Tokyo J. Math.
Vol. 11, No. 1, 1988

The Factorization of p in $Q(a^{1/p^k})$ and the Genus Field of $Q(a^{1/n})$

William Yslas VÉLEZ*

University of Arizona

(Communicated by Y. Kawada)

Abstract. Let $x^{p^k}-a$ be irreducible over $\boldsymbol{Q}$. The first part of this paper is to explicitly give the decomposition rules for the factorization of p in the ring of integers of $\boldsymbol{Q}(a^{1/p^k})$.

As an application of the above we use these results to determine the genus field of $\boldsymbol{Q}(a^{1/n})$, where x^n-a is irreducible over $\boldsymbol{Q}$ and we make no restrictions on a.

Let K/F be a finite extension of algebraic number fields, O_F the ring of integers in F, and P a prime ideal in O_F. The question of the factorization of PO_K into prime ideals is an old one and plays an important role in algebraic number theory.

The determination of the number of distinct prime divisors is quite easy to answer for it only depends on the number of distinct prime factors of $h(x)=\mathrm{Irr}(\theta, F)$ (where $K=F(\theta)$, $\theta\in O_K$ with $\mathrm{Irr}(\theta, F)$ monic, of course) either modulo P or over F_P, the P-adic completion of F. We shall prefer to work in F_P. So, if $h(x)=h_1(x)\cdots h_g(x)$ is the factorization of $h(x)$ into irreducible factors over F_P, then PO_K factors into g distinct prime ideals, $P_1, \cdots, P_g$. Furthermore, $K_{P_i}\cong F_P(\theta_i)$, where $h_i(\theta_i)=0$ and the relative inertial and ramification degrees, e_i, f_i, of P_i over P are the relative inertial and ramification degrees of $F_P(\theta_i)/F_P$ and $e_if_i=\deg h_i(x)$.

Even though the $\deg h_i(x)$ is easily available, the determination of e_i and f_i is not. In fact, even for the case when $K=F(a^{1/p^k})$, where p is prime, the determination of the relative inertial and ramification degrees has not been accomplished, in general. Several special case however have been solved. For example, if $P\nmid p$, then the e_1, f_i were determined by Mann and Vélez [19]. If $P\mid p$, then this has appeared to be the much more intractable case, and in the literature we have found only the case

Received August 19, 1986

* The author was supported in part by National Science Foundation Grant PRM82-13783. Part of this work was done while the author was a visiting professor at the Mathematics Institute, University of Heidelberg.

$k=1$ treated.

Thus, for the case $F(a^{1/p})/F$, $P\mid p$, we have found the following published results (of course, we ignore $p=2$).

a) $F=\boldsymbol{Q}$, $p=3$ (p. 156, [3]).

b) $F=\boldsymbol{Q}$, any odd prime p ([27]).

c) F contains a primitive p-th root of unity (pp. 254-257 of [11]).

d) Any algebraic number field F ([25]).

Thus for the case $k=1$ the determination of the relative inertial and ramification degrees has been resolved. However, nowhere in the literature do we see any results for the case $k\geqq 2$, even when $F=\boldsymbol{Q}$.

There has recently been some activity in studying fields defined by roots of binomials, x^n-a, and various questions have been posed and resolved. Since these results are rather recent, let us mention at least some of the questions that have been posed and where one can find these results.

Let char $F\nmid n$ and let x^n-a be irreducible over F.

1) If x^n-b is irreducible over F and $F(a^{1/n})\cong F(b^{1/n})$, then what is the relationship between a and b? [1, 21].

2) If $b^{1/k}\in F(a^{1/n})$, how are k, n and a, b related? [2, 9].

3) What can one say about the lattice of subfields of $F(a^{1/n})/F$? [1].

4) When is $F(a^{1/n})/F$ a normal extension [1, 7, 8, 20, 24] and in particular when is its Galois group abelian? [22, 24, 28].

5) When are $\boldsymbol{Q}(a^{1/n})$, $\boldsymbol{Q}(b^{1/n})$ arithmetically equivalent? [15, 17, 18].

The main purpose of this paper is to show that by using some very simple results from the theory of radical extensions of fields, we can completely determine how p factors in the extension $\boldsymbol{Q}(a^{1/p^k})/\boldsymbol{Q}$.

These results have an immediate application. For F an algebraic number field, let F^* denote the maximal abelian extension of F which is the composite of an absolute abelian field L with F and F^*/F is unramified at all of the finite prime ideals of F.

Various authors [4, 5, 10, 12, 13, 14] have considered the problem of determining $\boldsymbol{Q}(a^{1/n})^*$. However in all the previous investigations they have put the condition that if p^r exactly divides a then $(r, n)=1$. This condition yields that p is totally ramified in $\boldsymbol{Q}(a^{1/n})/\boldsymbol{Q}$, and this makes the determination of $\boldsymbol{Q}(a^{1/n})^*$ much easier.

By using the results on the decomposition of p in $\boldsymbol{Q}(a^{1/p^k})$ we shall be able to completely determine $\boldsymbol{Q}(a^{1/n})^*$, without having to make assumptions as to how the primes divide a.

In order to make this paper self-contained, we shall prove the few results on radical extensions that we shall need.

Perhaps our success at realizing a solution arises from a different point of view than in our previous attempts. Our method of attack before had been to induct on k and this led to rather complicated computations in the residue system modulo P^r. In this paper we take a much more local point of view and consider the properties of $x^{p^k}-a$ over $\boldsymbol{Q}_p$.

Since we shall be working over p-adic fields we shall use the general results concerning them (for example, the material contained in the first four chapters of Weiss [26]). Moreover, we wish to single out the following results, which are quite standard.

Throughout this paper ζ_n shall denote a primitive n-th root of unity.

PROPOSITION 1. a) *Let $E/\boldsymbol{Q}_p$ be finite with $|\bar{E}|=q$ ($\bar{E}$ denotes the residue class field). Then for each f, $E(\zeta_{q^f-1})$ is the unique unramified extension of E of degree f over E.*
b) *Let F/E, $E/\boldsymbol{Q}_p$ be finite extensions and $f=f(F/E)$ the relative inertial degree. Then $E(\zeta_{q^f-1})\subset F$ and $F/E(\zeta_{q^f-1})$ is totally ramified.*
c) *If $a\equiv 1 \pmod{2^{r+2}}$ then $a\in \boldsymbol{Q}_2^{2^r}$.* □

Let $\phi_n(x)=\prod_i(x-\zeta_n^i)$, where $1\leqq i\leqq n$ and $(i, n)=1$. Given b, $b\neq 0$, let $\phi_n(x, b)=\prod_i(x-b\zeta_n^i)$, where i ranges over the same set as above. It is obvious that $\phi_n(x)$, $\phi_n(x, b)$ factor in the same way over F and in fact the roots of $\phi_n(x)$, $\phi_n(x, b)$ determine the same field extensions.

Let us first dispose of the trivial case. Throughout this paper $K=\boldsymbol{Q}(a^{1/p^k})$.

THEOREM 2. a) *If $p\mid a$, $p^2\nmid a$, then $pO_K=P^{p^k}$, $f(P/p)=1$.*
b) *If $a\in\boldsymbol{Q}_p^{p^k}$, then $pO_K=P_0(P_1P_2^p\cdots P_k^{p^{k-1}})^{p-1}$, $f(P_i/p)=1$ for all i.*

PROOF. a) is trivial since $x^{p^k}-a$ is Eisenstein.

For b) let $a=b^{p^k}$, $b\in\boldsymbol{Q}_p$. Then $x^{p^k}-a=x^{p^k}-b^{p^k}=\prod_{i=0}^k\phi_{p^i}(x, b)$. However, $\phi_{p^i}(x, b)$ is irreducible over $\boldsymbol{Q}_p$ and its roots yield totally ramified extensions of $\boldsymbol{Q}_p$. □

The following proposition collects together the results that we shall need from the theory of radical extensions, but first a definition.

DEFINITION. Let E/F be a finite extension. We say that E/F has the unique subfield property, abbreviated usp, if for every divisor m of $[E:F]$ there exists a unique field L with $E\supset L\supset F$ such that $[L:F]=m$.

PROPOSITION 3. *Let E be a field,* $\operatorname{char} E\nmid p$, *and x^p-a irreducible over E.*

a) *If p is odd or if $\zeta_4 \in E$, then $x^{p^k}-a$ is irreducible over E for all k. If $p=2$, then $x^{2^k}-a$ is irreducible over E iff x^4-a is irreducible over E iff $-4a \notin E^4$.*

Suppose that $x^{p^k}-a$ is irreducible over E for all $k \geqq 1$.

b) *$\zeta_4 \in E(a^{1/2^k}) \setminus E$ (set theoretic difference) iff $E(\zeta_4)=E(a^{1/2})$ iff $-a \in E^2$.*

c) *If $k>1$, then $E(a^{1/p^k})/E$ has the usp iff $\zeta_{2p} \notin E(a^{1/p^k}) \setminus E$.*

d) *If $\zeta_4 \in E(a^{1/2^k})$ then $E(a^{1/2^k})/E(\zeta_4)$ has the usp.*

Proof. a) is quite standard (see pp. 60-62 of [16]).

b) Suppose $\zeta_4 \in E(a^{1/2^k}) \setminus E$. If $E(\zeta_4) \neq E(a^{1/2})$, then x^2-a is irreducible over $E(\zeta_4)$. However, $[E(a^{1/2^k}) : E(\zeta_4)] = 2^{k-1}$, so $x^{2^k}-a$ must be reducible over $E(\zeta_4)$, thus by a), $-4a \in E(\zeta_4)^4$. However, $(1+\zeta_4)^4=-4$, so this implies that $a \in E(\zeta_4)^4$, contradicting the assumption that x^2-a is irreducible over $E(\zeta_4)$. Thus $E(\zeta_4)=E(a^{1/2})$. The rest of b) is quite standard.

c) Let $E(a^{1/p^k}) \supset L \supset E$ with $[L:E]=p^r$. Suppose $\zeta_{2p} \notin E(a^{1/p^k}) \setminus E$ (of course if p is odd this always holds). Let $\alpha=a^{1/p^k}$ and define t by $\alpha^{p^t} \in L$, $\alpha^{p^{t-1}} \notin L$ (since $\alpha^{p^k} \in E \subset L$, $t \leqq k$). Then α satisfies the binomial $x^{p^t}-\alpha^{p^t}$ over L. However, by a), it follows that $x^{p^t}-\alpha^{p^t}$ is irreducible over L. Thus $p^t=[E(\alpha):L]$, so $[L:E]=p^r=p^{k-t}$. On the other hand $[E(\alpha^{p^t}):E]=p^{k-t}$, thus since $L \supset E(\alpha^{p^t})$, we have that $L=E(\alpha^{p^t})=E(a^{1/p^r})$.

This takes care of the case of odd primes.

Finally, assume that $p=2$ and for each $0 \leqq r \leqq k$ we have that $E(a^{1/2^r})$ is the unique subfield of $E(a^{1/2^k})$ of degree 2^r over E. If $\zeta_4 \in E(a^{1/2^k}) \setminus E$, then by b), we have that $E(\zeta_4)=E(a^{1/2})$. Thus $\zeta_4 \in E(a^{1/4})$, so $E(a^{1/4})/E$ is a normal extension and it is easy to show that the Galois group of this extension is $\boldsymbol{Z}_2+\boldsymbol{Z}_2$. This implies that there are 3 quadratic subfields of $E(a^{1/2^k})/E$, contradicting the hypothesis. Thus $\zeta_4 \notin E(a^{1/2^k}) \setminus E$.

d) follows easily from b) and c). □

We remark that c) is a special case of Theorem 2.1 of [1].

We can now settle the case of an odd prime. The following lemma contains the essential information needed for this case.

Lemma 4. *Let p be odd, $b \notin \boldsymbol{Q}_p^p$. Then $\boldsymbol{Q}_p(\zeta_{p^s}, b^{1/p^r})/\boldsymbol{Q}_p$ is totally ramified for all r, s. Further, if $s>0$, the ramification degree is $p^{r+s-1}(p-1)$.*

Proof. We begin by making the following observation. Again, let E be any field of characteristic different from p. If $\zeta_p \notin E$ and $a \notin E^p$, then $a^{1/p}$ cannot be in any abelian extension of E, for if it were, this would imply that $E(a^{1/p})/E$ is abelian, thus $\zeta_p \in E(a^{1/p})$, yet $[E(\zeta_p):E] \mid p-1$.

Since $b \notin \boldsymbol{Q}_p^p$, we have that $x^{p^r}-b$ is irreducible over $\boldsymbol{Q}_p$ for all r. Let $\beta=b^{1/p^r}$. If $\boldsymbol{Q}_p(\beta)/\boldsymbol{Q}_p$ were not totally ramified, then there would be an unramified extension of degree p in $\boldsymbol{Q}_p(\beta)/\boldsymbol{Q}_p$. However by Prop. 3 c) we would have that this unramified extension would be $\boldsymbol{Q}_p(b^{1/p})$. However, unramified extensions are abelian, thus giving us a contradiction, so $\boldsymbol{Q}_p(\beta)/\boldsymbol{Q}_p$ is totally ramified.

Since $\boldsymbol{Q}_p(\zeta_{p^s})/\boldsymbol{Q}_p$ is abelian, $b^{1/p} \notin \boldsymbol{Q}_p(\zeta_{p^s})$, so by Prop. 3 a), $x^{p^r}-b$ is irreducible over $\boldsymbol{Q}_p(\zeta_{p^s})$, thus $p^r=[\boldsymbol{Q}_p(\zeta_{p^s}, \beta):\boldsymbol{Q}_p(\zeta_{p^s})]$. If this extension were not totally ramified, then just as in the preceding paragraph, we would have that $\boldsymbol{Q}_p(\zeta_{p^s}, b^{1/p})/\boldsymbol{Q}_p(\zeta_{p^s})$ is unramified. However, this implies that $\boldsymbol{Q}_p(\zeta_{p^s}, b^{1/p})=\boldsymbol{Q}_p(\zeta_{p^s}, \zeta_{p^p-1})$, and this last field is an abelian extension of $\boldsymbol{Q}_p$, which yields that $b^{1/p}$ is in an abelian extension of $\boldsymbol{Q}_p$, a contradiction. □

THEOREM 5. *Let p be odd and define s by $a \in \boldsymbol{Q}_p^{p^s}$ and $a \notin \boldsymbol{Q}_p^{p^{s+1}}$ if $s<k$, then $pO_K=P_0^{p^{k-s}}(P_1P_2^p \cdots P_s^{p^{s-1}})^{(p-1)p^{k-s}}$.*

PROOF. Let $a=b^{p^s}$, where $b \in \boldsymbol{Q}_p$, $b \notin \boldsymbol{Q}_p^p$. Then the following is a factorization into irreducibles:

$$x^{p^s}-a=x^{p^s}-b^{p^s}=(x-b)\phi_p(x, b) \cdots \phi_{p^s}(x, b) .$$

If $(b\zeta_{p^i})^{1/p} \in \boldsymbol{Q}_p(\zeta_{p^i}) \subset \boldsymbol{Q}_p(\zeta_{p^{i+1}})$, this would imply that $b^{1/p}$ is in an abelian extension of $\boldsymbol{Q}_p$, which cannot occur. Thus $(b\zeta_{p^i})^{1/p} \notin \boldsymbol{Q}_p(\zeta_{p^i})$, which in turn implies that $\phi_{p^i}(x^{p^j})$ is irreducible for all i, j. Thus the following is a factorization into irreducibles:

$$x^{p^k}-a=(x^{p^{k-s}}-b)\phi_p(x^{p^{k-s}}, b) \cdots \phi_{p^s}(x^{p^{k-s}}, b) .$$

Now, a root of $\phi_{p^i}(x^{p^{k-s}}, b)$ is of the form $b^{1/p^{k-s}}\zeta_{p^{k-s+i}}$, which is an element of the field $\boldsymbol{Q}_p(\zeta_{p^{k-s+i}}, b^{1/p^{k-s}})$. However, this last field is totally ramified, so every subfield is totally ramified. Thus, each of the above factors of $x^{p^k}-a$ yields a totally ramified extension. □

We now want to consider the case $p=2$. The following lemma is the even analogue of Lemma 4 and in fact is the key result needed to determine the decomposition of 2.

LEMMA 6. *Let $x^{2^t}-b$ be irreducible over $\boldsymbol{Q}_2$, then $f(\boldsymbol{Q}_2(b^{1/2^t}, \zeta_{2^s})/\boldsymbol{Q}_2) \leqq 2$ for all s.*

PROOF. Set $M=\boldsymbol{Q}_2(\beta, \zeta_{2^s})$, where $\beta=b^{1/2^t}$, and $f=f(M/\boldsymbol{Q}_2)$.

Let us first consider the case when $\zeta_{2^s} \in \boldsymbol{Q}_2(\beta)$. Suppose that $f \geqq 4$. Then there exists a subfield L of M with $L/\boldsymbol{Q}_2$ unramified and $[L:\boldsymbol{Q}_2]=4$. If $\zeta_4 \notin M$, then by Prop. 3 c), we have that $L=\boldsymbol{Q}_2(b^{1/4})$, implying that $\boldsymbol{Q}_2(b^{1/4})$ is normal, so $\zeta_4 \in \boldsymbol{Q}_2(b^{1/4})$. However, $\boldsymbol{Q}_2(\zeta_4)/\boldsymbol{Q}_2$ is ramified while

$\boldsymbol{Q}_2(b^{1/4})/\boldsymbol{Q}_2$ is unramified, yielding a contradiction. Thus we may assume that $\zeta_4 \in M$. Then by Prop. 3 b), $\boldsymbol{Q}_2(b^{1/2})=\boldsymbol{Q}_2(\zeta_4)$ and thus $L \cap \boldsymbol{Q}_2(b^{1/2})=\boldsymbol{Q}_2$ since one field is unramified while the other is totally ramified. So $[L(\zeta_4)\colon \boldsymbol{Q}_2]=8$ and $f(L(\zeta_4)/\boldsymbol{Q}_2)=4$, $e(L(\zeta_4)/\boldsymbol{Q}_2)=2$. By Prop. 3 d), $L(\zeta_4)=\boldsymbol{Q}_2(b^{1/8})$. However, since $L/\boldsymbol{Q}_2$ is abelian, we have that $L(\zeta_4)=\boldsymbol{Q}_2(b^{1/8})$ must be abelian over $\boldsymbol{Q}_2$. This implies that $\zeta_8 \in L(\zeta_4)$, yet $e(\boldsymbol{Q}_2(\zeta_8)/\boldsymbol{Q}_2)=4$ while $e(L(\zeta_4)/\boldsymbol{Q}_2)=2$, a contradiction.

We next consider the case $\zeta_{2^s} \notin \boldsymbol{Q}_2(\beta)$. Let 2^h denote the degree of the maximal abelian extension of $\boldsymbol{Q}_2(\beta)/\boldsymbol{Q}_2$. Then by Prop. 3 d), we have that the maximal abelian extension must have the form $\boldsymbol{Q}_2(b^{1/2^h})$. Thus $\zeta_{2^h} \in \boldsymbol{Q}_2(b^{1/2^h})$, so $s>h$. Let $2^r=[\boldsymbol{Q}_2(\beta) \cap \boldsymbol{Q}_2(\zeta_{2^s})\colon \boldsymbol{Q}_2]$. Then $r=h-1$ or h. In either case it follows that $\boldsymbol{Q}_2(\beta) \cap \boldsymbol{Q}_2(\zeta_{2^s})=\boldsymbol{Q}_2(b^{1/2^r})$, by Prop. 3. Thus we have that $\beta^{2^{t-r}} \in \boldsymbol{Q}_2(\zeta_{2^s})$ and in fact $[M\colon \boldsymbol{Q}_2(\zeta_{2^s})]=2^{t-r}$ since $\zeta_4 \in \boldsymbol{Q}_2(\zeta_{2^s})$ ($s>h\geqq 1$, so $s \geqq 2$ and Prop. 3 now yields that $x^{2^{t-r}}-b^{1/2^r}$ is irreducible over $\boldsymbol{Q}_2(\zeta_{2^s})$). Also by Prop. 3 c), since $\zeta_4 \in \boldsymbol{Q}_2(\zeta_{2^s})$, we have that $M/\boldsymbol{Q}_2(\zeta_{2^s})$ has the usp. If $f \geqq 4$ and since $\boldsymbol{Q}_2(\zeta_{2^s})$ is totally ramified, we must have that $f(M/\boldsymbol{Q}_2(\zeta_{2^s}))\geqq 4$, so $\boldsymbol{Q}_2(\zeta_{2^s}, b^{1/2^{r+2}})$ must be unramified over $\boldsymbol{Q}_2(\zeta_{2^s})$. From the structure of unramified extensions we see that

$$\boldsymbol{Q}_2(\zeta_{2^s}, b^{1/2^{r+2}})=\boldsymbol{Q}_2(\zeta_{2^s}, \zeta_{2^4-1})$$

which is an abelian extension of $\boldsymbol{Q}_2$, thus $\boldsymbol{Q}_2(b^{1/2^{r+2}})/\boldsymbol{Q}_2$ is an abelian extesion, yet $r+2>h$, contradicting the maximality of h.

So we must have that $f \leqq 2$. □

In studying the case when p is odd, it was irrelevant how much p divided a. For the case $p=2$, the behavior of the factorization exhibits some peculiarities which depend upon the power of 2 dividing a. This behavior again verifies the old adage that 2 is the oddest prime.

We now want to write a in a special form. If $a=2^r a_1$, a_1 odd (a_1 may be negative) and $(r, 2^k)=2^d$, then let y be such that $(y, 2)=1$ and $ry-x2^k=2^d$. Then since y is odd, $\boldsymbol{Q}(a^{1/2^k})=\boldsymbol{Q}(a^{y/2^k})=\boldsymbol{Q}((2^{2^d}a_1^y)^{1/2^k})$. Thus, in the following we will assume that a has the form

$$(*) \qquad a=2^{2^d}a_1\,, \qquad a_1 \text{ odd}\,, \quad 0 \leqq d \leqq k\,.$$

Note that if $d=k$, then $\boldsymbol{Q}(a^{1/2^k})=\boldsymbol{Q}(a_1^{1/2^k})$, so the case when a is odd is subsumed under the case $d=k$.

We can now state the results for $p=2$. Recall that by Th. 2, we may assume that $d \neq 0$ and that if $d=k$, then $a_1 \notin \boldsymbol{Q}_2^{2^k}$. Also we define t as follows: If $a_1 \in \boldsymbol{Q}_2^{2^k}$, then set $t=k$, otherwise define t by $a_1 \in \boldsymbol{Q}_2^{2^t}$, $a_1 \notin \boldsymbol{Q}_2^{2^{t+1}}$. We shall assume that $k \geqq 2$ and we set $K=\boldsymbol{Q}(a^{1/2^k})$. Also $0<d$

since if a is odd we may take $d=k$.

THEOREM 7. A) *If* $a_1 \equiv 3 \pmod 8$, *then* $2O_K = P^{2^k}$, $f(P/2)=1$.

B) *If* $a_1 \equiv 5 \pmod 8$ *and* $d>0$, *then* $2O_K = P^{2^{k-1}}$, $f(P/2)=2$.

C) *If* $a_1 \equiv 7 \pmod 8$ *and* $d \geqq 2$, *then* $2O_K = P^{2^k}$, $f(P/2)=1$.
If $d=1$ *and* $a_1 \equiv 15 \pmod{16}$, *then* $2O_K = (P_1P_2)^{2^{k-1}}$, $f(P_i/2)=1$, $i=1, 2$.
If $d=1$ *and* $a_1 \equiv 7 \pmod{16}$, *then* $2O_K = P^{2^{k-1}}$, $f(P/2)=2$.

D) *If* $a_1 \equiv 1 \pmod 8$, *then*

i) *If* $d=k$, $2O_K = P_0^{2^{k-t-1}}(P_1P_2^2 \cdots P_t^{2^{t-1}})^{2^{k-t}}$,
$f(P_0/2)=2$ *and* $f(P_i/2)=1$, $i>0$.

ii) *If* $0<d<k$, *then*

a) *If* $t \geqq d+1$, *then*
if $k=2$, $2O_K = (P_0P_1)^2$, $f(P_i/2)=1$, $i=0, 1$,
if $k>2$, $2O_K = (P_0P_1P_2P_2'P_3^4 \cdots P_d^{2^{d-1}})^{2^{k-d}}$,
$f(P_i/2)=f(P_i'/2)=1$, *for all* i.

b) *If* $t=d$ *then* $2O_K = (P_0P_1P_2P_3^4 \cdots P_t^{2^{t-1}})^{2^{k-t}}$,
$f(P_0/2)=2$ *and* $f(P_i/2)=1$ *for* $i>0$.

c) *If* $t<d$ *then* $2O_K = P_0^{2^{k-t-1}}(P_1P_2^2 \cdots P_t^{2^{t-1}})^{2^{k-1}}$,
$f(P_0/2)=2$, $f(P_i/2)=1$, *for* $i>0$.

PROOF. A), B) If $a_1 \equiv 3$ or $5 \pmod 8$, then by applying Prop. 3 a), we see that $x^{2^k}-a$ is irreducible over $\boldsymbol{Q}_2$, so 2 has exactly one factor in O_K. If $a_1 \equiv 3 \pmod 8$, then $\boldsymbol{Q}_2(a^{1/2}) = \boldsymbol{Q}_2(3^{1/2})$ and this is ramified over $\boldsymbol{Q}_2$. Further, $\boldsymbol{Q}_2(3^{1/2}) \neq \boldsymbol{Q}_2(\zeta_4)$, so $\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2$ has the usp by Prop. 3 c). Thus if $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2) \geqq 2$ then we would have that $\boldsymbol{Q}_2(3^{1/2})/\boldsymbol{Q}_2$ would be unramified. So $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2)=1$.

If $a_1 \equiv 5 \equiv -3 \pmod 8$ and $d>0$, then $\boldsymbol{Q}_2(a^{1/2}) = \boldsymbol{Q}_2((-3)^{1/2}) = \boldsymbol{Q}_2(\zeta_3)$, which is an unramified extension of $\boldsymbol{Q}_2$. However, by Lemma 6, $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2) \leqq 2$, so $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2(a^{1/2}))=1$ and the result follows.

C) If $a_1 \equiv -1 \pmod 8$, then $a_1 = -c^2$, $c \in \boldsymbol{Q}_2$. If $d \geqq 2$, then $x^{2^k}-a$ is irreducible over $\boldsymbol{Q}_2$ by Prop. 3 a). Further, since $d \geqq 2$, $\boldsymbol{Q}_2(a^{1/4}) = \boldsymbol{Q}_2(a_1^{1/4})$. If $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2)=2$, then $\boldsymbol{Q}_2((-3)^{1/2}) \subset \boldsymbol{Q}_2(a^{1/2^k})$, and thus $\boldsymbol{Q}_2((-3)^{1/2}, \zeta_4) = \boldsymbol{Q}_2(a_1^{1/4})$ by Prop. 3 d). However since x^2-a is irreducible over $\boldsymbol{Q}_2(\zeta_3)$, this would imply x^4-a_1 is reducible over $\boldsymbol{Q}_2(\zeta_3)$, thus $-4a_1 \in \boldsymbol{Q}_2(\zeta_3)^4$. Since a_1 is odd and 2 is prime in $\boldsymbol{Q}_2(\zeta_3)$, this is impossible. Thus $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2)=1$ and $2O_K = P^{2^k}$, $f(P/2)=1$.

Now, let us assume that $d=1$.

If $a_1 \equiv -1 \pmod{16}$, then $a_1 = -c^4$, $c \in \boldsymbol{Q}_2$, thus $x^4-a = x^4+4c^4 = (x^2+2cx+2c^2)(x^2-2cx+2c^2)$ and thus $x^{2^k}-a = (x^{2^{k-1}}+2cx^{2^{k-2}}+2c^2)(x^{2^{k-1}}-2cx^{2^{k-2}}+2c^2)$, and both factors are Eisenstein at 2 over $\boldsymbol{Q}_2$, thus irreducible, and $2O_K = (P_1P_2)^{2^{k-1}}$, $f(P_i/2)=1$.

If $a_1 \equiv 7 \pmod{16}$, then by Prop. 3 a), $x^{2^k}-a$ is irreducible over $\boldsymbol{Q}_2$. However, $a_1=-c^2$, where $c \equiv \pm 3 \pmod 8$ and without loss of generality we may take $c \equiv 3 \pmod 8$. Thus we have that $a=-(2\cdot 3)^2 c_2^4$, where $c_2 \in \boldsymbol{Q}_2$. So $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(\zeta_4)$ and $\boldsymbol{Q}_2(a^{1/4})=\boldsymbol{Q}_2(\zeta_8 2^{1/2}3^{1/2})=\boldsymbol{Q}_2((1+\zeta_4)3^{1/2})=\boldsymbol{Q}_2(\zeta_4, (-3)^{1/2})$, so $f(\boldsymbol{Q}_2(a^{1/4})/\boldsymbol{Q}_2)=2$, thus by Lemma 6, we have that $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2(a^{1/4}))=1$, so $f(\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2)=2$ and $2O_K=P^{2^{k-1}}$, where $f(P/2)=2$.

D) Finally we come to the case $a_1 \equiv 1 \pmod 8$. This situation is more complicated than the preceding cases since $x^{2^k}-a$ may have many factors.

Case 1) $t \leqq d$. If $d=k$ then since we have already treated the case when $a \in \boldsymbol{Q}_2^{2^k}$, we may assume that $t<k$. If $d<k$, then since $t \leqq d$, we have that $t<k$. Thus in all cases we have that $t<k$ so $a_1=b_1^{2^t}$, $\pm b_1 \notin \boldsymbol{Q}_2^2$. Since a_1 is odd, this implies that $b_1 \equiv \pm 3 \pmod 8$, and without loss of generality we will take $b_1 \equiv -3 \pmod 8$.

Set $b=2^{2^{d-t}}b_1$, thus $a=b^{2^t}$ and

$$x^{2^t}-a=x^{2^t}-b^{2^t}=(x-b)(x+b)(x^2+b^2)\cdots(x^{2^{t-1}}+b^{2^{t-1}}) .$$

Thus

$$x^{2^k}-a=(x^{2^{k-t}}-b)(x^{2^{k-t}}+b^2)\cdots(x^{2^{k-1}}+b^{2^{t-1}}) .$$

By applying Prop. 3 a) we find that each of the factors of $x^{2^k}-a$ is irreducible. Further since $-b^{2^i} \equiv -1 \pmod 8$, we can apply C) to all but the first two or three factors (three when $t=d$ as we shall see below) to conclude that each of the factors (that is all but possibly the first two or three) gives rise to a totally ramified extension.

If $t<d$, then since $b_1 \equiv -3 \pmod 8$ we can apply B) to conclude that the first factor gives rise to a prime divisor P_0 of inertial degree 2 and ramification degree 2^{k-t-1}. Since $-b_1 \equiv 3 \pmod 8$ we can apply A) to the second factor to conclude that the second factor gives rise to a totally ramified extension.

If $t=d$, then $b=2b_1$ thus the first two factors are Eisenstein at 2 so they give rise to totally ramified extensions. The third factor has the form $x^{2^{k-t+1}}+2^2 b_1^2$. Since $-b_1^2 \equiv 7 \pmod 8$, we may apply C), $d=1$, to conclude that this factor gives rise to a divisor P_0 with $f(P_0/2)=2$. From the fourth factor on we apply C), $d \geqq 2$, to obtain totally ramified factors. Case 1 takes care of D) i) and D) ii) b), c).

Case 2) $t>d$. Set $b=2b_1^{2^{t-d}}$. Then $a=b^{2^d}$ and $x^{2^d}-a=(x-b)(x+b)\times(x^2+b^2)(x^4+b^4)\cdots(x^{2^{d-1}}+b^{2^{d-1}})$, where each of these factors is irreducible. Thus

$$x^{2^k}-a=(x^{2^{k-d}}-b)(x^{2^{k-d}}+b)(x^{2^{k-d+1}}+b^2)(x^{2^{k-d+2}}+b^4)\cdots(x^{2^{k-1}}+b^{2^{d-1}}) .$$

The first two factors are Eisenstein at 2 so give rise to totally ramified extensions. Also from the fourth factor on we may apply Prop. 3 a) to conclude that each of the factors is irreducible and by C) each gives rise to a totally ramified extension.

The third factor (if it appears at all, that is, if $k=2$ then under the assumptions $k \geqq t > d > 0$, we obtain $t=2$, $d=1$) however is reducible since $b=2b_1^{2^{t-d}}$ and thus $b^2=4b_1^{2^{t-d+1}}=4c^4$, where $c=b_1^{2^{t-d-1}}$. Thus

$$x^{2^{k-d+1}}+b^2=x^{2^{k-d+1}}+4c^4=(x^{2^{k-d}}-2cx^{2^{k-d-1}}+2c^2)(x^{2^{k-d}}+2cx^{2^{k-d-1}}+2c^2) .$$

Since both factors are Eisenstein at 2 they give rise to totally ramified extensions. Thus the third factor gives rise to 2 totally ramified extensions of degree 2^{k-d}. □

In the case when $K/\boldsymbol{Q}$ is an abelian extension and p is a prime of $\boldsymbol{Z}$, then in constructing the Hilbert tower we see that there is a sequence of fields $K \supset T \supset U \supset \boldsymbol{Q}$ where p splits into g factors in U, each of these factors pick up their inertial degrees from U to T, and then each totally ramifies from T to K. For the case when $K/\boldsymbol{Q}$ is not normal one usually expects splitting, followed by inertial degrees and then ramification. In general this does not happen, not even for the class of radical extensions.

For example, if $d=1$ and $a_1 \equiv 15 \pmod{16}$, then (by looking back to the proof) we see that 2 ramifies in $\boldsymbol{Q}(a^{1/2})$, then this unique factor of 2 in $\boldsymbol{Q}(a^{1/2})$ splits in $\boldsymbol{Q}(a^{1/4})/\boldsymbol{Q}(a^{1/2})$ and then total ramification for both factors in $\boldsymbol{Q}(a^{1/2^k})/\boldsymbol{Q}(a^{1/4})$.

If $d=1$ and $a_1 \equiv 7 \pmod{16}$, then 2 ramifies in $\boldsymbol{Q}(a^{1/2})$ and then the unique prime factor of 2 in $\boldsymbol{Q}(a^{1/2})$ remains inert in $\boldsymbol{Q}(a^{1/4})/\boldsymbol{Q}(a^{1/2})$ and then totally ramifies in $\boldsymbol{Q}(a^{1/2^k})/\boldsymbol{Q}(a^{1/4})$.

Furthermore if $\boldsymbol{Q}(a^{1/2}) \neq \boldsymbol{Q}(\zeta_4)$, then $\boldsymbol{Q}(a^{1/2})$ is the unique quadratic subfield of $\boldsymbol{Q}(a^{1/2^k})$ so it is not possible to circumvent this phenomenon in this situation.

When $a_1 \equiv 1 \pmod 8$ the factorization behavior of 2 in the tower of fields $\boldsymbol{Q} \subset \boldsymbol{Q}(a^{1/2}) \subset \boldsymbol{Q}(a^{1/4}) \subset \cdots \subset \boldsymbol{Q}(a^{1/2^k})$ is even more complicated.

As an application of our results we shall determine the genus field of $\boldsymbol{Q}(a^{1/n})$. We shall develop the few results that we need on genus fields. This development is different from that found in [12] and should be of interest in its own right.

Genus theory of fields. Let $[F:\boldsymbol{Q}]<\infty$. The genus field F^* of F is the maximal abelian extension of F which is a composite of an absolute abelian field L with F and is unramified at all of the finite prime ideals of F. Set F_* to be the maximal abelian number field of F^*. Clearly

$F^* = F \cdot F_*$. Set $g_F = [F^* : F]$. The number g_F is called the genus number of F.

LEMMA 8. *Let $p_1, \cdots, p_s$ be s distinct primes, $L_i \subset \boldsymbol{Q}(\zeta_{p_i^{f_i}})$, and $F = L_1 \cdots L_s$, then $F^* = F$.*

PROOF. We shall induct on s. If $s=1$ then F^*/F is unramified at all finite primes. However since $F^*/\boldsymbol{Q}$ is abelian over $\boldsymbol{Q}$ and the only ramified prime of F^* is p_1, we have that $F^* \subset \boldsymbol{Q}(\zeta_{p_1^t})$, for some t. But $\boldsymbol{Q}(\zeta_{p^t})/\boldsymbol{Q}$ is totally ramified, so $F^*/\boldsymbol{Q}$, F^*/F is totally ramified, thus $F^* = F$.

Now assume that the induction hypothesis is true when $k = s-1$ and let $F_1 = L_1 \cdots L_{s-1}$, $F_2 = L_s$, and $g_F = [F^* : F]$. Let $e_i = e(p_i, L_i/\boldsymbol{Q})$. Clearly $e_i = e(p_i, F^*/\boldsymbol{Q})$. Let V be the ramification field for p_s in F^*, then $e_s = [F^* : V]$ and $V \supset F_1$ since p_s is unramified in F_1. Since $e(p_i, F^*/\boldsymbol{Q}) = e(p_i, F_1/\boldsymbol{Q}) = e(p_i, V/\boldsymbol{Q})$ for $i < s$ and p_s is unramified in V, we see that V/F_1 is unramified at all finite primes, thus $V = F_1$ by the induction hypothesis, and then $[F^* : \boldsymbol{Q}] = [F^* : F_1] \cdot [F_1 : \boldsymbol{Q}] = e_1 \cdots e_s = [F : \boldsymbol{Q}]$, so $F^* = F$. □

COROLLARY 9. *If $F = \boldsymbol{Q}(\zeta_m)$, then $\boldsymbol{Q}(\zeta_m)^* = \boldsymbol{Q}(\zeta_m)$.* □

A useful tool for constructing abelian unramified extensions is the following lemma. See [23] for a proof.

ABHYANKAR'S LEMMA. *Let F_1, F_2 be algebraic number fields and $L = F_1 F_2$. Let P be a prime ideal of L dividing prime ideals P_1, P_2 and p of F_1, F_2 and $\boldsymbol{Q}$ respectively. Let $e_i = e(P_i, F_i/\boldsymbol{Q})$. If $p \nmid e_1$ and $e_1 \mid e_2$ then P is unramified over F_2.* □

If $F/\boldsymbol{Q}$ is an abelian extension then we know that there exists an m such that $F \subset \boldsymbol{Q}(\zeta_m)$. We remark that we can choose m so that m is divisible only by the primes that ramify in $F/\boldsymbol{Q}$ and further if $p^d \| e(p, F/\boldsymbol{Q})$ then if p is odd $p^{d+1} \| m$ and if $p=2$, then either $2^{d+1} \| m$ or $2^{d+2} \| m$.

The following result describes the structure of F_*.

THEOREM 10. *Let $F/\boldsymbol{Q}$ be finite and $\{p_1, \cdots, p_s\}$ the set of all distinct primes that ramify in $F_*/\boldsymbol{Q}$. Then there exist fields $L_1, \cdots, L_s$ such that $L_i \subset \boldsymbol{Q}(\zeta_{p_i^{f_i}})$ and $F_* = L_1 \cdots L_s$. Further, if p_i is odd then L_i is the unique subfield of $\boldsymbol{Q}(\zeta_{p_i^{f_i}})$ of degree $e(p_i, F_*/\boldsymbol{Q})$ over $\boldsymbol{Q}$. If $p_i = 2$, then L_i is one of the three fields*

$$\boldsymbol{Q}(\zeta_{2^{e+1}}) \; , \quad \boldsymbol{Q}(\zeta_{2^{e+2}} + \zeta_{2^{e+2}}^{-1}) \; , \quad \boldsymbol{Q}(\zeta_4(\zeta_{2^{e+2}} + \zeta_{2^{e+2}}^{-1})) \; ,$$

where $2^e = e(2, F_*/\boldsymbol{Q})$.

PROOF. Since F_* is abelian, $F_* \subset \boldsymbol{Q}(\zeta_m)$ for some m. With $e_i = e(p_i, F_*/\boldsymbol{Q})$ we have that $e_i \mid (p_i - 1)p_i^{f_i}$ for some f_i. Set $e_i = n_i p_i^{d_i}$, where $n_i \mid p_i - 1$. Let F_i be the unique subfield of $\boldsymbol{Q}(\zeta_{p_i})$ of degree n_i over $\boldsymbol{Q}$. Then by Abhyankhar's Lemma, we have that $F_i F_*/F_*$ is unramified at all finite primes, so $F_i F_* F/F$ is unramified at all finite primes, hence $F_i \subset F_*$, since F_* is the maximal abelian subfield of F_*.

Now, let us consider the power $p_i^{d_i}$.

If p_i is odd then there exists exactly one subfield of $\boldsymbol{Q}(\zeta_{p_i^{d_i+1}})$ of degree $p_i^{d_i}$ over $\boldsymbol{Q}$. Call this field F_i'. Recall that $F_* \subset \boldsymbol{Q}(\zeta_m)$, where $p_i^{d_i+1} \| m$. Thus $F_i' \cdot F_* \subset \boldsymbol{Q}(\zeta_m)$. However, since $p_i^{d_i} \| e(p_i, F_*/\boldsymbol{Q})$ and $p_i^{d_i} \| e(p_i, \boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$, we must have that $F_i' \cdot F_*/F_*$ is unramified at all finite primes, which yields that $F_i' \subset F_*$, thus we may set $L_i = F_i \cdot F_i'$ and we obtain that $[L_i : \boldsymbol{Q}] = e_i$ and $L_i \subset \boldsymbol{Q}(\zeta_{p_i^{d_i+1}})$.

Next consider $p = p_i = 2$ and set $2^e = e_i$. Then of course there are exactly three subfields of $\boldsymbol{Q}(\zeta_{2^{e+2}})$ of degree 2^e over $\boldsymbol{Q}$. Further, since $e(2, F_*/\boldsymbol{Q}) = 2^e$, we have that $F_* \subset \boldsymbol{Q}(\zeta_m)$, where $2^{e+2} \| m$. Thus only the factors of 2 in F_* ramify in $F_*(\zeta_{2^{e+2}})/F_*$. Let P be any prime divisor of 2 in $F_*(\zeta_{2^{e+2}})$ and let V be its ramification field in $F_*(\zeta_{2^{e+2}})/F_*$. Thus $2 = [F_*(\zeta_{2^{e+2}}) : V]$. Since $F_* \subset V \subset F_*(\zeta_{2^{e+2}})$ only the divisors of 2 can ramify in the extension V/F_*. However by definition of V, the divisors of 2 in F_* do not ramify, so V/F_* is unramified at all finite primes, and the same holds for VF_*F/F, thus $V = F_*$. So $[F_*(\zeta_{2^{e+2}}) : F_*] = 2$, thus $[F_* \cap \boldsymbol{Q}(\zeta_{2^{e+2}}) : \boldsymbol{Q}] = 2^e$ and since $\boldsymbol{Q}(\zeta_{2^{e+2}})$ contains exactly three subfields of degree 2^e, F_* must contain exactly one of them.

Thus, for p_i, $i = 1, \cdots, s$, we have a field L_i with $L_i \subset \boldsymbol{Q}(\zeta_{p_i^{f_i}})$, $L_i \subset F_*$ and $e_i = [L_i : \boldsymbol{Q}]$. Clearly $[L_1 \cdots L_s : \boldsymbol{Q}] = e_1 \cdots e_s$ and $F_* \supset L_1 \cdots L_s$. If $F_* \neq L_1 \cdots L_s$, then since $e(p_i, F_*/\boldsymbol{Q}) = e(p_i, L_i/\boldsymbol{Q})$, we have that $F_*/L_1 \cdots L_s$ is unramified at all finite primes. However by Lemma 8, $(L_1 \cdots L_s)^* = L_1 \cdots L_s$, thus $F_* = L_1 \cdots L_s$. □

Let $a \in \boldsymbol{Z}$ be such that $x^n - a$ is irreducible over $\boldsymbol{Q}$. For a prime p let $v_p(a)$ denote that exponent for which $p^{v_p(a)} \| a$. For the rest of this paper set $K = \boldsymbol{Q}(a^{1/n})$. We are now ready to compute K_*, however the following lemma, whose proof can be found on page 46 of [12], will prove useful.

LEMMA 11. *Let* $F = F_1 \cdot F_2$ *where* $[F_1 : \boldsymbol{Q}] = n_i$, $(n_1, n_2) = 1$ *and* $[F : \boldsymbol{Q}] = n_1 n_2$. *Then* $F^* = F_1^* \cdot F_2^*$ *and* $F_* = F_{1*} \cdot F_{2*}$. □

Using the notation of Theorem 10 we have that $K_* = L_1 \cdots L_s$. We wish to give a local characterization of the L_i. Thus let us fix i and set $L=L_i$, $p=p_i$ and suppose that $pO_K=P_1^{e_1}\cdots P_g^{e_g}$. Since KL/K is unramified at all finite primes and p is totally ramified in $L/\boldsymbol{Q}$, we see that $[L:\boldsymbol{Q}]\,|\,(e_1,\cdots,e_g)$. So if $(e_1,\cdots,e_g)=1$ then $L=\boldsymbol{Q}$. It is easy to see that L is the maximal subfield of $\boldsymbol{Q}(\zeta_{p^\infty})$ (the field of p^n-th roots of unity for all n) with the property that $i(L)\cdot K_{p_j}/K_{p_j}$ is unramified for all j, where $i(L)$ denotes an appropriate embedding of L into an algebraic closure of $\boldsymbol{Q}_p$. From this it follows that if there is at least one j for which $i(L')K_{p_j}/K_{p_j}$ is ramified for all subfields L' $(\neq\boldsymbol{Q})$ of $\boldsymbol{Q}(\zeta_{p^\infty})$, then necessarily $L=\boldsymbol{Q}$.

If p_i is odd then $L_i\subset\boldsymbol{Q}(\zeta_{p_i^\infty})$. Further we may decompose L_i into $L_i=L_i'\cdot L_i''$ where $L_i'\subset\boldsymbol{Q}(\zeta_{p_i})$, $[L_i'':\boldsymbol{Q}]$ is a power of p. The following lemma determines L_i' and Lemma 13 will show that $L_i''=\boldsymbol{Q}$.

LEMMA 12. *Suppose that $(n,p)=1$, $d=(v_p(a),n)$ and let $K_{(p)}$ denote the maximal subfield of $\boldsymbol{Q}(\zeta_{p^\infty})$ contained in K_*. Then $K_{(p)}$ is the unique subfield of $\boldsymbol{Q}(\zeta_p)$ of degree $(n/d,p-1)$ over $\boldsymbol{Q}$.*

PROOF. Let us first determine the factorization of p in K. Let $h=v_p(a)$ and $a=p^h a_1$, $(a_1,p)=1$. Write $d=hx-ny$ with $(x,n)=1$. Since $(x,n)=1$ we have that $K=\boldsymbol{Q}(a^{x/n})$. Now $a^x=p^{hx}a_1^x=(p^y)^n p^d a_1^x$ and obviously $K=\boldsymbol{Q}((p^d a_1^x)^{1/n})=\boldsymbol{Q}((pa_1^{x/d})^{1/r})$, where $r=n/d$.

If $M=\boldsymbol{Q}(a_1^{x/d})$, then since $(p,da_1^x)=1$, we have that p is unramified in $M/\boldsymbol{Q}$. However K is obtained from M by adjoining a root of $x^r-pa_1^{x/d}$ to M. If P is any divisor of p in O_M, then the polynomial $x^r-pa_1^{x/d}$ is Eisenstein at P, so

$$pO_K=(P_1\cdots P_g)^r\,,\qquad \text{where}\quad r\,|\,n\,.$$

Since $(p,r)=1$, $K_{(p)}\subset\boldsymbol{Q}(\zeta_{p^\infty})$ and $[K_{(p)}:\boldsymbol{Q}]\,|\,r$, we see that $K_{(p)}\subset\boldsymbol{Q}(\zeta_p)$. Thus the maximal possible such field is of degree $(p-1,r)$. However, if $K_{(p)}$ is the unique subfield of $\boldsymbol{Q}(\zeta_p)$ of degree $(p-1,r)$ over $\boldsymbol{Q}$, then by applying Abhyankhar's Lemma to $K_{(p)}$ and K, we see that $K_{(p)}K/K$ is unramified at all finite primes. □

LEMMA 13. *Let p be an odd prime, $n=p^k$ and let $K_{(p)}$ denote the maximal subfield of $\boldsymbol{Q}(\zeta_{p^\infty})$ contained in K_*. Then $K_{(p)}=\boldsymbol{Q}$.*

PROOF. By Th. 5 we see that there is a divisor P_0 of p in O_K with the property that

$$K_{P_0}=\boldsymbol{Q}_p(b^{1/p^{k-s}})\qquad \text{where } b\notin\boldsymbol{Q}_p^p \text{ if } k-s>0\,.$$

If $k-s=0$, then $e(P_0/p)=1$ so $K_{(p)}=\boldsymbol{Q}$. Thus we may take $k-s>0$.

However, by Lemma 4, we have that $\boldsymbol{Q}_p(b^{1/p^{k-s}}, \zeta_{p^t})$ is totally ramified over $\boldsymbol{Q}_p$ for all t and $[\boldsymbol{Q}_p(b^{1/p^{k-s}}, \zeta_{p^t}) : \boldsymbol{Q}_p] = p^{k-s+t-1}(p-1)$. This degree statement shows that $\boldsymbol{Q}_p(b^{1/p^{k-s}}) \cap \boldsymbol{Q}_p(\zeta_{p^\infty}) = \boldsymbol{Q}_p$.

There is a t for which $K_{(p)} \subset \boldsymbol{Q}(\zeta_{p^t})$, thus $K_{P_0} \cap i(K_{(p)}) = \boldsymbol{Q}_p$ (we take the natural embedding in $\bar{\boldsymbol{Q}}_p$) and $K_{P_0} \cdot K_{(p)}/K_{P_0}$ is totally ramified thus $K_{(p)} = \boldsymbol{Q}$. □

The following notation will be in force for the rest of this paper. Given K, let $K_{(p_i)}$ denote the maximal subfield of $\boldsymbol{Q}(\zeta_{p_i^\infty})$ contained in K_*. Thus

$$K_* = K_{(p_1)} \cdots K_{(p_s)} ,$$

where $\{p_1, \cdots, p_s\}$ is the set of primes that ramify in K_*. Further if p_i is odd we shall write $K_{(p_i)} = K'_{(p_i)} \cdot K''_{(p_i)}$, where $K'_{(p_i)} \subset \boldsymbol{Q}(\zeta_{p_i})$ and $[K''_{(p_i)} : \boldsymbol{Q}]$ is a power of p.

COROLLARY 14. *Let p be an odd prime, $n = p^r m$, $(m, p) = 1$, and $d = (v_p(a), m)$ and $K = \boldsymbol{Q}(a^{1/n})$. Then $K_{(p)}$ is the unique subfield of $\boldsymbol{Q}(\zeta_p)$ of degree $(m/d, p-1)$ over $\boldsymbol{Q}$.*

PROOF. Let $K_1 = \boldsymbol{Q}(a^{1/p^r})$, $K_2 = \boldsymbol{Q}(a^{1/m})$. Then by Lemma 11 we have that $K_* = K_{1*} \cdot K_{2*}$, and thus

$$K_{(p)} = K_{1(p)} \cdot K_{2(p)} .$$

By Lemma 13, $K_{1(p)} = \boldsymbol{Q}$ and Lemma 12 yields $K_{(p)} = K_{2(p)}$. □

For $K = \boldsymbol{Q}(a^{1/n})$ it only remains to determine $K_{(2)}$. If $n = 2^k m$, m odd, then by Lemma 12, $\boldsymbol{Q}(a^{1/m})_{(2)} = \boldsymbol{Q}$, thus $\boldsymbol{Q}(a^{1/n})_{(2)} = \boldsymbol{Q}(a^{1/2^k})_{(2)}$. For the rest of this paper we shall take $m = 1$ so $K = \boldsymbol{Q}(a^{1/2^k})$. Furthermore we may assume that a has the form

$$(*) \qquad a = 2^{2^d} a_1 , \qquad a_1 \text{ odd}, \quad n \leqq d \leqq k .$$

We shall determine $K_{(2)}$ using local methods and so we first set some generic terminology.

(**) If $[F : \boldsymbol{Q}_2] = 2^t$ then 2^h is the degree of the maximal abelian subfield of $F/\boldsymbol{Q}_2$. If $F = \boldsymbol{Q}_2(b^{1/2^t})$ then by Prop. 3 c), d), the maximal abelian subfield has the form $\boldsymbol{Q}_2(b^{1/2^h})$. Finally given F, T shall denote the maximal subfield of $\boldsymbol{Q}_2(\zeta_{2^\infty})$ with the property that FT/F is unramified. Obviously $[FT : F] = [T : T \cap F]$ and we denote this common degree by 2^r.

We have previously shown that if $x^{2^k} - b$ is irreducible over $\boldsymbol{Q}_2$ then

$f(\boldsymbol{Q}_2(b^{1/2^k}, \zeta_{2^s})/\boldsymbol{Q}_2) \leqq 2$. It shall be important to determine when this inertial degree is actually 2. This is accomplished in Lemma 16 but first one more result from the theory of radical extensions.

PROPOSITION 15. *Let $x^{2^k}-b_1$, $x^{2^k}-b_2$ be irreducible over $\boldsymbol{Q}_2$. Then there are roots $\beta_1^{2^k}=b_1$, $\beta_2^{2^k}=b_2$ with $\boldsymbol{Q}_2(\beta_1)=\boldsymbol{Q}_2(\beta_2)$ iff either* (1) *$b_1b_2^i \in \boldsymbol{Q}_2^{2^k}$ for some odd i or* (2) *$k \geqq 3$, $-b_1 \in \boldsymbol{Q}_2^2$, $-b_2 \in \boldsymbol{Q}_2^2$ and $b_1b_2^i2^{2^{k-1}} \in \boldsymbol{Q}_2^{2^k}$ for some odd i.*

Proposition 15 is a special case of Corollary 4.1 of [1]. □

LEMMA 16. *Let $x^{2^k}-a$ be irreducible, a has form $(*)$, assume $(**)$ and $f=f(\boldsymbol{Q}_2(a^{1/2^k}, \zeta_{2^s})/\boldsymbol{Q}_2)$. Then $f=2$ iff either*
(A) *$s \leqq h$ and either $a=-3c^2$ or if $k \geqq 2$, $a=-(2\cdot 3)^2c^4$, for some $c \in \boldsymbol{Q}_2$,*
(B) *$s>h$ then $\boldsymbol{Q}_2(a^{1/2^h}) \not\subset \boldsymbol{Q}_2(\zeta_{2^s})$ and either $s \geqq 3$ or if $s=2$ then $a=(\pm 3)c^2$, $c \in \boldsymbol{Q}_2$.*

PROOF. Recall that $\boldsymbol{Q}_2(a^{1/2^h})$ is the maximal abelian subfield of $\boldsymbol{Q}_2(a^{1/2^k})$. Since $x^{2^h}-a$ is irreducible, this implies that $\zeta_{2^h} \in \boldsymbol{Q}_2(a^{1/2^h})$ and in fact since $2^{h-1}=[\boldsymbol{Q}_2(\zeta_{2^h}):\boldsymbol{Q}_2]$, we have by Prop. 3 d) that $\boldsymbol{Q}_2(a^{1/2^{h-1}})=\boldsymbol{Q}_2(\zeta_{2^h})$. By Lemma 6 we know that $f \leqq 2$.

If $s \leqq h$ then of course, $\boldsymbol{Q}_2(a^{1/2^k}, \zeta_{2^s})=\boldsymbol{Q}_2(a^{1/2^k})$. In order to determine f we have to apply Th. 7, or rather a local version of Th. 7. However, the proof of Th. 7 is local anyway. By Th. 7 we see that $f=2$ iff either (i) $d>0$ and $a=2^{2^d}(-3)c^2$ (so $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2((-3)^{1/2})=\boldsymbol{Q}_2(\zeta_3)$) or (ii) if $k \geqq 2$, $d=1$ and $a=-(2\cdot 3)^2c^4$ (so $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(\zeta_4)$ and $\boldsymbol{Q}_2(a^{1/4})=\boldsymbol{Q}_2(\zeta_4, 3^{1/2})=\boldsymbol{Q}_2(\zeta_4, \zeta_3)$).

Let now $s>h$ and set $2^t=[\boldsymbol{Q}_2(a^{1/2^k}) \cap \boldsymbol{Q}_2(\zeta_{2^s}):\boldsymbol{Q}_2]$. Since $\zeta_{2^h} \in \boldsymbol{Q}_2(a^{1/2^k})$ and 2^h is the degree of the maximal abelian subfield we have that $t=h-1$ or $t=h$. In either case it follows that $\boldsymbol{Q}_2(a^{1/2^k}) \cap \boldsymbol{Q}_2(\zeta_{2^s})=\boldsymbol{Q}_2(a^{1/2^t})$. Let $M=\boldsymbol{Q}_2(a^{1/2^k}, \zeta_{2^s})$.

If $t=h$ then $\boldsymbol{Q}_2(a^{1/2^h}) \subset \boldsymbol{Q}_2(\zeta_{2^s})$. Since $\zeta_4 \in \boldsymbol{Q}_2(\zeta_{2^s})$ we have by Prop. 3 c) that $\boldsymbol{Q}_2(\zeta_{2^s}, a^{1/2^{h+1}})$ is the unique quadratic subfield of M over $\boldsymbol{Q}_2(\zeta_{2^s})$. However, $\boldsymbol{Q}_2(\zeta_{2^s})/\boldsymbol{Q}_2$ is totally ramified so $f=2$ iff $f(M/\boldsymbol{Q}_2(\zeta_{2^s}))=2$ iff $\boldsymbol{Q}_2(\zeta_{2^s}, a^{1/2^{h+1}})$ is unramified over $\boldsymbol{Q}_2(\zeta_{2^s})$. If $\boldsymbol{Q}_2(\zeta_{2^s}, a^{1/2^{h+1}})/\boldsymbol{Q}_2(\zeta_{2^s})$ is unramified then $\boldsymbol{Q}_2(\zeta_{2^s}, a^{1/2^{h+1}})=\boldsymbol{Q}_2(\zeta_{2^s}, \zeta_3)$, which is abelian over $\boldsymbol{Q}_2$. This implies that $\boldsymbol{Q}_2(a^{1/2^{h+1}})/\boldsymbol{Q}_2$ is abelian. If $k>h$ then this contradicts the maximality of h. If $k=h$, then $M=\boldsymbol{Q}_2(\zeta_{2^s})$. Thus, if $t=h$, then $f=1$.

Now assume that $t=h-1$, thus $\boldsymbol{Q}_2(a^{1/2^h}) \not\subset \boldsymbol{Q}_2(\zeta_{2^s})$. However, we do have that $\boldsymbol{Q}_2(a^{1/2^{h-1}})=\boldsymbol{Q}_2(\zeta_{2^h})$. Since $a^{1/2^{h-1}}$, ζ_{2^h} both satisfy irreducible binomials of degree 2^{h-1}, we have by Prop. 15 that either $a^{1/2^{h-1}}=c\zeta_{2^h}$ or if $8 \mid 2^{h-1}$ then $a^{1/2^{h-1}}=c2^{1/2}\zeta_{2^h}$, for some $c \in \boldsymbol{Q}_2$. If the latter then $a^{1/2^h}=c^{1/2}2^{1/4}\zeta_{2^{h+1}}$. However, this implies that $2^{1/4} \in \boldsymbol{Q}_2(a^{1/2^h}, c^{1/2}, \zeta_{2^{h+1}})$, which is an abelian extension of $\boldsymbol{Q}_2$, yet $\boldsymbol{Q}_2(2^{1/4})/\boldsymbol{Q}_2$ isn't even a normal extension. So $a^{1/2^h}=c^{1/2}\zeta_{2^{h+1}}$. By assumption $(\boldsymbol{Q}_2(a^{1/2^h})\not\subset\boldsymbol{Q}_2(\zeta_{2^s}))$, $a^{1/2^h}\notin\boldsymbol{Q}_2(\zeta_{2^s})$, so $c^{1/2}\notin\boldsymbol{Q}_2(\zeta_{2^s})$ (recall $s>h$).

If $s\geqq 3$, then $\boldsymbol{Q}_2(\zeta_{2^s})$ contains $(-1)^{1/2}$, $(\pm 2)^{1/2}$, thus since there are only 7 quadratic extensions of $\boldsymbol{Q}_2$, this implies that $c=\pm 3c_1^2$ or $c=\pm 6c_1^2$. In both instances we have

$$\boldsymbol{Q}_2(\zeta_{2^s},\ a^{1/2^h})=\boldsymbol{Q}_2(\zeta_{2^s},\ (-3)^{1/2})$$

which has inertial degree 2 over $\boldsymbol{Q}_2$.

If $s=2$ then $s>h$ implies that $h=1$ and thus $t=h-1=0$, so $\boldsymbol{Q}_2(a^{1/2^k})\cap\boldsymbol{Q}_2(\zeta_4)=\boldsymbol{Q}_2$. Since $(-1)^{1/2}$ is the only square root in $\boldsymbol{Q}_2(\zeta_4)$ and $\boldsymbol{Q}_2(a^{1/2})\cap\boldsymbol{Q}_2(\zeta_4)=\boldsymbol{Q}_2$ we have that $a=\pm 2c^2$, $\pm 3c^2$, $\pm 6c^2$. However, $f=2$ iff $\boldsymbol{Q}_2(\zeta_4,\ a^{1/2})/\boldsymbol{Q}_2(\zeta_4)$ is unramified, and this occurs iff $a=(\pm 3)c^2$, $c\in\boldsymbol{Q}_2$. □

COROLLARY 17. *Let $x^{2^k}-b$ be irreducible over $\boldsymbol{Q}_2$, $F=\boldsymbol{Q}_2(b^{1/2^k})$, r and T as in $(**)$ for F and s such that $T\subset\boldsymbol{Q}_2(\zeta_{2^s})$. If $f(F(\zeta_{2^s})/\boldsymbol{Q}_2)=1$ or $f(F/\boldsymbol{Q}_2)=2$ then $r=0$. If $f(F/\boldsymbol{Q}_2)=1$ then $r\leqq 1$.*

PROOF. From $(**)$ we see that

$$2^r f(F/\boldsymbol{Q}_2)=f(FT/\boldsymbol{Q}_2)\leqq f(F(\zeta_{2^s})/\boldsymbol{Q}_2)\leqq 2$$

by Lemma 6. If $f(F(\zeta_{2^s})/\boldsymbol{Q}_2)=1$ or $f(F/\boldsymbol{Q}_2)=2$, then $r=0$. If $f(F/\boldsymbol{Q}_2)=1$ then $r\leqq 1$. □

For a having form $(*)$ we can now determine $K_{(2)}$ when $d=0$.

THEOREM 18. *Let $K=\boldsymbol{Q}(a^{1/2^k})$, a have form $(*)$ and $d=0$. If $a_1\equiv 1\ (\mathrm{mod}\ 4)$ then $K_{(2)}=\boldsymbol{Q}(2^{1/2})$. If $a_1\equiv 3\ (\mathrm{mod}\ 4)$ then $K_{(2)}=\boldsymbol{Q}((-2)^{1/2})$.*

PROOF. Let $F=\boldsymbol{Q}_2(a^{1/2^k})$. Since $a=2a_1$, $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2((2a_1)^{1/2})\neq\boldsymbol{Q}_2(\zeta_4)$, thus $\zeta_4\notin F$ by Prop. 3 b) and $F/\boldsymbol{Q}_2$ has the usp by Prop. 3 c). Further, $\boldsymbol{Q}_2(a^{1/2})$ is the maximal abelian subfield of $F/\boldsymbol{Q}_2$, so $h=1$. Let s be such that $T\subset\boldsymbol{Q}_2(\zeta_{2^s})$. The cases $a_1\equiv\pm 3\ (\mathrm{mod}\ 8)$, $a_1\equiv\pm 1\ (\mathrm{mod}\ 8)$ are handled identically so we shall do one argument and carry the other in brackets.

If $a_1\equiv 1\ (\mathrm{mod}\ 8)$ $[a_1\equiv -1\ (\mathrm{mod}\ 8)]$, then $\boldsymbol{Q}_2(a^{1/2})\subset\boldsymbol{Q}_2(\zeta_{2^3})$. Thus by Lemma 16 B), $f(F(\zeta_{2^s})/\boldsymbol{Q}_2)=1$, so by Cor. 17, $r=0$, thus $T=\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(2^{1/2})$ $[T=\boldsymbol{Q}_2((-2)^{1/2})]$.

If $a_1\equiv\pm 3\ (\mathrm{mod}\ 8)$, then $F\cap\boldsymbol{Q}_2(\zeta_{2^\infty})=\boldsymbol{Q}_2$. By Cor. 17, $r\leqq 1$, so T must be one of the four fields, $\boldsymbol{Q}_2$, $\boldsymbol{Q}_2((\pm 2)^{1/2})$, $\boldsymbol{Q}_2(\zeta_4)$. It is easy to check that $\boldsymbol{Q}_2((2(-3))^{1/2},\ 2^{1/2})/\boldsymbol{Q}_2((2(-3))^{1/2})$, $\boldsymbol{Q}_2((2\cdot 3)^{1/2},\ (-2)^{1/2})/\boldsymbol{Q}_2((2\cdot 3)^{1/2})$ are unramified extensions, thus $T=\boldsymbol{Q}_2(2^{1/2})$ if $a_1\equiv -3\ (\mathrm{mod}\ 8)$ and $T=\boldsymbol{Q}_2((-2)^{1/2})$ if $a_1\equiv 3\ (\mathrm{mod}\ 8)$. □

In the following we may assume that $0<d\leqq k$.

THEOREM 19. *Let* $K=\boldsymbol{Q}(a^{1/2^k})$, *a has form* $(*)$ *and* $d>0$. *If* $a_1\equiv -3 \pmod 8$ *then* $K_{(2)}=\boldsymbol{Q}$. *If* $a_1\equiv 3 \pmod 8$ *then* $K_{(2)}=\boldsymbol{Q}(\zeta_4)$.

PROOF. If $a_1\equiv \pm 3 \pmod 8$ then $x^{2^k}-a$ is irreducible over $\boldsymbol{Q}_2$. Set $F=\boldsymbol{Q}_2(a^{1/2^k})$ and let s be such that $T\subset \boldsymbol{Q}_2(\zeta_{2^s})$.

Since $\boldsymbol{Q}_2(a^{1/2})\neq \boldsymbol{Q}_2(\zeta_4)$ we see that $\zeta_4\notin F$, $F/\boldsymbol{Q}_2$ has the usp by Prop. 3 b), c), $h=1$, and $F\cap \boldsymbol{Q}_2(\zeta_{2^\infty})=\boldsymbol{Q}_2$. By Cor. 17 we have that $[T:\boldsymbol{Q}_2]\leqq 2$. Further since $f(F/\boldsymbol{Q}_2)=2$ if $a_1\equiv -3 \pmod 8$, Cor. 17 gives that $T=\boldsymbol{Q}_2$, so $K_{(2)}=\boldsymbol{Q}$.

If $a_1\equiv 3 \pmod 8$ then $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(3^{1/2})$ and it is easy to check that $\boldsymbol{Q}_2(3^{1/2}, \zeta_4)/\boldsymbol{Q}_2(3^{1/2})$ is unramified thus $F(\zeta_4)/F$ is unramified, so $T=\boldsymbol{Q}_2(\zeta_4)$, thus $K_{(2)}=\boldsymbol{Q}(\zeta_4)$. □

THEOREM 20. *Let* $K=(a^{1/2^k})$, *a has form* $(*)$ *and* $d>0$. *If* $a_1\equiv 1 \pmod 8$ *then* $K_{(2)}=0$.

PROOF. In order to prove this theorem we must go back to the proof of Th. 7 for the case $a_1\equiv 1 \pmod 8$. We will use the notation developed there.

There are two cases to be considered, $t\leqq d$ and $t>d$, where $a_1=b_1^{2^t}$ and if $t<k$ then $b_1\equiv \pm 3 \pmod 8$. If $t=d=k$, then $2O_K$ has a divisor P with $K_P=\boldsymbol{Q}_2$, which implies that $K_{(2)}=\boldsymbol{Q}$. Thus we may assume that if $k=d$ then $t<k$.

In both cases, that is, $t\leqq d$ and $t>d$, $x^{2^k}-a$ has two irreducible factors of the form

$$x^{2^r}-b\ , \qquad x^{2^r}+b$$

where (i) if $t\leqq d$, $r=k-t$ and $b=2^{2^{d-t}}b_1$, $b_1\equiv -3 \pmod 8$ and (ii) if $t>d$, $r=k-d$ and $b=2b_1^{2^{t-d}}$.

Let T_1, T_2 be the maximal subfields of $\boldsymbol{Q}_2(\zeta_{2^\infty})$ with the property that $T_1\boldsymbol{Q}_2(b^{1/2^r})/\boldsymbol{Q}_2(b^{1/2^r})$ and $T_2\boldsymbol{Q}_2((-b)^{1/2^r})/\boldsymbol{Q}_2((-b)^{1/2^r})$ are unramified.

If $t\leqq d$, then by Th. 19, $T_1=\boldsymbol{Q}_2$, so $K_{(2)}=\boldsymbol{Q}$.

If $t>d$ then by the local interpretation of Th. 18, $T_1=\boldsymbol{Q}_2(2^{1/2})$, $T_2=\boldsymbol{Q}_2((-2)^{1/2})$, thus $T_1\cap T_2=\boldsymbol{Q}_2$, so $K_{(2)}=\boldsymbol{Q}$. □

If $a_1\equiv -1 \pmod 8$ then $-a_1\in \boldsymbol{Q}_2^2$. Define s to be the maximal integer $\leqq k$ for which $-a_1\in \boldsymbol{Q}_2^{2^s}$. Thus $-a_1=b_1^{2^s}$. If $s<k$ then $b_1\equiv \pm 3 \pmod 8$.

THEOREM 21. *Let* $K=\boldsymbol{Q}(a^{1/2^k})$, *a has form* $(*)$, $d>0$ *and* $a_1\equiv -1 \pmod 8$. *If* $d=1$, *then* $K_{(2)}=\boldsymbol{Q}(\zeta_4)$. *If* $d=k=s$, $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{k+1}})$. *If* $1<d<k$ *or if* $s<d=k$, *then* $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{r+2}})$, $r=\min\{d, s\}$.

PROOF. Since $d>0$, $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(\zeta_4)$, thus $K_{(2)}\supset\boldsymbol{Q}(\zeta_4)$.

If $d=1$ then there is an anomaly in the factorization of 2 in O_K. If $a_1\equiv 7 \pmod{16}$ then by Th. 7 C) $2O_K=P^{2^{k-1}}$, $f(P/2)=2$. By Cor. 17 we obtain that $r=0$, so $T\subset\boldsymbol{Q}_2(a^{1/2^k})$. However, from $a=-(2\cdot 3)^2c^4$, $\boldsymbol{Q}_2(a^{1/4})=\boldsymbol{Q}_2(\zeta_4, \zeta_3)$ (see the proof of Th. 7 C)). If $h\geqq 3$ then we would have $\zeta_8\in\boldsymbol{Q}_2(a^{1/2^k})$, so by Prop. 3 d) $\boldsymbol{Q}_2(\zeta_8)=\boldsymbol{Q}_2(a^{1/4})=\boldsymbol{Q}_2(\zeta_4, \zeta_3)$, an impossibility, thus $h=2$ and $\boldsymbol{Q}_2(a^{1/4})\cap\boldsymbol{Q}_2(\zeta_{2^\infty})=\boldsymbol{Q}_2(\zeta_4)$, so $T=\boldsymbol{Q}_2(\zeta_4)$ and $K_{(2)}=\boldsymbol{Q}(\zeta_4)$.

If $a_1\equiv -1 \pmod{16}$ then $a=-4c^4$ and $2O_K=(P_1P_2)^{2^{k-1}}$. Now $\boldsymbol{Q}_2(a^{1/2})=\boldsymbol{Q}_2(\zeta_4)$ and $\boldsymbol{Q}_2(a^{1/4})=\boldsymbol{Q}_2(a^{1/2})$. Further, $a^{1/2^k}$ satisfies the irreducible binomial $x^{2^{k-2}}-a^{1/4}$ over $\boldsymbol{Q}_2(\zeta_4)$, and thus by Prop. 3 c), $\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2(\zeta_4)$ has the usp. If $\zeta_8\in\boldsymbol{Q}_2(a^{1/2^k})$, then by Prop. 3 c), $\boldsymbol{Q}_2(\zeta_8)=\boldsymbol{Q}_2(a^{1/8})$. However, $a^{1/8}=\zeta_{16}2^{1/4}c^{1/2}$ and $2^{1/4}$ is not contained in any abelian extension of $\boldsymbol{Q}_2$, so $\zeta_8\notin\boldsymbol{Q}_2(a^{1/2^k})$, so the maximal abelian subfield of $\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2$ is $\boldsymbol{Q}_2(\zeta_4)$. Thus $\boldsymbol{Q}_2(a^{1/2^k})\cap\boldsymbol{Q}_2(\zeta_{2^\infty})=\boldsymbol{Q}_2(\zeta_4)$.

Recall that $2^r=[T\colon T\cap\boldsymbol{Q}_2(a^{1/2^k})]=[T(a^{1/2^k})\colon \boldsymbol{Q}_2(a^{1/2^k})]=f(T(a^{1/2^k})/\boldsymbol{Q}_2(a^{1/2^k}))$. If $r>0$, then since $T/\boldsymbol{Q}_2$ is totally ramified, $f(T(a^{1/2^k})/T)>1$. Since $T(a^{1/2^k})/T$ has the usp ($x^{2^{k-2}}-a^{1/4}$ is irreducible over T and $\zeta_4\in T$), we would have that $T(a^{1/8})/T$ (this is a quadratic extension) would be unramified. Thus $T(a^{1/8})=T(\zeta_3)$ is an abelian extension of $\boldsymbol{Q}_2$. But $a^{1/8}=\zeta_{16}2^{1/4}c^{1/2}$, so $2^{1/4}$ would be in an abelian extension of $\boldsymbol{Q}_2$, a contradiction. Thus $r=0$, $T=\boldsymbol{Q}_2(\zeta_4)$, so $K_{(2)}=\boldsymbol{Q}(\zeta_4)$.

In the following we may assume that $d\geqq 2$, which in turn implies that $x^{2^k}-a$ is irreducible over $\boldsymbol{Q}_2$.

If $s<d$ set $b=2^{2^{d-s}}b_1$, $b_1\equiv 3 \pmod 8$, thus $a=-b^{2^s}$, $\boldsymbol{Q}_2(a^{1/2^s})=\boldsymbol{Q}_2(\zeta_{2^{s+1}})$ and $\boldsymbol{Q}_2(a^{1/2^{s+1}})=\boldsymbol{Q}_2(\zeta_{2^{s+2}}3^{1/2})\not\subset\boldsymbol{Q}_2(\zeta_{2^\infty})$, so $h=s+1$ and by Cor. 17, $[T\colon T\cap\boldsymbol{Q}_2(a^{1/2^k})]\leqq 2$. However, an easy calculation shows $T=\boldsymbol{Q}_2(\zeta_{2^{s+2}})$, so $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{s+2}})$.

If $s=d$ set $b=2b_1$ and $a=-b^{2^d}$. If $d=k$, then $\boldsymbol{Q}_2(a^{1/2^k})=\boldsymbol{Q}_2(\zeta_{2^{k+1}})$, so $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{k+1}})$. If $d<k$, then $s<k$, so $b_1\equiv 3 \pmod 8$ and $\boldsymbol{Q}_2(a^{1/2^s})=\boldsymbol{Q}_2(\zeta_{2^{s+1}})$, $\boldsymbol{Q}_2(a^{1/2^{s+1}})=\boldsymbol{Q}_2(\zeta_{2^{s+2}}(2\cdot 3)^{1/2})\not\subset\boldsymbol{Q}_2(\zeta_{2^\infty})$, so $h=s+1$. The same argument as for the case $s<d$ applies and we have that $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{s+2}})$.

If $s>d$, set $b=2b_1^{2^{s-d}}$, thus $a=-b^{2^d}$ and $\boldsymbol{Q}_2(a^{1/2^d})=\boldsymbol{Q}_2(\zeta_{2^{d+1}})$, $\boldsymbol{Q}_2(a^{1/2^{d+1}})=\boldsymbol{Q}_2(\zeta_{2^{d+2}}2^{1/2})=\boldsymbol{Q}_2(\zeta_{2^{d+2}})$, since $d\geqq 2$. Now $\boldsymbol{Q}_2(a^{1/2^{d+2}})=\boldsymbol{Q}_2(\zeta_{2^{d+3}}2^{1/4}c^{1/2})$, $c=b_1^{2^{s-d-1}}$ and this last field cannot be in an abelian extension of $\boldsymbol{Q}_2$ because of the factor $2^{1/4}$. Thus $h=d+1$. By Cor. 17, $[T\colon\boldsymbol{Q}_2(a^{1/2^k})\cap T]\leqq 2$ and $T\supset\boldsymbol{Q}_2(\zeta_{2^{d+2}})$ yields that the only possibility for T is $\boldsymbol{Q}_2(\zeta_{2^{d+3}})$. However, by Lemma 16 we have that since $\boldsymbol{Q}_2(a^{1/2^h})\subset\boldsymbol{Q}_2(\zeta_{2^{d+3}})$, $f(T\cdot\boldsymbol{Q}_2(a^{1/2^k})/\boldsymbol{Q}_2(a^{1/2^k}))=1$, so $T(a^{1/2^k})/\boldsymbol{Q}_2(a^{1/2^k})$ is ramified. Thus $T=\boldsymbol{Q}_2(\zeta_{2^{d+2}})$ and $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{d+2}})$. □

Collecting all of these results together we have the following theorem.

THEOREM 22. *Let $n=2^km$, m odd, x^n-a irreducible over $\boldsymbol{Q}$, $a\in\boldsymbol{Z}$,*

$K=\boldsymbol{Q}(a^{1/n})$, and $p_1, \cdots, p_t$ the distinct odd prime divisors of a. Then

A) *$K_*=K_{(2)}\cdot\prod_{i=1}^{t} K_{(p_i)}$, where $K_{(2)}\subset\boldsymbol{Q}(\zeta_{2^\infty})$, $K_{(p_i)}\subset\boldsymbol{Q}(\zeta_{p_i})$.*

Let $n_i=n/p_i^{v_{p_i}(n)}$.

B) *$K_{(p_i)}$ is the unique subfield of $\boldsymbol{Q}(\zeta_{p_i})$ of degree $(n_i/(v_{p_i}(a), n_i), p_i-1)$ over $\boldsymbol{Q}$.*

Let $2^d=(v_2(a), 2^k)$, $a=2^{v_2(a)}a_1$ odd, where we take $d=k$ if a is odd.

C) *If $d=0$ then if $a_1\equiv 1 \pmod 4$, $K_{(2)}=\boldsymbol{Q}(2^{1/2})$, and if $a_1\equiv 3 \pmod 4$, $K_{(2)}=\boldsymbol{Q}((-2)^{1/2})$.*

If $d>0$ then (i) *if $a_1\equiv 1$ or $-3 \pmod 8$, $K_{(2)}=\boldsymbol{Q}$,*
(ii) *if $a_1\equiv 3 \pmod 8$, $K_{(2)}=\boldsymbol{Q}(\zeta_4)$.*

If $d=1$ and $a_1\equiv -1 \pmod 8$ then $K_{(2)}=\boldsymbol{Q}(\zeta_4)$.

If $d>1$ and $a_1\equiv -1 \pmod 8$ let $2^{s+2}\|a_1+1$. Then
(i) *if $d=k$ and $s\geqq k$, then $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{k+1}})$,*
(ii) *if $d<k$ or if $s<d=k$ then $K_{(2)}=\boldsymbol{Q}(\zeta_{2^{r+2}})$, $r=\min\{d, s\}$.* □

References

[1] M. A. de Orozco and W. Y. Vélez, The lattice of subfields of a radical extension, J. Number Theory, **15** (1982), 388–405.

[2] M. A. de Orozco and W. Y. Vélez, The torsion group of a field defined by radicals, J. Number Theory, **19** (1984), 283–294.

[3] R. Dedekind, *Mathematische Werke*, Vols. II, III, Chelsea, New York, 1969.

[4] A. Fröhlich, The genus field and genus group in finite number fields, Mathematika, **6** (1959), 40–46.

[5] A. Fröhlich, The genus field and genus group in finite number fields, II, Mathematika, **6** (1959), 142–146.

[6] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemporary Math., **24**, Amer. Math. Soc., 1983.

[7] D. Gay, On normal radical extensions of real fields, Acta Arith., **35** (1979), 273–288.

[8] D. Gay, Normal binomials over algebraic number fields, J. Number Theory, **12** (1980), 311–326.

[9] D. Gay and W. Y. Vélez, The torsion group of a radical extension, Pacific J. Math., **92** (1981), 317–327.

[10] R. Gold and M. L. Madan, Some applications of Abyhankhar's lemma, Math. Nachr., **82** (1978), 115–119.

[11] D. Hilbert, *Gesammelte Abhandlungen*, Vol. 1, Chelsea, New York, 1965.

[12] M. Ishida, *The Genus Fields of Algebraic Number Theory*, Springer-Verlag, 1976.

[13] M. Ishida, On the genus fields of pure number fields, Tokyo J. Math., **3** (1980), 163–172.

[14] M. Ishida, On the genus fields of pure number fields II, Tokyo J. Math., **4** (1981), 213–220.

[15] E. Jacobson and W. Y. Vélez, On the adèle rings of radical extensions of the rationals, Archiv Math., **45** (1985), 12–20.

[16] I. Kaplansky, *Fields and Rings*, 2nd ed., University of Chicago Press, Chicago/London, 1972.

[17] K. Komatsu, On the adèle rings of algebraic number fields, Kodai Math. Sem. Rep., **28** (1976), 78–84.

[18] K. Komatsu, On the adèle rings and zeta functions of algebraic number fields, Kodai

Math. J., **1** (1978), 394–400.

[19] H. B. MANN and W. Y. VÉLEZ, Prime ideal decomposition in $F(\mu^{1/m})$, Monatsh. Math. Phys., **81** (1976), 1–8.

[20] H. B. MANN and W. Y. VÉLEZ, On normal radical extensions of the rationals, J. Linear and Multilinear Algebra, **3** (1975), 73–80.

[21] A. SCHINZEL, On linear dependence of roots, Acta Arith., **28** (1975), 161–175.

[22] A. SCHINZEL, Abelian binomials, power residues and exponential congruences, Acta Arith., **32** (1977), 245–274.

[23] W. Y. VÉLEZ, A characterization of completely regular fields, Pacific J. Math., **63** (1976), 553–554.

[24] W. Y. VÉLEZ, On normal binomials, Acta Arith., **36** (1980), 113–124.

[25] W. Y. VÉLEZ, Prime ideal decomposition of $F(\mu^{1/p})$, Pacific J. Math., **75** (1978), 589–600.

[26] E. WEISS, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[27] J. WESTLUND, On the fundamental number of the algebraic number field $K(m^{1/p})$, Trans. Amer. Math. Soc., **11** (1910), 388–392.

[28] J. WOJCIK, Contributions to the theory of Kummer extensions, Acta Arith., **40** (1982), 155–174.

Present Address:
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ARIZONA
TUCSON, ARIZONA 85721, U.S.A.