(\frac{b_2}{b_1}\right)^{y_2}\left(\frac{b_3}{b_1}\right)^{y_3}\cdots\Big(\prod_{d|m-1} b_d^{\mu(\frac{m-1}{d})}\Big)^{y_{m-1}}\Big(\prod_{d|m} b_d^{\mu(\frac{m}{d})}\Big)^{y_m} = b_1^{u_1}\cdots b_{m-1}^{u_{m-1}}\cdot b_m^{y_m}$$

for $u_1, \cdots, u_{m-1} \in \mathbb{Z}$. Since $b_1, \cdots, b_m$ are n-independent, we have $n|u_1, \cdots, n|u_{m-1}$ and $n|y_m$, a contradiction. Therefore $c_1, \cdots, c_m$ are n-independent. □

Proposition 10. *Let $f(x) = x^n + a \in \mathbb{Z}[x]$ $(a > 0,\ n = 2^t)$ be irreducible. If none of $c_1, \cdots, c_m$ are in $\mathbb{Q}^n$ then* $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$.

Proof. The irreducibility of $f(x)$ implies that all $f_m(x)$ are irreducible since the unit elements in $\mathbb{Z}$ are only ± 1 ([4, Corollary 4]). Due to Proposition 6 and 8, every $c_i > 0$ and $\gcd(c_i, c_j) = 1$ for all i, j. Thus the nonzero residue classes of c_i in $\mathbb{Q}/(\mathbb{Q}^*)^n$ are linearly independent and $c_1, \cdots, c_m$ are $n(=2^t)$-independent in $\mathbb{Q}$ by Proposition 3. Owing to Proposition 9, we will show that the n-independence $b_1, \cdots, b_m$ in $\mathbb{Q}$ implies $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$ by induction on m.

Clearly $\mathrm{Gal}(f/\mathbb{Q}(\varepsilon_n)) \cong C_n$ because $x^n + a$ is irreducible over $\mathbb{Q}(\varepsilon_n)$. Assume that $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$ if $b_1, \cdots, b_m$ are n-independent. Now let $b_1, \cdots, b_{m+1}$ be n-independent. Then $b_1, \cdots, b_m$ are n-independent, so $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$ due to the hypothesis. Hence $b_{m+1} \notin (E_m)^2$, so $[E_{m+1} : E_m] = n^{n^m}$ by Proposition 7 (2) and (1). Thus together $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^m$ with $[E_{m+1} : E_m] = n^{n^m}$ yields $\mathrm{Gal}(f_{m+1}/\mathbb{Q}(\varepsilon_n)) \cong [C_n]^{m+1}$ by Proposition 2. □

We let

$$g(x) = a^3x^4 + 1, \quad \beta_1 = g(0) \text{ and } \beta_m = g(\beta_{m-1}) \text{ for all } m > 1$$

and, with the Möbius map μ, let

$$\gamma_m = \prod_{d|m} \beta_d^{\mu(m/d)} \text{ for all } m > 0.$$

Proposition 11. *Let $f(x) = x^4 + a$ $(a \neq 0, -1)$ be irreducible, and $g(x) = a^3x^4 + 1$. Then β_m is a constant term of $g_m(x)$, whose sign is equal to that of a for $m > 1$. Moreover $b_m = a\beta_m$ for $m \geq 1$, and $c_m = \gamma_m$ for $m > 1$.*

Proof. Obviously $\beta_m = g(\beta_{m-1}) = g_m(0)$ the constant term of $g_m(x)$. Moreover since $\beta_1 = g(0) = 1$, $\beta_2 = g(\beta_1) = a^3 + 1$ and $\beta_3 = g_3(0) = g(a^3+1) = a^3(a^3+1)^4 + 1$, if $a > 0$ then $\beta_m > 0$ for all $m \geq 1$, and if $a < 0$ then $\beta_m < 0$ for all $m > 1$.

Furthermore since $b_1 = a = a\beta_1$ and $b_2 = a(a^3+1) = a\beta_2$, it is clear that

$$b_m = f(b_{m-1}) = (a\beta_{m-1})^4 + a = a(a^3\beta_{m-1}^4 + 1) = ag(\beta_{m-1}) = a\beta_m$$

for all $m \geq 1$. Therefore, for any $m > 1$

$$c_m = \prod_{d|m} (a\beta_d)^{\mu(\frac{m}{d})} = \prod_{d|m} a^{\mu(\frac{m}{d})} \prod_{d|m} \beta_d^{\mu(\frac{m}{d})} = a^{\sum_{d|m} \mu(\frac{m}{d})} \prod_{d|m} \beta_d^{\mu(\frac{m}{d})} = \gamma_m,$$

because $\sum_{d|k} \mu(d) = 0$ for all $k > 1$. We note that $c_1 = a$ while $\gamma_1 = 1$. □

Proposition 12. *Let $f(x) = x^4 + a$, $g(x) = a^3x^4 + 1$, and β_m, γ_m be as before. Let $m = m'v_m$ (m' the square free part of m), and $M_m = \beta_{v_m} + \beta_{v_m+1}$. Then $\gamma_m \equiv -1$ (mod M_n), $\beta_{v_m+1} \equiv 1$ (mod β_{v_m}) and $gcd(\beta_{v_m}, M_m) = 1$.*

Proof. Let $m = q_1^{k_1} \cdots q_t^{k_t}$, $m' = q_1 \cdots q_t$ and $v_m = m/m'$. Since $g(x)$ is an even function, so are every $g_m(x)$, thus by mod M_m,

$$\beta_{v_m+1} = g(\beta_{v_m}) \equiv g(-\beta_{v_m+1}) = g(\beta_{v_m+1}) = \beta_{v_m+2} = \beta_{v_m+3} \equiv \cdots \equiv \beta_{2v_m},$$

thus $\beta_{2v_m} \equiv \beta_{v_m+1} \equiv -\beta_{v_m}$ (mod M_m). Moreover, since

$$\beta_{3v_m} = g_{v_m}(\beta_{2v_m}) \equiv g_{v_m}(-\beta_{v_m}) = g_{v_m}(\beta_{v_m}) = \beta_{2v_m} \pmod{M_m},$$

it follows that $\beta_{dv_m} \equiv \beta_{2v_m} \equiv -\beta_{v_m}$ for all $d > 1$. Hence by mod M_m,

$$\gamma_m = \prod_{d|m} (\beta_d)^{\mu(\frac{m}{d})} = \prod_{d|m'} (\beta_{dv_m})^{\mu(\frac{m'}{d})}$$

$$= (\beta_{v_m})^{\mu(m')} \prod_{1<d|m'} (\beta_{dv_m})^{\mu(\frac{m'}{d})} \equiv (\beta_{v_m})^{\mu(m')} \prod_{1<d|m'} (-\beta_{v_m})^{\mu(\frac{m'}{d})}$$

$$= (-1)(-\beta_{v_m})^{\mu(m')} \prod_{1<d|m'} (-\beta_{v_m})^{\mu(\frac{m'}{d})} = (-1)\prod_{d|m'} (-\beta_{v_m})^{\mu(\frac{m'}{d})}$$

$$= (-1)(-\beta_{v_m})^{\sum_{d|m'} \mu(\frac{m'}{d})} \equiv -1,$$

so $c_m = \gamma_m \equiv -1 \pmod{M_m}$ for all $m > 1$. It is also clear that $\beta_{v_m+1} = g(\beta_{v_m}) \equiv g(0) = 1 \pmod{\beta_{v_m}}$, thus

$$\gcd(\beta_{v_m}, M_m) = \gcd(\beta_{v_m}, \beta_{v_m} + \beta_{v_m+1}) = \gcd(\beta_{v_m}, \beta_{v_m+1}) = \gcd(\beta_{v_m}, 1) = 1.$$

□

Now we are able to compute the Galois group of $f_m(x)$ over $\mathbb{Q}(\varepsilon_4)$.

Theorem 13. *Let $f(x) = x^4 + a$ ($0 < a$ integer) be an irreducible polynomial over $\mathbb{Q}$. If $a \not\equiv \pm 1 \pmod 8$ then $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_4))$ is isomorphic to $[C_4]^m$ for all m.*

Proof. Due to Proposition 10, it is enough to show that $c_1, \cdots, c_m \notin \mathbb{Q}^4$. Consider $g(x) = a^3x^4 + 1$, $\beta_1 = g(0)$, $\beta_m = g(\beta_{m-1})$, and $\gamma_m = \prod_{d|m} \beta_d^{\mu(m/d)}$. Let $m = m'v_m$ (m' the square free part of m) and $M_m = \beta_{v_m} + \beta_{v_m+1}$.

Suppose that some c_t ($1 < t \le m$) belong to $\mathbb{Q}^4$. Then the equation $X^4 = c_t$ is solvable over $\mathbb{Z}$. Since c_t and β_t are positive integers, and $c_t = \gamma_t \equiv -1 \pmod{M_t}$ ($t > 1$) by Proposition 6, 11 and 12,

$$X^4 \equiv -1 \pmod{M_t} \text{ is solvable over } \mathbb{Z} \text{ for } t > 1,$$

that is,

$$X^4 \equiv -1 \pmod{p^e} \text{ is solvable for every } p^e || M_t, \quad (p : \text{prime}, t > 1).$$

(i) We first consider the case $a \equiv \pm 2 \pmod 8$, i.e., $f(x) \equiv x^4 \pm 2 \pmod 8$ and $g(x) \equiv \pm 8x^4 + 1 \equiv 1 \pmod 8$. Then every $\beta_i \equiv \gamma_i \equiv 1 \pmod 8$ for all i, and $M_t = \beta_{v_t} + \beta_{v_t+1} \equiv 2 \pmod 8$. Since $M_t = 2(4k+1)$ ($k \in \mathbb{Z}$) and $4k+1$ is odd, we have $2||M_t$. However due to (*): $X^4 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 8$ (refer [8, p. 100]), $X^4 \equiv -1 \pmod 2$ is not solvable. This yields a contradiction to $c_t \in \mathbb{Q}^4$ for $1 < t \le m$.

In particular if $c_1 \equiv \pm 2 \pmod 8$ belongs to $\mathbb{Q}^4$ then $\pm 2 + 8k = u^4$ for some $k, u \in \mathbb{Z}$. Since u is even, say $u = 2v$ ($v \in \mathbb{Z}$), we have $\pm 2 + 8k = 16v^4$, i.e., $\pm 1 = 4(2v^4 - k)$, a contradiction. So every c_t ($1 \le t \le m$) does not belong to $\mathbb{Q}^4$.

(ii) If $a \equiv 3 \pmod 8$ then $b_1 \equiv 3$, $b_2 \equiv 4$, and $b_t \equiv 3$ or $4 \pmod 8$ depending on t is odd or even. Also $c_1 \equiv 3$, $c_2 \equiv \frac{4}{3} \equiv 4 \cdot 3 \equiv 4$, and we can show that $c_t \equiv 1 \pmod 8$ for $t > 2$. In fact if $t = q^k > 2$ then $c_t = \frac{b_{q^k}}{b_{q^{k-1}}}$ is either $\frac{3}{3}$ or $\frac{4}{4}$, so $c_t \equiv 1 \pmod 8$. When $t = q_1^{k_1} q_2^{k_2}$, if $q_1, q_2 > 2$ then $c_t \equiv \frac{3 \cdot 3}{3 \cdot 3} \equiv 1$ due to Proposition 5. When $q_1 = 2$, $c_t \equiv \frac{4 \cdot 3}{4 \cdot 3} \equiv 1$ if $k_1 = 1$, while $c_t \equiv \frac{4 \cdot 4}{4 \cdot 4} \equiv 1$ if $k_1 > 1$. Similarly when $t = q_1^{k_1} \cdots q_s^{k_s}$ with all $k_i \geq 1$, if every $q_i > 2$ then $c_t \equiv \frac{3 \cdots 3}{3 \cdots 3} \equiv 1$. If $q_1 = 2$, there are the same number of b_i's in denominator and numerator which are even (or odd), hence $c_t \equiv 1 \pmod 8$. (See the Table below.)

Now $\beta_1 = 1$, $\beta_2 = 4$, $\beta_3 \equiv 3 \cdot 4^4 + 1 \equiv 1 \pmod 8$. And β_t is either 1 or 4 $\pmod 8$ alternatively, because $b_t = a\beta_t$ $(t \geq 1)$ in Proposition 11. Furthermore $\gamma_1 \equiv 1$, $\gamma_2 \equiv 4$, and $\gamma_t \equiv 1$ for all $t > 2$. Therefore $M_t = \beta_{v_t} + \beta_{v_t + 1} \equiv 5 \pmod 8$, which shows that $X^4 \equiv -1 \pmod{M_t}$ is not solvable for $t > 1$ by (*), a contradiction.

In particular if $c_1 \equiv 3 \pmod 8 \in \mathbb{Q}^4$ then $3 + 8k = u^4$ for some $k, u \in \mathbb{Z}$. Since u is odd (say, $u = 2v + 1$, $v \in \mathbb{Z}$), $3 + 8k = 16v^4 + 32v^3 + 24v^2 + 8v + 1$ yields a contradiction $8|2$. Hence every c_t $(1 \leq t \leq m)$ does not belong to $\mathbb{Q}^4$.

(iii) If $a \equiv 5 \pmod 8$ then $b_1 \equiv 5$, $b_2 \equiv 6 \pmod 8$, and b_t is either 5 or 6 $\pmod 8$ whether t is odd or even. And $c_1 \equiv 5$, $c_2 \equiv \frac{6}{5} \equiv 6 \cdot 5 \equiv 6 \pmod 8$, and it is easy to see $c_t \equiv 1$ for all $t > 2$. Moreover $\beta_1 = 1$, $\beta_2 = 6$, $\beta_3 \equiv 5 \cdot 36^2 + 1 \equiv 1 \pmod 8$. And β_t is either 1 or 6 $\pmod 8$ alternatively. Hence $\gamma_1 \equiv 1$, $\gamma_2 \equiv 6$, and $\gamma_t \equiv 1$ for all $t > 2$. Since $M_t = \beta_{v_t} + \beta_{v_t+1} \equiv 7 \pmod 8$, this shows that the equation $X^4 \equiv -1 \pmod{M_t}$ is not solvable by (*). Hence $c_t \notin \mathbb{Q}^4$ for $t > 1$.

In particular if $c_1 \equiv 5 \pmod 8 \in \mathbb{Q}^4$ then $5 + 8k = u^4$ for some $k, u \in \mathbb{Z}$. So u is odd (say $u = 2v + 1$, $v \in \mathbb{Z}$), $5 + 8k = 16v^4 + 32v^3 + 24v^2 + 8v + 1$ yields a contradiction $8|4$. Thus every c_t $(1 \leq t \leq m)$ does not belong to $\mathbb{Q}^4$.

t		$a \equiv 3 \pmod 8$				$a \equiv 5$				$a \equiv 4$			
t	v_t	b_t	c_t	β_t	γ_t	b_t	c_t	β_t	γ_t	b_t	c_t	β_t	γ_t
1	1	3	3	1	1	5	5	1	1	4	4	1	1
2	1	4	4	4	4	6	6	6	6	4	1	1	1
3	1	3	1	1	1	5	1	1	1	4	1	1	1
4	2	4	1	4	1	6	1	6	1	4	1	1	1
5	1	3	1	1	1	5	1	1	1	4	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

(iv) Finally if $a \equiv 4 \pmod 8$ then $b_t \equiv 4$ for all $t \geq 1$ and $c_1 \equiv 4$, $c_t \equiv 1$ for all $t > 1$. And $\beta_t \equiv \gamma_t \equiv 1 \pmod 8$, so $M_t \equiv 2 \pmod 8$. Hence the equation $X^4 \equiv -1$

(mod M_t) is not solvable, thus $c_t \notin \mathbb{Q}^4$ for $t > 1$. If $c_1 \equiv 4 \pmod 8 \in \mathbb{Q}^4$ then $4 + 8k = u^4$ for $k, u \in \mathbb{Z}$. Since u is even (say $u = 2v$, $v \in \mathbb{Z}$), $1 + 2k = 4v^4$ yields a contradiction. Hence every c_t $(1 \le t \le m)$ does not belong to $\mathbb{Q}^4$.

Therefore we conclude that in cases of $a \equiv \pm 2, \pm 3, 4 \pmod 8$, every c_t does not belong to $\mathbb{Q}^4$. Thus $\mathrm{Gal}(f_m/\mathbb{Q}(\varepsilon_4)) \cong [C_4]^m$. □

Remark. We consider the cases that $a \equiv \pm 1 \pmod 8$. If $a \equiv 1 \pmod 8$ then $f(x) = x^4 + 1 = g(x)$, $b_1 \equiv \beta_1 = 1$, $b_2 \equiv \beta_2 \equiv 2$, so $b_t \equiv \beta_t$ is either 1 or 2 (mod 8) alternatively. And $c_1 \equiv 1 \pmod 8$. If $1 + 8k = u^4 = (2v+1)^4$ for some $u, v \in \mathbb{Q}$ then $k = 2v^4 + 4v^3 + 3v^2 + v$. Hence, for instance if $v = 0, 1$ or 2 then $k = 0, 10$ or 78, so $c_1 = 1, 81$ or 625 are contained in $\mathbb{Q}^4$. If $a \equiv -1 \pmod 8$, $f(x) \equiv x^4 - 1 \pmod 8$ yields $b_i \equiv -1$ or $0 \pmod 8$ according to i odd or even, furthermore $c_1 \equiv -1$ and $c_i \equiv 0$ (even i) or $1 \pmod 8$ (odd $i > 1$). Hence every c_i $(i > 1)$ belong to $\mathbb{Q}^4$.

REFERENCES

1. W. A. Beyer & J. D. Louck: Galois groups for polynomials related to quadratic map iterates. *Ulam Quart.* **2** (1994), no. 3, 1-39.
2. J. E. Cremona: On the Galois groups of the iterates of $x^2 + 1$. *Mathematika* **36** (1989), 259-261.
3. L. Danielson: *The Galois theory of iterated binomials.* Ph.D. Thesis, Oregon state university, 1995.
4. L. Danielson & B. Fein: On the irreducibility of the iterates of $x^n - b$. Proc. Amer. Math. Soc. **130** (2001), 1589-1596.
5. S. Lang: *Algebra.* 3rd. Addison-Wesley, Reading, 1993.
6. R. W. K. Odoni: The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc.* **51** (1985), 385-414.
7. ———: Realising wreath products of cyclic groups as Galois groups. *Mathematika* **35** (1988), 101-113.
8. H. E. Rose: *A course in number theory, 2nd ed.* Oxford Science Publications, 1994.
9. M. Stoll: Galois groups over $\mathbb{Q}$ of some iterated polynomials. *Arch. Math.* **59** (1992), 239-244.

DEPARTMENT OF MATHEMATICS, HANNAM UNIVERSITY, DAEJON 306-791, KOREA
Email address: `emc@hnu.ac.kr`