Kummer Extensions with Few Roots of Unity

TOMA ALBU

Facultatea de Matematică, Universitatea din București,
Str. Academiei 14, RO-70109 Bucharest 1, Romania

Communicated by the Editors
Received June 6, 1990; revised March 26, 1991

Let $K$ be an arbitrary field, $\bar{K}$ an algebraic closure of $K$, $n \geq 1$ a natural number, and $\mu_n(K) = \{z \in \bar{K}, z^n = 1\}$. A finite Kummer extension of $K$ of exponent $n$ with few (resp., many) roots of unity is an extension $K(x_1, ..., x_k)$ of $K$, where $k \in \mathbb{N}^*$, $x_1, ..., x_k \in \bar{K}^*$ are such that $x_i^n \in K$ for all $i$, $1 \leq i \leq k$, and $\mu_n(K) \cap K(x_1, ..., x_k) \subseteq \{1, -1\}$ (resp., $\mu_n(K) \subseteq K$).

We prove that a classical result concerning the evaluation of the degree $[K(x_1, ..., x_k) : K]$ holds equally for finite Kummer extensions of exponent $n$ with few or with many roots of unity, if $\text{Char}(K) \nmid n$. For such an extension $K \subseteq K(x_1, ..., x_k)$ for which $[K(x_1, ..., x_k) : K] = \prod_{1 \leq i \leq k} [K(x_i) : K]$, it is shown that $K(x_1, ..., x_k) = K(x_1 + \cdots + x_k)$. Further, if $K$ is an arbitrary field and $n$ is a prime number other than $\text{Char}(K)$, then any extension $K \subseteq K(x_1, ..., x_k)$, where $k \in \mathbb{N}^*$ and $x_1, ..., x_k \in \bar{K}^*$ are such that $x_i^n \in K$ for all $i$, $1 \leq i \leq k$, is a finite Kummer extension of exponent $n$ with few or with many roots of unity, and, consequently, the above results hold in this case.

Our results complete, unify, or extend some of the results of J. L. Mordell, H. Hasse, A. Baker and H. M. Stark, I. Kaplansky, I. Richards, and H. D. Ursell appearing in the literature, and reveal the connections between them. © 1992 Academic Press, Inc.

A nice result of Besicovitch [3] states that if $k \in \mathbb{N}^*$, $p_1, ..., p_k$ are different positive prime integers, $b_1, ..., b_k$ are positive integers not divisible by any of these primes, $a_1 = b_1 p_1, ..., a_k = b_k p_k$, and $x_1, ..., x_k$ are positive real roots of the polynomials $X^{n_1} - a_1, ..., X^{n_k} - a_k$, respectively, where $n_1, ..., n_k \in \mathbb{N}^*$ are arbitrary, then

$$[\mathbb{Q}(x_1, ..., x_k) : \mathbb{Q}] = n_1 \cdot \cdots \cdot n_k.$$ 

As an immediate consequence one deduces that

$$[\mathbb{Q}(\sqrt{n_1 p_1}, ..., \sqrt{n_k p_k}) : \mathbb{Q}] = n^k$$

for any $n \in \mathbb{N}^*$. Another proof of this last equality, using elementary Galois theory, was given by Richards [11] (see also Gaal [5], where the Richards 322
proof is reproduced). A result of the same nature has been established by Ursell [13] (see Sect. 5).

An extension of Besicovitch's result to algebraic number fields satisfying certain conditions is due to Mordell [9] (see 5.5).

All these results deal with a particular case of the following:

**Problem 1.** Let $K$ be a field, $\bar{K}$ an algebraic closure of $K$, and $x_1, \ldots, x_k \in \bar{K}$ of degree $n_1, \ldots, n_k$, respectively, over $K$. When does the field $K(x_1, \ldots, x_k)$ have degree $n_1 \cdot \cdots \cdot n_k$ over $K$?

A more precise problem is as follows.

**Problem 2.** With the same notations and hypotheses as in Problem 1, is it possible to find an algorithm for the computation of $[K(x_1, \ldots, x_k) : K]$?

Partial answers to this last problem are given by a well-known result on (classical) finite Kummer extensions (see 3.4) as well as a result appearing in Kaplansky [7, Theorems 60 and 64] and extended by Baker and Stark [1].

The aim of the present paper is to unify and extend all the above-mentioned results appearing in the literature, as well as to reveal the connections between them. We shall investigate extensions of the type $K \subseteq K(x_1, \ldots, x_k)$, where $K$ is an arbitrary field and $x_1, \ldots, x_k$ are radical elements in an algebraic closure $\bar{K}$ of $K$ (this means that for each $i$, $1 \leq i \leq k$, some power $x_i^n$ of $x_i$ lies in $K$); we find conditions on the field $K$, including all the conditions appearing in the results above, under which we can solve Problem 2 affirmatively and exhaustively. As a consequence, we obtain necessary and sufficient conditions under which Problem 1 holds for such extensions.

More precisely, we define the notion of a finite Kummer extension of exponent $n$ with few (resp., many) roots of unity as an extension $K \subseteq K(x_1, \ldots, x_k)$, where $k \in \mathbb{N}^*$, and $x_1, \ldots, x_k \in \bar{K}^*$ are such that $x_i^n \in K$ for all $i$, $1 \leq i \leq k$, and $\mu_n(\bar{K}) \cap K(x_1, \ldots, x_k) \subseteq \{1, -1\}$ (resp., $\mu_n(\bar{K}) \subseteq K$), where $\mu_n(\bar{K}) = \{z \mid z \in \bar{K}, z^n = 1\}$. The classical finite Kummer extensions of exponent $n$ are exactly the finite Kummer extensions of exponent $n$ with many roots of unity for which the characteristic $\text{Char}(K)$ of $K$ does not divide $n$.

We prove mainly that the classical result concerning the evaluation of the degree $[K(x_1, \ldots, x_k) : K]$ holds equally for finite Kummer extensions of exponent $n$ with few or with many roots of unity if $\text{Char}(K) \nmid n$; for such an extension it is shown that $[K(x_1, \ldots, x_k) : K] = \prod_{1 \leq i \leq k} [K(x_i) : K]$ if and only if the condition (M) from Mordell's theorem (see 5.5) is satisfied, and in this case $K(x_1, \ldots, x_k) = K(x_1 + \cdots + x_k)$. Further, if $K$ is an arbitrary field and $n$ is a prime number other than $\text{Char}(K)$, then we prove that any
extension $K \subseteq K(x_1, ..., x_k)$, where $k \in \mathbb{N}^*$ and $x_1, ..., x_k \in K^*$ are such that $x_i^n \in K$ for all $i$, $1 \leq i \leq k$ is a finite Kummer extension of exponent $n$ with few or with many roots of unity, and consequently the results above hold in this case.

0. Terminology and Notation

Throughout this paper $K$ denotes a fixed field, $e(K)$ its characteristic exponent (that is, $e(K) = 1$ if $K$ has characteristic 0 and $e(K) = p$ if $K$ has characteristic $p > 0$), and $\Omega$ a fixed algebraically closed field containing $K$ as a subfield.

For an arbitrary nonempty subset $S$ of $\Omega$ and a natural number $n \geq 1$ we shall use the notation

\[ S^* = S \setminus \{0\}, \]
\[ \mu_n(S) = \{x \in S \mid x^n = 1\}, \]
\[ S^n = \{x^n \mid x \in S\}. \]

It is well known that $\mu_n(\Omega)$ is a cyclic subgroup of the multiplicative group $\Omega^*$; it has order $n$ if and only if $n$ and $e(K)$ are relatively prime. By a primitive $n$th root of unity we mean any generator of the group $\mu_n(\Omega)$.

If $x \in \Omega$ is an algebraic element over $K$ then $\text{Irr}(x, K)$ will denote the minimal polynomial of $x$ over $K$. For a field extension $K \subseteq L$ we shall denote by $[L : K]$ its degree and by $\text{Gal}(L/K)$ its Galois group. By an abelian extension we mean a Galois extension (not necessarily finite) having the Galois group abelian. For all other undefined terms and notation concerning field theory the reader is referred to Bourbaki [4].

If $x \in \Omega^*$, then $\dot{x}$ will denote throughout this paper the coset $xK^*$ in the quotient group $\Omega^*/K^*$. The order of an element $g$ of a group $G$ will be denoted by $\text{ord}(g)$. If $M$ is a finite set, then $|M|$ will signify the number of elements of $M$.

1. A. Vahlen-Caelli Like Criterion for the Reducibility of Binomials

The following result is well known (see, e.g., Kaplansky [7], Lang [8], or Tchebotarow [12]).

The Vahlen-Caelli Criterion. Let $K$ be an arbitrary field, $a \in K^*$ and $n \in \mathbb{N}$, $n \geq 2$. Then $X^n - a$ is reducible in $K[X]$ if and only if either (i) there exists $s \in \mathbb{N}$, $s > 1$, $s \mid n$, such that $a \in K^s$, or (ii) $4 \mid n$ and $-4a \in K^*$. 


By imposing additional conditions on $K$ or on the binomial $X^n - a$, the somewhat uncomfortable statement (ii) above can be deleted. The main purpose of this section is to show that under such a condition, suggested by the lemma from Mordell [9], namely the condition $(\ast)$ below, the Vahlen-Capelli criterion works only with (i).

1.1. Lemma. Let $X^n - a \in K[X]$ with $a \in K^*$ and $n \geq 2$. Suppose that the following condition is satisfied:

$(\ast)$ There exists a subfield $E$ of $\Omega$, $E \supseteq K$, such that $E$ contains a certain root, say $\sqrt[n]{a}$, of $X^n - a$, and $\mu_n(E) \subseteq K$.

Then, the following assertions hold:

(i) $X^n - a$ is reducible over $K$ if and only if there exists $s \in \mathbb{N}$, $s > 1$ such that $s \mid n$ and $a \in K^s$.

(ii) $\text{Irr}(\sqrt[n]{a}, K) = X^n - b$ for some $b \in K^*$ and some divisor $m$ of $n$; more precisely, $m = \text{ord}(\sqrt[n]{a})$ in the quotient group $\Omega^* / K^*$, and $b = \sqrt[n]{a^m}$.

Proof. Let $f = \text{Irr}(\sqrt[n]{a}, K)$. Then $f$ is a product in $\Omega[X]$ of $m$ binomials of the type $X - \zeta^l \sqrt[n]{a}$, where $m$ is the degree of $f$ and $\zeta$ is a primitive $n$th root of unity; hence the constant term $b_0$ of $f$ has the form

$$b_0 = \pm \zeta^r \sqrt[n]{a^m}.$$  

This implies $\zeta^r = \pm b_0 \zeta^{-m} \in E \cap \mu_n(\Omega) = \mu_n(E) \subseteq K$, and so $\sqrt[n]{a}$ is a root of the polynomial

$$X^m - b \in K[X],$$

where $b = \pm b_0 \zeta^{-r}$. Consequently $f = \text{Irr}(\sqrt[n]{a}, K) = X^n - b$.

Clearly, if $a \in K^s$ for some $s \in \mathbb{N}$, $s > 1$, $s \mid n$, then $X^n - a$ is reducible over $K$. Conversely, suppose that $X^n - a$ is reducible over $K$; in this case $1 \leq m < n$. Let us denote $d = (m, n)$; then $n = ds$, $m = dt$, and $(s, t) = 1$; hence there exist $u, v \in \mathbb{Z}$ such that $ut + vs = 1$. If we denote $x = \sqrt[n]{a}$, then $a = x^{ds}$, $b = x^{dt}$, and so $a' = b'$. Consequently

$$a = a^{st} + vs = a^{st}b^{ns} = (a^tb^s)^e \in K^e.$$

Note that $s \mid n$, and $m < n$ implies $s > 1$.

It remains to prove that $m = \text{ord}(\sqrt[n]{a})$. Denote $k = \text{ord}(\sqrt[n]{a})$; then $x^k \in K^*$ where $x = \sqrt[n]{a}$, and $k$ is the least integer $> 0$ such that $b' = x^k \in K^*$. Since $x^n = a \in K^*$, it follows by the definition of $k$ that $k \mid n$.

We claim that $\text{Irr}(x, K) = X^k - b'$; i.e., $X^k - b'$ is an irreducible polynomial over $K$. Indeed, suppose that $X^k - b'$ is a reducible polynomial over $K$. Note that the first part of the lemma is valid for the polynomial $X^k - b'$.
instead of the polynomial \( X^n - a \) since \( k \mid n \) implies \( \mu_k(E) \subseteq \mu_n(E) \subseteq K \), and consequently the condition \((\ast)\) is fulfilled for the polynomial \( X^k - b' \). Thus \( b' = c^p \) for some \( c \in K^* \) and \( p \in \mathbb{N}, \ p > 1, \ p \mid k \). Then \( k = pq > q \), where \( q \in \mathbb{N} \), and

\[
b' = X^k = \sqrt[1/p]{q} = (\sqrt[1/p]{a})^p = c^p,
\]

so \( \sqrt[1/p]{a} \cdot c^{-1} \in \mu_p(\Omega) \cap E = \mu_p(E) \subseteq \mu_n(E) \subseteq K \). Therefore \( x^q = \sqrt[1/p]{a}^q \in K^* \) with \( 1 \leq q < k \), contradicting the definition of \( k \).

Consequently \( \text{Irr}(\sqrt[1/p]{a}, K) = X^k - b' = X^m - b \); hence \( m = k, \ m \mid n, \) and \( m = \text{ord}(\sqrt[1/p]{a}) \). The proof is now complete.

Clearly, the condition \((\ast)\) from 1.1 is satisfied if and only if the polynomial \( X^n - a \) has a certain root in \( \Omega \), say \( \sqrt[1/p]{a} \), such that \( \mu_n(K(\sqrt[1/p]{a})) \subseteq K \).

1.2. Remark. With the notations and hypotheses of 1.1, let \( d \) be the coset of \( a \) in the quotient group \( K^*/K^{*n} \). If \( d \) is the greatest divisor of \( n \) such that \( a \in K^*d \), then

\[
\text{ord}(\sqrt[1/p]{a}) = \text{ord}(\hat{d}) = n/d.
\]

Indeed, it is clear that the condition \((\ast)\) from 1.1 implies \( \text{ord}(\sqrt[1/p]{a}) = \text{Min}\{s \mid s \in \mathbb{N}^*, \ \sqrt[1/p]{a}^s \in K^*\} = \text{Min}\{s \mid s \in \mathbb{N}^*, \ a^s \in K^{*n}\} = \text{ord}(\hat{d}) \). Denote \( k = \text{ord}(\sqrt[1/p]{a}) \). Then \( (\sqrt[1/p]{a}^{n/d})^d = a - b^d \) for some \( b \in K^* \); hence \( \sqrt[1/p]{a}^{n/d} b^{-1} \in \mu_d(\Omega) \cap E \subseteq \mu_n(E) \subseteq K \). Thus \( \sqrt[1/p]{a}^{n/d} \in K^* \), and so, by the definition of \( k \), \( k \mid n/d \), i.e., \( n/d = kt \) for some \( t \in \mathbb{N}^* \). If \( t > 1 \), then \( a = \sqrt[1/p]{a} = \sqrt[1/p]{a}^k d^t = c^d \in K^{*d} \), where \( c = \sqrt[1/p]{a}^k \in K^* \), contradicting the definition of \( d \). Consequently \( \text{ord}(\sqrt[1/p]{a}) = n/d \).

1.3. Proposition. With the notations and hypotheses of 1.1, let \( m - [K(\sqrt[1/p]{a}) : K] \). Then, the mapping

\[
a: \mathcal{D}(m) \to \mathcal{N}
\]

\[
a(d) = K(\sqrt[1/p]{a}^d)
\]

establishes an antiisomorphism of lattices between the lattice \( \mathcal{D}(m) \) of all natural divisors of \( m \) and the lattice \( \mathcal{N} \) of all subfields of \( K(\sqrt[1/p]{a}) \) containing \( K \).

Proof. By 1.1, \( m = \text{ord}(\sqrt[1/p]{a}) \) and \( \text{Irr}(\sqrt[1/p]{a}, K) = X^m - b \) for some \( b \in K^* \). Denote \( \sqrt[1/p]{b} = \sqrt[1/p]{a} \) and let \( d \in \mathcal{D}(m) \). Then clearly \( \sqrt[1/p]{b}^d \) is a root of the polynomial \( X^m - b^d \), so we can denote it by \( \sqrt[1/p]{b}^d \). According to 1.1,

\[
[K(\sqrt[1/p]{b}^d) : K] = [K(\sqrt[1/p]{b}^d) : K] = \text{ord}(\sqrt[1/p]{b}^d) = \text{ord}(\sqrt[1/p]{b}^d)
\]

\[
= m/(m, \ d) = m/d.
\]
It follows that for every \( d \in \mathcal{O}(m) \) there exists \( L \in \mathcal{X} \), namely \( K(f_{mid}) \) such that \([L : K] = d\). If \( d, \in \mathcal{O}(m)\) and \( \sigma(d_1) = \sigma(d_2) \), then \( K(\sqrt[n]{a_d}) = K(\sqrt[n]{a_{d_2}}) \); hence \([K(\sqrt[n]{b_{d_1}}) : K] = [K(\sqrt[n]{b_{d_2}}) : K]\), and so \( m/d_1 - m/d_2, i.e., d_1 = d_2 \). Consequently \( \sigma \) is injective.

Now let \( F \in \mathcal{X} \), and consider \( g = \text{Irr}(\sqrt[n]{b}, F) \). Then \( g \in F[X] \) and \( K(\sqrt[n]{b}) = F(\sqrt[n]{b}) \). Clearly \( F \) satisfies the condition (\( \ast \)) from 1.1 with respect to the polynomial \( X^m - b \in F[X] \); hence \( \text{Irr}(\sqrt[n]{b}, F) = X^s - c \) for some \( s \in \mathbb{N}^*, s \mid m \), and some \( c \in F \). Then \( \sqrt[n]{b}^s - c \in F \).

We claim that \( K(\sqrt[n]{b^s}) = F \). Obviously we have \( K(\sqrt[n]{b^s}) \subseteq F \). On the other hand, \([K(\sqrt[n]{b}) : F] = [F(\sqrt[n]{b}) : F] = s\); hence \([F : K] = m/s\); but \([K(\sqrt[n]{b^s}) : K] = m/s\) as we have already seen above. It follows that necessarily \( F = K(\sqrt[n]{b^s}) = \sigma(s) \). Therefore, \( \sigma \) is surjective, and consequently \( \sigma \) is a bijective mapping. Since \( \sigma \) is clearly decreasing, it follows that \( \sigma \) is actually an antiisomorphism of lattices.

**Definition.** We say that the field \( K \) satisfies the condition (\( \ast \)) with respect to the polynomial \( X^n - a \), where \( n \in \mathbb{N}, n \geq 2, \) and \( a \in K^* \), if there exists a subfield \( E \) of \( \Omega \) with \( KG \subseteq E \) such that \( E \) contains a certain root of \( X^n - a \), and \( \mu_n(E) \subseteq K \).

### 1.4. Examples.

(i) Suppose that \( \mu_n(\Omega) \subseteq K \) for some \( n \in \mathbb{N}, n \geq 2 \); then clearly \( K \) satisfies the condition (\( \ast \)) with respect to \( X^n - a \) for any \( a \in K^* \).

(ii) If \( n \in \mathbb{N}, n \geq 2, a \in K^* \), and there exists a subfield \( E \) of \( \Omega, E \supseteq K \), such that \( E \) contains a certain root of \( X^n - a \) and \( \mu_n(E) \subseteq \{1, -1\} \), then obviously \( K \) satisfies the condition (\( \ast \)) with respect to \( X^n - a \); this happens for instance if \( K \) is any subfield of \( \mathbb{R} \) (take in this case \( E = \mathbb{R} \)), and either \( n \) is an arbitrary odd number and \( a \in K^* \) is arbitrary or \( n \) is an arbitrary even number and \( a \in K^* \) is positive.

(iii) If \( n \) is a prime number and \( a \in K \setminus K^n \), then a classical result due to Abel asserts that \( X^n - a \) is irreducible in \( K[X] \), without any additional condition on \( K \). For completeness, we include a proof here:

Let \( \sqrt[n]{a} \in \Omega \) be an arbitrary root of \( X^n - a \), and denote \( f = \text{Irr}(\sqrt[n]{a}, K) \).

With notations from the proof of 1.1, we have \( b_0 = \pm \zeta \cdot \sqrt[n]{a}^m \), where \( b_0 \) is the constant term of \( f \) and \( m \) is the degree of \( f \). Suppose that \( X^n - a \) is reducible over \( K \); then \( 1 \leq m < n \); hence \( 1 = um + vn \) for some \( u, v \in \mathbb{Z} \). So

\[
\sqrt[n]{a} = \sqrt[n]{a}^um \cdot \sqrt[n]{a}^vm = a^n \cdot (\pm b_0\zeta^{-r})^v;
\]

hence \( \sqrt[n]{a} \cdot \zeta^u \in K \) and \( (\sqrt[n]{a} \cdot \zeta^u)^n = a \), contradicting the condition \( a \in K \setminus K^n \).

We show now that any field \( K \) satisfies the condition (\( \ast \)) with respect to any binomial \( X^n - a \in K[X] \), \( a \in K^* \), having prime degree \( n \). Indeed, if
n = e(K) then μ_n(Ω) = {1} ≤ K. We can therefore assume that n ≠ e(K); then μ_n(Ω) ∩ K* is a subgroup of the group μ_n(Ω) having order n; hence μ_n(Ω) ∩ K* = μ_n(Ω) or μ_n(Ω) ∩ K* = {1}. If μ_n(Ω) ∩ K* = μ_n(Ω), then μ_n(Ω) ≤ K.

Suppose now that μ_n(Ω) ∩ K* = {1} and let \(\sqrt[n]{a} \in Ω\) be an arbitrary root of \(X^n - a\) if \(a \notin K^n\) and \(\sqrt[n]{a} = b\) if \(a = b^n\) for some \(b \in K\). If we take \(E = K(\sqrt[n]{a})\) we claim that μ_n(Ω) ∩ E* ≠ μ_n(Ω). This is clear when \(a \in K^n\) because \(E = K(\sqrt[n]{a}) = K\) and μ_n(Ω) ∩ E* = \{1\} ≠ μ_n(Ω).

Consider now the case when \(a \notin K^n\) and assume that μ_n(Ω) ∩ E* = μ_n(Ω). Then μ_n(Ω) ≤ E; hence \(K(\zeta) \subseteq K(\sqrt[n]{a})\), where \(\zeta \in μ_n(Ω)\) is a primitive n'th root of unity. On the other hand, \(X^n - a\) is irreducible in \(K[X]\) as we have already seen; hence \([K(\sqrt[n]{a}) : K] = n\). But \(K(\zeta) \subseteq K(\sqrt[n]{a})\), and so \([K(\zeta) : K]\) = \([K(\sqrt[n]{a}) : K]\). Since \([K(\zeta) : K]\) ≤ e(n) = n - 1 we have necessarily \([K(\zeta) : K] = 1\), i.e., \(\zeta \in K\). Then \(\zeta \in μ_n(Ω)\) and \(K(\zeta) = \{1\}\), a contradiction. Thus μ_n(Ω) ∩ E* ≠ μ_n(Ω), and therefore μ_n(Ω) ∩ E* = \{1\}.

In conclusion, if n is a prime number and \(a \notin K^n\), then either μ_n(Ω) ⊆ K or μ_n(Ω) ∩ K* = \{1\}; if μ_n(Ω) ∩ K* = \{1\}, then μ_n(Ω) = \{1\}, where \(\sqrt[n]{a}\) is an arbitrary root in Ω of the binomial \(X^n - a\) if \(a \notin K^n\), and \(\sqrt[n]{a} = b\) if \(a = b^n\) for some \(b \in K\).

(iv) The field \(Q\) does not satisfy the condition (*) with respect to the binomial \(X^4 + 4\). Indeed, any extension \(E\) of \(Q\) containing at least one of the roots \(1 + i, -1 - i, -1 + i, 1 - i\) of \(X^4 + 4\) must contain \(i\); hence μ_4(\(E\)) ⊄ \(Q\). Note that the minimal polynomial of each of the 4th roots of \(-4\) is a polynomial of degree 2 which is not a binomial (e.g., \(\text{Irr}(1 + i, Q) = X^2 - 2X + 2\)), and the order in the quotient group \(C*/Q*\) of each such a root is 4.

(v) The field \(Q\) satisfies the condition (*) with respect to the irreducible polynomial \(f = X^4 + 2 \in Q[X]\). Indeed, the complex roots of \(f\) are \((±1 ± i)/\sqrt[4]{2}\). Denote \(α = (1 + i)/\sqrt[4]{2}\); then \(α^2 = \sqrt[4]{2} i\) and \(α^3 = (-1 + i)/\sqrt[4]{2}\). We assert that \(i \notin Q(α)\), for otherwise, it would follow \(\sqrt[4]{2} \in Q(α)\); hence \(Q(\sqrt[4]{2}) = Q(α)\), a contradiction because \(α \in C\setminus R\). Therefore μ_4(Q(α)) ⊆ \{1, -1\}; i.e., \(Q\) satisfies the condition (*) with respect to the binomial \(X^4 + 2\).

(vi) The field \(Q\) does not satisfy the condition (*) with respect to the irreducible polynomial \(g = X^4 + 9 \in Q[X]\). Indeed, the complex roots of \(g\) are \(\sqrt[4]{6} (±1 ± i)/2\). Denote \(β = -\sqrt[4]{6} (1 + i)/2\); then \(β^2 = 3i\) and \(β^3 = -3\sqrt[4]{6} (-1 + i)/2\). Hence \(i \in Q(β)\), which shows that μ_4(Q(β)) = \{1, -1, i, -i\} and so \(β^3 + β^4 = -3\sqrt[4]{6} \in Q(β)\). Thus \(\sqrt[4]{6} \in Q(β)\) and consequently \(Q(β)\) has at least four distinct subfields: \(Q, Q(i), Q(\sqrt[4]{6}), Q(β)\). On the other hand, the set \(Ω(4)\) of all positive divisors of 4 is \{1, 2, 4\}. Thus, the result from 1.3 fails for \(Q(\sqrt[4]{-9})\).
2. A Key Lemma

The aim of this section is to establish a result, inspired by Lemma 2 of Richards [11], which is fundamental in our subsequent investigation.

Recall that $K$ denotes a fixed field and $\Omega$ a fixed algebraically closed field containing $K$ as a subfield.

An important class of fields satisfying the condition (\ast) from 1.1 is described in 1.4 (ii); due to its ubiquity throughout the paper this class deserves a special name:

**Definition.** We say that the field $K$ satisfies the condition $C(n; a)$, where $n \in \mathbb{N}$, $n \geq 2$, and $a \in K^*$, if there exists a subfield $E$ of $\Omega$ with $K \subseteq E$ such that $E$ contains a root of the polynomial $X^n - a$, and $\mu_n(E) \subseteq \{1, -1\}$.

Clearly, $K$ satisfies the condition $C(n; a)$ if and only if the binomial $X^n - a$ has a root in $\Omega$, say $\sqrt[n]{a}$, such that $\mu_n(K(\sqrt[n]{a})) \subseteq \{1, -1\}$.

Suppose that $K$ satisfies the condition $C(n; a)$. Then, if $E$ is a subfield of $\Omega$ as in the definition above, it is obvious that $K$ also satisfies the condition $C(n; b)$ for any $b \in K^*$ for which the binomial $X^n - b$ has a root in $E$; in particular, $K$ satisfies the condition $C(n; a^k)$ for any $k \in \mathbb{N}$. Note that $K$ also satisfies the condition $C(m; a)$ for each $m \in \mathbb{N}$, $m \geq 2$, $m \mid n$.

As examples of fields satisfying the condition $C(n; a)$ we mention the following:

— Any subfield $F$ of $\mathbb{R}$ satisfies the condition $C(n; a)$, where either $n > 2$ is an arbitrary odd number and $a \in F^*$ is arbitrary or $n \geq 2$ is an arbitrary even number and $a \in F$, $a > 0$.

— If $n$ is an arbitrary prime number and $K$ is a field such that $\mu_n(K) \cap K^* = \{1\}$, then $K$ satisfies the condition $C(n; a)$ for any $a \in K^*$ (see 1.4(iii)). In particular, if $K$ is a finite field $F_q$ such that $(n, q - 1) = 1$, then $F_q$ satisfies the condition $C(n; a)$ for any $a \in F_q^*$.

Note that by 1.4, $\mathbb{Q}$ satisfies the condition $C(4; -2)$, but $\mathbb{Q}$ satisfies neither the condition $C(4; -4)$ nor the condition $C(4; -9)$.

When the field $K$ satisfies the condition $C(n; a)$ we shall always denote in the sequel by $\sqrt[n]{a}$ a specified root of the binomial $X^n - a$ such that $\mu_n(K(\sqrt[n]{a})) \subseteq \{1, -1\}$.

2.1. Lemma. Let $n \in \mathbb{N}$, $n \geq 3$, $a \in K^*$, and suppose that $K$ satisfies the condition $C(n; a)$. If $L$ is an arbitrary abelian extension of $K$, then the following assertions hold:

(i) If $n$ is odd, $\sqrt[n]{a} \in L \iff \sqrt[n]{a} \in K$.

(ii) If $n = 4$, $\sqrt[4]{a} \in L \Rightarrow \sqrt[4]{a^2} \in K$. 
Proof. (i) The implication \( \Leftarrow \) is obvious. Suppose now that \( \sqrt[n]{a} \in L \backslash K \). Denote \( x = \sqrt[n]{a} \) and let \( k = \text{ord}(x) \) in \( \Omega^* / K^* \). Then \( x^k = b \in K \), \( k > 1 \), \( k \mid n \), and \( \text{Irr}(x, K) = X^k - b \) by 1.1.

Consider first the case when \( k \) is a prime number. Denote by \( \omega \) a primitive \( k \)th root of unity. Since \( k \mid n \), \( k > 1 \), and \( n \) is odd we have \( k \geq 3 \). But \( [K(x):K] = k \) and \( [K(\omega):K] \leq \varphi(k) = k - 1 \); hence \( x \notin K(\omega) \), for otherwise it would follow

\[
k = [K(x):K] \leq [K(\omega):K] \leq k - 1,
\]
a contradiction.

We claim that \( \text{Irr}(x, K(\omega)) = X^k - b \), for if not, there would be an \( s \in \mathbb{N} \), \( s > 1 \), \( s \mid k \), such that \( b \in K(\omega)^s \), by 1.1. But \( k \) is a prime number; hence \( s = k \), and then \( b \in K(\omega)^k \), i.e., \( x^k = b = y^k \) for some \( y \in K(\omega) \); thus \( x = y\omega^j \in K(\omega) \) for some \( j \in \mathbb{N} \), a contradiction.

Let us consider the following tower of fields:

\[
K \subseteq K(\omega) \subseteq K(\omega, \sqrt[n]{a}).
\]

Two cases arise: \( \text{Char}(K) \neq k \) and \( \text{Char}(K) = k \).

Case 1. \( \text{Char}(K) \neq k \). Then \( K(\omega) \neq K \), for otherwise \( \mu_k(\Omega) \subseteq K \); hence \( \mu_k(\Omega) = \mu_k(\Omega) \cap K \subseteq \mu_n(\Omega) \cap E \subseteq \{1, -1\} \), a contradiction because \( |\mu_k(\Omega)| = k \geq 3 \). Consequently \( [K(\omega):K] = d \geq 2 \). Note that \( [K(\omega):K] = 1 \) for \( k = 2 \).

But \( \omega \) has exactly \( d \) conjugates over \( K \), \( x = \sqrt[n]{a} = \sqrt[k]{b} \) has exactly \( k \) conjugates over \( K \), and \( K \subseteq K(\omega, \sqrt[n]{a}) \) is a Galois extension having degree \( dk \). It follows that any plausible \( K \)-automorphism of \( K(\omega, \sqrt[n]{a}) \) is actually a \( K \)-automorphism (see, e.g., Kaplansky [7, Theorem 61]). Thus we can consider the following elements \( \varphi_1, \varphi_2 \) of \( \text{Gal}(K(\omega, \sqrt[n]{a})/K) \) defined by

\[
\begin{align*}
\varphi_1(\omega) &= \omega, & \varphi_1(\sqrt[n]{a}) &= \sqrt[n]{a}, \\
\varphi_2(\omega) &= \omega^r, & \varphi_2(\sqrt[n]{a}) &= \sqrt[n]{a},
\end{align*}
\]

where \( \omega^r \) is a certain conjugate of \( \omega \) over \( K \) such that \( \omega^r \neq \omega \), possible because \( d \geq 2 \). We have

\[
\begin{align*}
\varphi_1(\varphi_2(\sqrt[n]{a})) &= \varphi_1(\sqrt[n]{a}) = \omega \sqrt[n]{a} \\
\varphi_2(\varphi_1(\sqrt[n]{a})) &= \varphi_2(\omega \sqrt[n]{a}) = \omega^r \sqrt[n]{a}.
\end{align*}
\]

Since \( \omega \neq \omega^r \) it follows that \( \varphi_1 \circ \varphi_2 \neq \varphi_2 \circ \varphi_1 \) and consequently \( \text{Gal}(K(\omega, \sqrt[n]{a})/K) \) is a noncommutative group.

On the other hand, \( K \subseteq L \) and \( K \subseteq K(\omega) \) are abelian extensions; hence the extension \( K \subseteq L(\omega) \) is also abelian (see, e.g., Bourbaki [4, A V. 74,
KUMMER EXTENSIONS

Corollaire, Prop. 1]). We deduce that $K \subseteq K(\omega, \sqrt[5]{a})$ is an abelian extension because

$$\text{Gal}(K(\omega, \sqrt[5]{a})/K) \cong \text{Gal}(L(\omega)/K)/\text{Gal}(L(\omega)/K(\omega, \sqrt[5]{a}))$$

(see, e.g., Bourbaki [4, A V. 66, Corollaire 4]). Thus we have obtained a contradiction, and consequently $x = \sqrt[5]{a} \in K$.

Case 2. Char$(K) = k$. Then $\omega = 1$, and so $K(\omega, \sqrt[5]{a}) = K(\sqrt[5]{a}) = K(\sqrt[5]{b})$. Since $X^k - b$ is a nonseparable irreducible polynomial, the extension $K \subseteq K(\sqrt[5]{a})$ is not a Galois extension. On the other hand, $\sqrt[5]{a} \in L$, and so $K(\sqrt[5]{a}) \subseteq L$. Since $K \subseteq L$ is an abelian extension, it follows that the extension $K \subseteq K(\sqrt[5]{a})$ is also abelian, in particular it is a Galois extension, a contradiction.

Suppose now that ord$(\hat{x}) = k = p_1 p_2 \cdots p_r$, where $r \geq 2$ and $p_1, p_2, \ldots, p_r$ are prime numbers, not necessarily distinct. Then $x = \sqrt[5]{a} = \sqrt[5]{b} \in L$ for some $b \in K$, and

$$(\sqrt[5]{b}^{p_1 \cdots p_r})^{p_1} = \sqrt[5]{b}^k = b;$$

hence $\sqrt[5]{b}^{p_1 \cdots p_r} \in K(\sqrt[5]{a})$ is a root of the binomial $X^{p_1} - b \in K[X]$, and so we can denote this root by $\sqrt[5]{b}$. Clearly ord$(\sqrt[5]{b}) = k/(p_1 \cdots p_r, k) = p_1$, and $p_1 \sqrt[5]{b} \in L$; hence $p_1 \sqrt[5]{b} \in K$ according to the proof given above. Then $\sqrt[5]{b}^{p_1 \cdots p_r} = 1$, a contradiction because ord$(\hat{x}) = p_1 p_2 \cdots p_r$.

(ii) Suppose that $\sqrt[5]{a} \in L$; then ord$(\sqrt[5]{a}) \in \{1, 2, 4\}$ because $\sqrt[5]{a}^4 = 1$. If ord$(\sqrt[5]{a}) = 1$, then $\sqrt[5]{a} \in K$, and so $\sqrt[5]{a}^2 \in K$. If ord$(\sqrt[5]{a}) = 2$ then $\sqrt[5]{a}^2 \in K$.

It remains to consider now the case ord$(\sqrt[5]{a}) = 4$. Then $[K(\sqrt[5]{a}) : K] = 4$ by 1.1. Let $\omega$ be a primitive 4th root of unity contained in $\Omega$.

Two cases arise: Char$(K) \neq 2$ and Char$(K) = 2$.

Case 1. If Char$(K) \neq 2$ then $\omega \in K(\sqrt[4]{a})$, for otherwise it would follow $\omega \in K(\sqrt[4]{a}) \cap \mu_4(\Omega) \subseteq E \cap \mu_4(\Omega) \subseteq \{1, -1\}$, a contradiction. Consequently $[K(\sqrt[4]{a}, \omega) : K(\sqrt[4]{a})] = 2$; hence

$$[K(\omega, \sqrt[4]{a}) : K] = [K(\omega, \sqrt[4]{a}) : K(\sqrt[4]{a})] \cdot [K(\sqrt[4]{a}) : K] = 8.$$ 

But $\omega^4 = 1$ and $\omega^2 = -1$. Since Char$(K) \neq 2$ we have $\omega \notin K$; hence $[K(\omega) : K] = 2$, from which follows that $[K(\omega, \sqrt[4]{a}) : K(\omega)] = 4$. Exactly as in the proof of (i) for the case ord$(\hat{x})$ is prime one shows that Gal$(K(\omega, \sqrt[4]{a})/K)$ is a noncommutative group, a contradiction.

Case 2. If Char$(K) = 2$ then $\omega = 1$, and so $K(\omega, \sqrt[4]{a}) = K(\sqrt[4]{a})$. Continue now as in the case ord$(\hat{x}) = k = \text{Char}(K) > 2$. 

2.2. Remarks. (i) The implication $\sqrt[4]{a^2} \in K \Rightarrow \sqrt[4]{a} \in L$ is not true, the notations and hypotheses being those of 2.1. For this, take $K = Q$, $L = Q(i)$, and $a = 9$.

(ii) Let $K = Q$, $L = Q(\zeta_8)$, and $a = 4$, where $\zeta_8$ is a primitive complex 8th root of unity; then $\sqrt[4]{4} = \sqrt{2} \in Q(\zeta_8)$ but $\sqrt[4]{4} \notin Q$. This shows that the implication $\sqrt[4]{a} \in L \Rightarrow \sqrt[4]{a} \in K$ is not true in general.

(iii) Let $e \in C \setminus R$ with $e^3 = 1$, $K = Q(e)$, and $L = K(\sqrt[4]{2})$, where $\sqrt[4]{2} \in R$. Then $K \subseteq L$ is an abelian extension, $\sqrt[4]{2} \in L$, but $\sqrt[4]{2} \notin K$. Note that $K = Q(e)$ does not satisfy the condition $C(3; 2)$. We have also $\sqrt[4]{-4} \in Q(i)$, but $\sqrt[4]{-4} \notin Q$ because $Q$ does not satisfy the condition $C(4; -4)$. Thus, the result from 2.1 fails for fields $K$ which do not satisfy the condition $C(n; a)$.

(iv) Let $a \in K^*$, $n \in N$, $n \geq 3$, be such that $(n, e(K)) = 1$, and denote by $N$ the splitting field contained in $\Omega$ of the polynomial $X^n - a$. It is well known that the Galois group $Gal(N/K)$ of the Galois extension $K \subseteq N$ is isomorphic to a subgroup of the group of all matrices $(\alpha \beta \gamma \delta)$, $x \in U(Z_n)$, $y \in Z_n$, where $U(Z_n)$ is the group of units of the ring $Z_n$.

If $K$ satisfies the condition $C(n; a)$, then using 2.1 we find that if $n \neq 4$,

$$Gal(N/K) \text{ is abelian } \iff a \in K^n.$$ 

If $n$ is a prime number (other than the characteristic of $K$), then, according to 1.4(iii), either $\mu_n(\Omega) \subseteq K$ or $K$ satisfies the condition $C(n; a)$. Using now the equivalence obtained just above we deduce at once the known result

$$Gal(N/K) \text{ is abelian } \iff \mu_n(\Omega) \subseteq K \text{ or } a \in K^n$$

(see, e.g., Bourbaki [4, A V. 153, Sect. 11, Ex. 6]).

3. Kummer Extensions of Odd Exponent with Few Roots of Unity

Usually, a Kummer extension of a field $K$ means an abelian extension $L$ of $K$ for which there exists an integer $n \geq 2$ with $(n, e(K)) = 1$, such that $\mu_n(\Omega) \subseteq K$ and $Gal(L/K)$ is a group of exponents $n$ (that is, $\sigma^n = 1$ for all $\sigma \in Gal(L/K)$); we say in this case that $L$ is a Kummer extension of exponent $n$.

It is well known (see, e.g., Artin [1]) that if $L$ is a subfield of $\Omega$, then $L$ is a finite Kummer extension of $K$ if and only if there exist integers $r \geq 1$, $n \geq 2$ with $(n, e(K)) = 1$ and elements $a_1, ..., a_r \in K^*$ such that $\mu_n(\Omega) \subseteq K$
and $L = K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$, where $\sqrt[n]{a_k}$ is for each $k$, $1 \leq k \leq r$, an arbitrary root in $\Omega$ of the polynomial $X^n - a_k$.

We extend the notion of Kummer extension as follows.

**Definition.** Let $n \in \mathbb{N}$, $n \geq 2$, and $L$ be a subfield of $\Omega$. We say that $L$ is a finite Kummer extension of $K$ of exponent $n$ if there exists $r \in \mathbb{N}^*$ and $a_1, ..., a_r \in K^*$ such that $L = K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$ and $\mu_n(L) \subseteq K$, where $\sqrt[n]{a_k}$ is for each $k$, $1 \leq k \leq r$, a certain root in $\Omega$ of the polynomial $X^n - a_k$; in case $r = 1$, $L$ is said to be a simple Kummer extension of $K$ of exponent $n$.

In the sequel, by a finite Kummer extension of $K$ we shall always mean an extension as in the above definition. To distinguish such extensions from the Kummer extensions in the usual sense we shall refer to the latter ones as classical Kummer extensions.

Let $L$ be a finite Kummer extension of $K$ of exponent $n$, $L \subseteq \Omega$. Two extreme cases arise:

(i) $\mu_n(\Omega) \subseteq K$;

(ii) $\mu_n(L) \subseteq \{1, -1\}$.

In case (i) we say that $L$ is a finite Kummer extension of $K$ of exponent $n$ with many roots of unity; if additionally $(n, e(K)) = 1$, this corresponds exactly to a classical finite Kummer extension of exponent $n$.

In case (ii) we say that $L$ is a finite Kummer extension of $K$ of exponent $n$ with few roots of unity. This type of Kummer extensions will be thoroughly investigated in the sequel.

Whenever the field $K$ satisfies the condition $C(n; a)$, $K(\sqrt[n]{a})$ is clearly a simple Kummer extension of $K$ of exponent $n$ with few roots of unity. The corresponding condition for obtaining finite Kummer extensions of exponent $n$ with few roots of unity is given by the following.

**Definition.** We say that the field $K$ satisfies the condition $C(n; a_1, ..., a_k)$, where $n \in \mathbb{N}$, $n \geq 2$, $k \in \mathbb{N}^*$, and $a_1, ..., a_k \in K^*$ if there exists a subfield $E$ of $\Omega$ with $K \subseteq E$ such that $E$ contains for each $i$, $1 \leq i \leq k$, a certain root of the polynomial $X^n - a_i$, and $\mu_n(E) \subseteq \{1, -1\}$.

Obviously, $K$ satisfies the condition $C(n; a_1, ..., a_k)$ if and only if for each $i$, $1 \leq i \leq k$, the binomial $X^n - a_i$ has a root in $\Omega$ say $\sqrt[n]{a_i}$, such that $\mu_n(K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k})) \subseteq \{1, -1\}$; in this case, $K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k})$ is a finite Kummer extension of $K$ of exponent $n$ with few roots of unity.

3.1. **Examples.** (i) If $K$ is an arbitrary subfield of $\mathbb{R}$, then taking $E = \mathbb{R}$ we see that $K$ satisfies the condition $C(n; a_1, ..., a_k)$ where either $n \geq 3$
is an arbitrary odd number, \(k \in \mathbb{N}^*\) and \(a_1, \ldots, a_k \in \mathbb{K}^*\) are arbitrary, or \(n \geq 2\) is an arbitrary even number, \(k \in \mathbb{N}^*\) is arbitrary, and \(a_i \in \mathbb{K}^*, \ a_i > 0\) for all \(i, 1 \leq i \leq k\).

(ii) Let \(K\) be an arbitrary field and \(n > 0\) be a prime number such that \(\mu_n(\Omega) \cap \mathbb{K}^* = \{1\}\). If \(k \in \mathbb{N}^*\) and \(a_1, \ldots, a_k \in \mathbb{K}^*\) are arbitrary, then \(K\) satisfies the condition \(C(n; a_1, \ldots, a_k)\). Indeed, let \(E_1 = K(\sqrt[n]{a_1})\), where \(\sqrt[n]{a_1} \in \Omega\) is an arbitrary root of the binomial \(X^n - a_1\) if \(a_1 \notin \mathbb{K}^*\) and \(\sqrt[n]{a_1} - b_1\) if \(a_1 = b_1^n\) for some \(b_1 \in K\). Then \(\mu_n(E_1) = \{1\}\) in view of 1.4(iii).

Let now \(\sqrt[n]{a_2} \in \Omega\) be an arbitrary root of \(X^n - a_2\) if \(a_2 \notin E_1^n\) and \(\sqrt[n]{a_2} = b_2\) if \(a_2 = b_2^n\) for some \(b_2 \in E_1\) and denote \(E_2 = E_1(\sqrt[n]{a_2}) = K(\sqrt[n]{a_1}, \sqrt[n]{a_2})\). Then, again by 1.4(iii) we have \(\mu_n(E_2) = \{1\}\), and so we have \(\mu_n(K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})) = \{1\}\), where \(\sqrt[n]{a_i}\) are defined inductively as above.

Consequently, if \(n\) is a prime number, then either

\[\mu_n(\Omega) \cap \mathbb{K}^* = \{1\},\]

in which case \(K\) satisfies the condition \(C(n; a_1, \ldots, a_k)\) for any \(a_1, \ldots, a_k \in \mathbb{K}^*\), or

\[\mu_n(\Omega) \subseteq \mathbb{K};\]

hence \(K \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})\) is always a finite Kummer extension of exponent \(n\), with few or with many roots of unity.

Note that if \(K\) satisfies the conditions \(C(n; a_1)\) and \(C(n; a_2)\), then \(K\) does not necessarily the condition \(C(n; a_1, a_2)\). For example, \(\mathbb{Q}\) satisfies both the conditions \(C(4; 2)\) and \(C(4; -2)\), but \(\mathbb{Q}\) does not satisfy the condition \(C(4; 2, -2)\), as is easily verified.

If \(K\) satisfies the condition \(C(n; a_1, \ldots, a_k)\) then we shall denote in the sequel for each \(i, 1 \leq i \leq k\), by \(\sqrt[n]{a_i}\) a specified root in \(\Omega\) of the binomial \(X^n - a_i\), such that \(\mu_n(K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})) \subseteq \{1, -1\}\). If \(\mu_n(\Omega) \subseteq \mathbb{K}\) and \(a \in \mathbb{K}^*\), then by \(\sqrt[n]{a}\) we shall denote an arbitrary root in \(\Omega\) of the binomial \(X^n - a\).

3.2. Theorem. Let \(n \geq 3\) be an odd number, \(k \in \mathbb{N}^*, a_1, \ldots, a_k \in \mathbb{K}^*\), and suppose that \(K\) satisfies the condition \(C(n; a_1, \ldots, a_k)\). If \(K \subseteq L\) is an abelian extension such that \(\mu_n(\Omega) \subseteq L \subseteq \Omega\), then

\[[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = [L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L].\]

Proof. We proceed by induction on \(k\). If \(k = 1\), then by 1.1 we have \(\text{Irr}(\sqrt[n]{a_1}, K) = X^m - b\), where \(m | n\) and \(b \in \mathbb{K}^*\). We assert that \(X^m - b\) is irreducible in \(L[X]\), for if not, then again by 1.1, with \(L\) instead of \(K\), there would be an \(s \in \mathbb{N}, s > 1, s | m\), such that \(b = c^s\) for some \(c \in L\). But
$b = \sqrt[n]{a_1^m}$ and $m = st$; hence $b = (\sqrt[n]{a_1})^s$, and so, $\sqrt[n]{a_1}$ is a root in $K(\sqrt[n]{a_1})$ of the binomial $X^s - b$; it follows that we can denote $\sqrt[n]{a_1}$ by $\sqrt[n]{b}$.

Hence $\sqrt[n]{b} = \zeta c$ for some $\zeta \in \mu_s(\Omega) \subseteq \mu_n(\Omega)$, and so $\sqrt[n]{b} \in L$. According to 2.1(i), we deduce that $\sqrt[n]{b} \in K$; then $X^m - b$ is reducible in $K[X]$, a contradiction. Consequently, $X^m - b$ is irreducible in $L[X]$; hence $[L(\sqrt[n]{a_1}) : L] = m = [K(\sqrt[n]{a_1}) : K]$.

Suppose now $k \geq 2$ and denote $K' = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}})$, $L' = L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}}) = K'L$. Then $K' \subseteq K'L$ is a Galois extension and

$$\text{Gal}(K'L/K') \simeq \text{Gal}(L/K' \cap L)$$

(see, e.g., Lang [8, Theorem 4, Chap. VIII, Sect. 1]). Since the group $\text{Gal}(L/K' \cap L)$ is abelian, it follows that $K' \subseteq L'$ is an abelian extension. But $\mu_n(\Omega) \subseteq L'$ and $K'$ satisfies obviously the condition $C(n; a_k)$, so, by the inductive assumption, we get

$$[K' : K] = [L' : L] \quad \text{and} \quad [K'(\sqrt[n]{a_k}) : K'] = [L'(\sqrt[n]{a_k}) : L'];$$

hence

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = [L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L].$$

3.3. Remarks. (i) Let $n \geq 3$ be an odd number, $k \in \mathbb{N}^*$, $a_1, \ldots, a_k \in K^*$, and suppose that $K$ satisfies the condition $C(n; a_1, \ldots, a_k)$. If $E$ is an arbitrary subfield of $\Omega$ containing $K$, such that $\mu_n(E) \subseteq \{1, -1\}$ and $E$ contains for each $i$, $1 \leq i \leq k$, a specified root, say $\sqrt[n]{a_i}$, of the binomial $X^n - a_i$, then arguments similar to those used in the proof of 3.2 show that for any abelian extension $\mathcal{L} \subseteq L$ with $L \subseteq E$ one has

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = [L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L].$$

In particular, if $L$ is an abelian extension of $K$ such that $L \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$, then necessarily $L = K$. Indeed, in this case we have $L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$; hence $[L : K] = 1$ by 3.2, i.e., $L = K$.

(ii) The conclusion of 3.2 fails for $n$ even; for example, $[Q(\sqrt{2}) : Q] = 2$ but $[L(\sqrt{2}) : L] = 1$, where $L = Q(\zeta_8)$ and $\zeta_8$ is a primitive complex 8th root of unity.

Also, the conclusion of 3.2 fails when the field $K$ does not satisfy the condition $C(n; a)$. For this, consider the example discussed in 2.2(iii): $K = Q(\epsilon)$ and $L = K(\sqrt[3]{2})$; one has

$$3 = [K(\sqrt[3]{2} \epsilon) : K] \neq [L(\sqrt[3]{2} \epsilon) : L] = 1.$$

(iii) The result of 3.2 holds also in the following slightly extended setting: Let $k \in \mathbb{N}^*$, $n_1, \ldots, n_k \in \mathbb{N}^*$, and $a_1, \ldots, a_k \in K^*$; suppose that for each $i$,
1 \leq i \leq k$, the binomial $X^n - a_i$ has a specified root in $\Omega$, say $\sqrt[n]{a_i}$, and there exists a subfield $E$ of $\Omega$ containing $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ such that $\mu_n(E) \subseteq \{1, -1\}$. If $[K(\sqrt[n]{a_i}) : K]$ is an odd number for each $i$, $1 \leq i \leq k$, then for any abelian extension $L$ of $K$ such that $\mu_n(\Omega) \subseteq L \subseteq \Omega$ or $L \subseteq E$, one has

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = [L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L].$$

Indeed, this setting can be reduced to that considered in 3.2 by taking as $n$ the least common multiple of the numbers $m_i = [K(\sqrt[n]{a_i}) : K]$, $1 \leq i \leq k$; if $\text{Irr}(\sqrt[n]{a_i}, K) = X^m_i - b_i$, then $\sqrt[n]{a_i} = \sqrt[m_i]{b_i} = \sqrt[n]{b_i^{p_i}}$, where $p_i$ is such that $n = m_i p_i$, $1 \leq i \leq k$, $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) = K(\sqrt[n]{b_1^{p_1}}, \ldots, \sqrt[n]{b_k^{p_k}})$, $n$ is odd, and we can apply 3.2.

Recall now a classical fundamental result concerning finite Kummer extensions with many roots of unity.

3.4. Theorem. Let $n \in \mathbb{N}$, $n \geq 2$, $k \in \mathbb{N}^*$, $K$ a field such that $\mu_n(\Omega) \subseteq K$ and $(n, e(K)) = 1$, and $a_1, \ldots, a_k \in K^*$. Then $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ is an abelian extension (in fact, a classical finite Kummer extension of exponent $n$), and there exists an isomorphism of groups

$$\text{Gal}(K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})/K) \simeq A_n/K^{*n},$$

where $A_n = \{a_1^{j_1} \cdots a_k^{j_k}a^n | a \in K^*, j_i \in \mathbb{Z}, 1 \leq i \leq k\}$. In particular,

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = |A_n/K^{*n}|.$$

Proof. See Artin [1, Satz 32].

3.5. Theorem. Let $n \geq 3$ be an odd natural number, $k \in \mathbb{N}^*$, and $a_1, \ldots, a_k \in K^*$. Suppose that $K$ satisfies the condition $C(n; a_1, \ldots, a_k)$ and $(n, e(K)) = 1$. Then

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = |\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle|,$$

where $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$ is the subgroup of $\Omega^*/K^*$ generated by $\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}$.

Proof. Denote

$$A_n = \{a_1^{j_1} \cdots a_k^{j_k}a^n | a \in K^*, j_i \in \mathbb{Z}, 1 \leq i \leq k\}$$

$$\overline{A}_n = \{a_1^{j_1} \cdots a_k^{j_k}b^n | b \in K(\omega)^*, j_i \in \mathbb{Z}, 1 \leq i \leq k\},$$

where $\omega \in \Omega$ is a primitive $n$th root of unity. Clearly $A_n$ and $\overline{A}_n$ are subgroups of $\Omega^*$ containing $K^{*n}$ and $K(\omega)^{*n}$, respectively.
The identity mapping $1_\Omega^*$ of the group $\Omega^*$ induces a morphism of groups

$$\alpha: A_n/K^{*n} \rightarrow \overline{A}_n/K(\omega)^{*n}$$

$$\alpha(x) = \bar{x},$$

where $\bar{x}$ (resp., $\bar{y}$) denotes the coset of $x \in A_n$ (resp., $y \in \overline{A}_n$) in $A_n/K^{*n}$ (resp., $\overline{A}_n/K(\omega)^{*n}$).

Clearly $\alpha$ is onto. We prove now that $\alpha$ is injective. Let $\bar{a}_1^{n_1} \cdots \bar{a}_k^{n_k} \in \text{Ker}(\alpha)$; then $a_1^{n_1} \cdots a_k^{n_k} \in K(\omega)^{*n}$; hence $\sqrt[n]{a_1^{n_1}} \cdots \sqrt[n]{a_k^{n_k}} \in K(\omega)$, and so, $\sqrt[n]{a_1^{n_1}} \cdots \sqrt[n]{a_k^{n_k}}$, which is by definition the element $\sqrt[n]{a_1^{n_1} \cdots a_k^{n_k}} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ is an element of $K(\omega)$. By 2.1(i) we get $\sqrt[n]{a_1^{n_1} \cdots a_k^{n_k}} = \bar{1}$. Thus, $\alpha$ is an isomorphism of groups.

We prove now that $A_n/K^{*n} \cong \langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$. For this, consider the morphism of groups

$$\varphi: K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})^* \rightarrow K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})^{*n}$$

$$\varphi(x) = x^n.$$

We have $\varphi(\sqrt[n]{a_i}) = a_i$ for all $i$, $1 \leq i \leq k$, and $\varphi(K^*) = K^{*n}$; hence $\varphi$ induces a morphism of groups

$$\bar{\varphi}: K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})^*/K^* \rightarrow K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})^{*n}/K^{*n}.$$

We claim that $\varphi$ is an isomorphism of groups. Indeed, $\varphi$ is obviously onto. Let now $x \in \text{Ker}(\varphi)$; then $x^n = 1$ and hence $x \in \mu_n(\Omega) \cap K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \subseteq \{1, -1\}$, and so $x = 1$ or $x = -1$. If $\text{Char}(K) = 2$ then $1 = -1$; hence $x = 1$. If $\text{Char}(K) \neq 2$ then $1 \neq -1$, and $n$ being odd we have $(-1)^n = \varphi(-1) = -1 \neq 1$; hence $x = 1$. Consequently $\varphi$ is an isomorphism of groups, and therefore so is $\bar{\varphi}$. But clearly $\bar{\varphi}(\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle) = A_n/K^{*n}$; hence

$$\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle \cong A_n/K^{*n}.$$

Applying now 3.2 and 3.4 we find

$$[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = [K(\omega)(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K(\omega)] = |\overline{A}_n/K(\omega)^{*n}| = |A_n/K^{*n}| = |\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle|.$$

Our next main goal is to show that the result of the above theorem also holds for an arbitrary natural number $n$, not necessarily odd.
However, if \( n \) is even, then some of the arguments used in the proof of 3.2 do not work, and so we need to find another way, namely, by looking to subextensions of Kummer extensions with few roots of unity. This is done in the next section.

4. SIMPLE KUMMER SUBEXTENSIONS OF KUMMER EXTENSIONS WITH FEW ROOTS OF UNITY

The aim of this section is to show that a well-known result concerning simple Kummer subextensions of classical finite Kummer extensions (see, e.g., Hasse [6, III, Sect. 9]) also holds for finite Kummer extensions with few roots of unity. The proof which we shall give, inspired by Hasse [6] is essentially based on 3.2 and on the lemma below; it has the advantage that it works equally for both kinds of Kummer extensions, with many as well as with few roots of unity.

4.1. LEMMA. Let \( n \geq 4 \) be an even number, \( a \in K^* \), and suppose that \( K \) satisfies the condition \( C(n; a) \). If \( [K((\sqrt[n]{a}) : K] \) is even, then for any abelian extension \( L \) of \( K \) such that \( \mu_n(\Omega) \subseteq L \subseteq \Omega \) one has

\[
\text{Irr}(\sqrt[n]{a}, K(\sqrt[n]{a}')) = \text{Irr}(\sqrt[n]{a}, L(\sqrt[n]{a}')),
\]

where \( s \in \mathbb{N} \) is such that \([K((\sqrt[n]{a})) : K] = 2 \) (it exists by 1.3).

Proof. By 1.1, \( \text{Irr}(\sqrt[n]{a}, K) = \prod_{b \in \mathbb{Z}} \text{Irr}(\sqrt[n]{a}, K) \). Since \( \sqrt[n]{a} = b \), we can denote by \( \sqrt[k]{b} \) the specified root \( \sqrt[n]{a} \) of \( X^k - b \). By hypothesis, \( k \) is even; hence \( k = 2s \) for some \( s \in \mathbb{N}^* \). One has

\[
b = \sqrt[k]{b}^k = \sqrt[k]{b}^{2s} = (\sqrt[k]{b}^s)^2
\]

hence \( \sqrt[k]{b}^s \) is a root contained in \( K((\sqrt[n]{a}) \) of the binomial \( X^2 - b \). We can therefore denote this root by \( \sqrt[k]{b} \). Clearly \( \sqrt[k]{b} \notin K \), for if not, it would follow that \( X^k - b = (X^s - \sqrt[k]{b})(X^s + \sqrt[k]{b}) \) is reducible over \( K \).

We assert that \( \text{Irr}(\sqrt[k]{b}, K(\sqrt[k]{b})) = X^s - \sqrt[k]{b} \); indeed, if \( X^s - \sqrt[k]{b} \in K(\sqrt[k]{b})[X] \) were reducible, then \([K(\sqrt[k]{b})(\sqrt[k]{b}) : K(\sqrt[k]{b})] < s \), and so

\[
k = [K(\sqrt[k]{b}) : K] = [K(\sqrt[k]{b}) : K] \cdot [K(\sqrt[k]{b})(\sqrt[k]{b}) : K(\sqrt[k]{b})] < 2s = k,
\]

a contradiction.

We must prove that \( X^s - \sqrt[k]{b} \) is an irreducible polynomial over \( L(\sqrt[k]{b}) \). Suppose that \( X^s - \sqrt[k]{b} \in L(\sqrt[k]{b})[X] \) is reducible. Since \( \mu_n(\Omega) \subseteq \mu_n(\Omega) \subseteq L(\sqrt[k]{b}) \) we can apply 1.1; hence there exists \( r \in \mathbb{N} \), \( r > 1 \), such that \( r | s \) and \( \sqrt[k]{b} = c^r \) for some \( c \in L(\sqrt[k]{b}) \). Two cases arise.
Case 1. $r$ has an odd factor $q \geq 3$. Then $r = qq'$ and $s = qt$ for some $q', t \in \mathbb{N}$. Thus

$$(\sqrt[4]{\sqrt{b}})^q = \sqrt[4]{b}^s = \sqrt[b]{b}.$$ 

We can therefore denote by $\sqrt[4]{\sqrt{b}}$ the specified root $\sqrt[4]{b}'$ contained in $K(\sqrt[4]{a})$ of the binomial $X^q - \sqrt[b]{b} \in K(\sqrt[b]{b})[X]$. On the other hand

$$(\sqrt[4]{\sqrt{b}})^q = \sqrt[4]{b} = c^{c^{q'}} = (c^{q'})^r.$$ 

It follows that $\sqrt[4]{\sqrt{b}} = \omega c^{q'} \in L(\sqrt[b]{b})$ for some $\omega \in \mu_q(\Omega) \subseteq L$. But $K(\sqrt[b]{b}) \subseteq L(\sqrt[b]{b})$ is an abelian extension, and $K(\sqrt[b]{b})$ satisfies the condition $C(q; \sqrt[b]{b})$ because the binomial $X^q - \sqrt[b]{b} \in K(\sqrt[b]{b})[X]$ has a root, namely $\sqrt[4]{\sqrt{b}} = \sqrt[4]{b}'$ contained in $K(\sqrt[4]{a})$, $K(\sqrt[b]{b}) \subseteq K(\sqrt[4]{a})$, and $\mu_q(K(\sqrt[4]{a})) \subseteq \mu_q(K(\sqrt[b]{b})) \subseteq \{1, -1\}$. By 2.1(i) applied to the extension $K(\sqrt[b]{b}) \subseteq L(\sqrt[b]{b})$, one has $\sqrt[4]{\sqrt{b}} \in K(\sqrt[b]{b})$, and so $\sqrt[4]{\sqrt{b}} \in K(\sqrt[b]{b})^q$. Since $q | s$ and $q \geq 3$ it follows that $X^s - X^{q} \in K(\sqrt[b]{b})[X]$ is a reducible polynomial, a contradiction.

Case 2. $r = 2^n$ for some $m \in \mathbb{N}^*$. Then $4 | k$ because $2^n | s$, and $\sqrt[b]{b} = c^{2^n} = (c^{2^{n-1}})^2 = d^2$, where $d = c^{2^{n-1}} \in L(\sqrt[b]{b})$; hence $d^q = b = \sqrt[4]{b}^4$ and consequently $\sqrt[4]{b} = \zeta_d \in L$ for some $\zeta \in \mu_4(\Omega) \subseteq \mu_4(\Omega) \subseteq L$. Note that $K$ satisfies the condition $C(4; b)$. By 2.1(ii) we deduce that $\sqrt[4]{b}^2 = \sqrt[b]{b} \in K$, a contradiction.

We conclude that $X^s - \sqrt[b]{b}$ is irreducible over $L(\sqrt[b]{b})$, and so, we are done.

4.2. Remarks. (i) Arguments similar with those used in the proof above show that if $E$ is an arbitrary subfield of $\Omega$ such that $\mu_n(E) \subseteq \{1, -1\}$ and $E$ contains a specified root $\sqrt[n]{a}$ of the binomial $X^n - a$, then

$$\text{Irr}(\sqrt[n]{a}, K(\sqrt[n]{a}^s)) = \text{Irr}(\sqrt[n]{a}, L(\sqrt[n]{a}^s))$$

for any abelian extension $L$ of $K$ with $L \subseteq E$, the notations being those of 4.1.

(ii) With the notations and hypotheses of 4.1 one has clearly

$$[K(\sqrt[n]{a}) : K(\sqrt[n]{a}^s)] = [L(\sqrt[n]{a}) : L(\sqrt[n]{a}^s)].$$

It seems that a similar equality is to be expected also for finite Kummer extensions, but we could not prove it. More precisely, we have the following.
Problem. Let \( n \geq 4 \) be an even natural number, \( k \in \mathbb{N}, k \geq 2, \) and \( a_1, ..., a_k \in K^* \). Suppose that \( K \) satisfies the condition \( C(n; a_1, ..., a_k) \) and that \( [K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] \) is even for each \( i, 1 \leq i \leq k \). Then, for any abelian extension \( L \) of \( K \) such that \( \mu_n(\Omega) \subseteq L \subseteq \Omega \) or \( L \subseteq K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) \) one has

\[
[K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K(\sqrt[n]{a_1^{s_1}}, ..., \sqrt[n]{a_k^{s_k}})] = [L(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : L(\sqrt[n]{a_1^{s_1}}, ..., \sqrt[n]{a_k^{s_k}})],
\]

\[(*)\]

where \( s_1, ..., s_k \in \mathbb{N} \) are such that \( s_i | n \) and \( [K(\sqrt[n]{a_i}) : K] = 2 \) for all \( i, 1 \leq i \leq k \).

In the next section we prove that \((*)\) holds in the case \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K] \) (see 5.10).

(iii) Note that if \( K \) satisfies the condition \( C(n; a) \), then for every subfield \( E \) of \( \Omega \) such that \( \mu_n(E) \subseteq \{1, -1\} \) and \( K(\sqrt[n]{a}) \subseteq E \), the number \([F(\sqrt[n]{a}) : F] \) is a divisor of \([K(\sqrt[n]{a}) : K] \) for any subfield \( F \) of \( K \), containing \( K \). Indeed, it is clear that \( F \) satisfies the condition \( C(n; a) \). If \( k = [K(\sqrt[n]{a}) : K] \), then \( \text{Irr}(\sqrt[n]{a}, K) = x^k - b \) and \( \sqrt[n]{b} = \sqrt[n]{a} \). So \( F(\sqrt[n]{a}) = F(\sqrt[n]{b}) \), and consequently, the degree \([F(\sqrt[n]{b}) : F] \) of the polynomial \( \text{Irr}(\sqrt[n]{b}, F) \) is a divisor of \( k \), by 1.1.

A repeated application of the above argument shows that if the field \( K \) satisfies the condition \( C(a; a_1, ..., a_k) \), then \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] \) is a divisor of \( \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K] \); in particular, if each of the numbers \([K(\sqrt[n]{a_i}) : K] \) is odd, then \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] \) is also odd. Note that if \( K \) does not satisfy the condition \( C(n; a_1, ..., a_k) \), then the result fails; for example, \([\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{-2}) : \mathbb{Q}] = 8 \) and \([\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{-2}) : \mathbb{Q}] = 4 \), where \( \sqrt[4]{2} \in \mathbb{R} \) and \( \sqrt[4]{-2} \) is one of the complex 4th roots of \(-2 \).

(iv) Let \( \sqrt[4]{-9} \) be one of the complex 4th roots of \(-9 \), e.g., \( \sqrt[4]{6}(1+i)/2 \); then \( \sqrt[4]{-9} = 3i \). Consider the abelian extension \( L = \mathbb{Q}(i, \sqrt[4]{6}) \) of \( \mathbb{Q} \). We have

\[
[\mathbb{Q}(\sqrt[4]{-9}) : \mathbb{Q}(\sqrt[4]{-9}^2)] = 2, \quad [L(\sqrt[4]{-9}) : L(\sqrt[4]{-9}^2)] = 1.
\]

Note that \( \mathbb{Q} \) does not satisfy the condition \( C(4; -9) \) (see 1.4(vi)). Thus, the result of 4.1 fails if the field \( K \) does not satisfy the condition \( C(n; a) \).

4.3. Theorem. Let \( n \in \mathbb{N}, n \geq 2, K \) a field with \((n, e(K)) = 1\), and \( a, a' \in K \). Suppose that either \( K \) satisfies the condition \( C(n; a, a') \) or \( \mu_n(\Omega) \subseteq K \). Then \( K(\sqrt[n]{a}) \subseteq K(\sqrt[n]{a'}) \) if and only if there exist \( c \in K^* \) and \( j \in \mathbb{N} \) such that \( a' = a'^c \).

Proof. First of all, recall that \( \sqrt[n]{a} \) and \( \sqrt[n]{a'} \) denote specified roots of the binomials \( X^n - a \) and \( X^n - a' \), respectively, such that \( \mu_n(K(\sqrt[n]{a}, \sqrt[n]{a'})) \subseteq \)
If $a' = a'' c^n$ then $\sqrt[n]{a''} = (\sqrt[n]{a''})^c$, hence $\sqrt[n]{a''} = \pm c \sqrt[n]{a'}$ if $K$ satisfies the condition $C(n; a, a')$ or $\sqrt[n]{a'} = \omega c \sqrt[n]{a'}$ for some $\omega \in \mu_n(\Omega)$ if $\mu_n(\Omega) \subseteq K$. Thus $\sqrt[n]{a'} \in K(\sqrt[n]{a})$, and so $K(\sqrt[n]{a'}) \subseteq K(\sqrt[n]{a})$.

Conversely, suppose that $K(\sqrt[n]{a'}) \subseteq K(\sqrt[n]{a})$ and denote $k = [K(\sqrt[n]{a}) : K]$. Then $k|n$; hence $k = n/d$ for some $d \in \mathbb{N}^*$, $d|n$. Let $\zeta$ be a primitive $n$th root of unity and denote $L = K(\zeta)$.

We shall examine two cases: $k$ is odd and $k$ is even. This division of the proof is unnecessary in the case when $\mu_n(\Omega) \subseteq K$.

**Case 1.** $k$ is odd. Clearly we can assume that $k \geq 3$. Since $\text{Irr}(\sqrt[n]{a}, K) = X^n - b$ for some $b \in K^*$, one has $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$; hence we can apply 3.1 to obtain the equality $[K(\sqrt[n]{a}) : K] = [L(\sqrt[n]{a}) : L] = k$. Since $(n, e(K)) = 1$, it follows that $L \subseteq L(\sqrt[n]{a})$ is a Galois extension, and the map

$$\text{Gal}(L(\sqrt[n]{a})/L) \to \mu_n(\Omega)$$

$$\tau \mapsto \zeta^\tau,$$

where $\tau(\sqrt[n]{a}) = \zeta^t \sqrt[n]{a}$, $t \in \mathbb{N}$, is a group monomorphism; hence $\text{Gal}(L(\sqrt[n]{a})/L)$ is a cyclic group of order $k$. Denote by $\sigma_0$, $\sigma_0(\sqrt[n]{a}) = \zeta^t \sqrt[n]{a}$, a generator of this group; then $\text{ord}(\sigma_0) = \text{ord}(\zeta^t) = n/d$.

Consider the function $\sigma: L(\sqrt[n]{a}) \to L(\sqrt[n]{a})$ defined by $\sigma(\sqrt[n]{a}) = \zeta^d \sqrt[n]{a}$. We assert that $\sigma \in \text{Gal}(L(\sqrt[n]{a})/L)$ and $\langle \sigma \rangle = \langle \sigma_0 \rangle$, where $\langle \sigma_0 \rangle$ denotes the subgroup of $\text{Gal}(L(\sqrt[n]{a})/L)$ generated by $\sigma_0$. We have $\text{ord}(\zeta^d) = n/(n, d) = n/d = k$, because $(n, e(K)) = 1$ and so $\text{ord}(\zeta) = n$. Therefore $\langle \zeta^d \rangle$ is a subgroup of order $k$ of the cyclic group $\mu_n(\Omega)$; but $\langle \zeta^t \rangle$ is also such a subgroup of $\mu_n(\Omega)$, and consequently they must coincide. It follows that $\zeta^d = (\zeta^t)^m$ for some $m \in \mathbb{N}^*$; hence $\sigma = \sigma_0^m$, i.e., $\sigma \in \langle \sigma_0 \rangle$. We deduce that $\sigma \in \text{Gal}(L(\sqrt[n]{a})/L)$, and $\langle \sigma \rangle = \langle \sigma_0 \rangle$ because $\text{ord}(\sigma) = \text{ord}(\zeta^d) = k$.

Since $K(\sqrt[n]{a'}) \subseteq K(\sqrt[n]{a})$, there exists $c_0, c_1, ..., c_k \in K$ such that

$$\sqrt[n]{a'} = \sum_{j=0}^{k-1} c_j \sqrt[n]{a'^j} .$$

Then

$$\sigma(\sqrt[n]{a'}) = \sum_{j=0}^{k-1} c_j \zeta^{dj} \sqrt[n]{a'^j} .$$

On the other hand $(\sigma(\sqrt[n]{a'}))^n = \sigma(a') = a'$; hence there exists $r \in \mathbb{N}$ such that $\sigma(\sqrt[n]{a'}) = \zeta^r \sqrt[n]{a'}$, and so, using $(\ast)$ one gets

$$\sigma(\sqrt[n]{a'}) = \sum_{j=0}^{k-1} c_j \zeta^r \sqrt[n]{a'^j} .$$
But \([L(\sqrt[3]{a}) : L] = [K(\sqrt[3]{a}) : K] = k\) by 3.1, hence \(\{1, \sqrt[3]{a}, \sqrt[3]{a^2}, \ldots, \sqrt[3]{a^{k-1}}\}\) is a basis of the vector space \(L(\sqrt[3]{a})\) over \(L\). It follows that \(c_j \zeta^d = c_j \zeta^r\) for all \(j, 0 \leq j \leq k - 1\). So, if \(dj \not\equiv r \pmod{n}\) for some \(j, 0 \leq j \leq k - 1\), then necessarily we must have \(c_j = 0\).

It is not possible to have \(dj \equiv r \pmod{n}\) for all \(j, 0 \leq j \leq k - 1\), for otherwise it would follow that \(c_j = 0\) for all \(j\), and then \(\sqrt[3]{a} = 0\), a contradiction. Therefore, there exists \(j_0, 0 \leq j_0 \leq k - 1\) such that \(dj_0 \equiv r \pmod{n}\); we cannot have another \(j_0, 0 \leq j_0 \leq k - 1\), \(j_0 \not\equiv j_0\), with \(dj_0 \equiv r \pmod{n}\), for if not we should have \(dj_0 \equiv dj_0 \pmod{dk}\); hence \(j_0 \equiv j_0 \pmod{k}\), a contradiction because \(j_0, j_0 \in \{0, 1, \ldots, k - 1\}\).

Consequently, in the equality (*) above there exists a single \(j, 0 \leq j \leq k - 1\), such that \(c_j \not= 0\), and so \(\sqrt[3]{a} = c_j \sqrt[3]{a^j}\), i.e., \(a' = a^j \cdot c_j\). This completes the proof in the case \(k\) is odd.

Case 2. \(k\) is even. Then, by 1.3, there exists an \(s \in \mathbb{N}, s \mid n\), such that \([K(\sqrt[3]{a}) : K] = 2\). Denote \(K' = K(\sqrt[3]{a})\). Then \(K'(\sqrt[3]{a}) = K(\sqrt[3]{a})\) and \([K'(\sqrt[3]{a}) : K'] = k/2\). But \(k = n/d\); hence \(k/2 = n/2d\). If we denote \(n/2 = n'\), then \(k/2 = n'/d\) and \(d \mid n'\); hence \(2d \mid n\).

The proof in this case will follow the proof given above for \(k\) odd with these changes: \(K'\) instead of \(K\), \(L' = K'(\zeta)\) instead of \(L = K(\zeta)\), \(k' = k/2\) instead of \(k\), and \(d' = 2d\) instead of \(d\); recall that \(\zeta\) denotes a primitive \(n\)th root of unity. These changes are possible because in view of 4.1 one has

\[
[K'(\sqrt[3]{a}) : K'] = [K(\sqrt[3]{a}) : K(\sqrt[3]{a'})] = [L(\sqrt[3]{a}) : L(\sqrt[3]{a'})] = [L'(\sqrt[3]{a}) : L'] = k/2 = k',
\]

\(K'(\sqrt[3]{a'}) \subseteq K'(\sqrt[3]{a})\), and \(K'\) satisfies the condition \(C(n; a, a')\) or \(\mu_n(\mathcal{O}) \subseteq K'\).

With these changes, denote by \(\sigma_0\) the generator of the group \(\text{Gal}(L'(\sqrt[3]{a})/L')\), which is defined by \(\sigma_0(\sqrt[3]{a}) = \zeta^{2d} \sqrt[3]{a}\). Since \(K'(\sqrt[3]{a'}) \subseteq K'(\sqrt[3]{a})\), there exists \(c_0, c_1, \ldots, c_{k' - 1} \in K'\) such that

\[
\sqrt[3]{a'} = \sum_{j=0}^{k'-1} c_j \sqrt[3]{a^j}.
\]

As in the proof of the previous case one deduces that there exists a unique \(j, 0 \leq j \leq k' - 1\), such that \(c_j = 0\) for all \(r, r \in \{0, 1, \ldots, k' - 1\}\); hence \(a' = a^j \cdot c_j\). Denote for brevity \(c_j = c \in K' = K(\sqrt[3]{a'})\). Since \([K(\sqrt[3]{a^3}) : K] = 2\), it follows that there exists \(\lambda, \mu \in K\) such that

\[
c = \lambda + \mu \sqrt[3]{a^3}.
\]

If \(c \in K\), then we are done. Suppose now that \(c \not\in K\); then \([K(c) : K] = 2\). Note that \(c^n = a^r \cdot a^{-j} \in K\); hence \(c\) is a root of the polynomial \(X^n - c^n \in K[X]\), \(c \in K(\sqrt[3]{a})\), and \(\mu_n(K(\sqrt[3]{a})) \subseteq \{1, -1\}\); hence we can apply 1.1 to
conclude that \( \text{Irr}(c, K) = X^2 - d \) for some \( d \in K \). On the other hand, \( c \) is a root of the polynomial

\[
f = X^2 - 2\lambda X + (\lambda^2 - \mu^2 \cdot (\sqrt[n]{a})^2) \in K[X];
\]

hence necessarily \( f = \text{Irr}(c, K) \). It follows that \( \lambda = 0 \); hence \( c = \mu \cdot \sqrt[n]{a} \), and consequently \( c^n = \mu^n \cdot a^i \). Thus \( a' = a^j \cdot c^n = a^{j + i} \cdot \mu^n \), with \( \mu \in K \). The proof is now complete.

4.4. COROLLARY. Let \( n \in \mathbb{N}, n \geq 2, k \in \mathbb{N}^*, K \) a field with \( (n, e(K)) = 1, \) and \( a', a_1, \ldots, a_k \in K \). Suppose that either \( K \) satisfies the condition \( C(n; a', a_1, \ldots, a_k) \) or \( \mu_n(\Omega) \subseteq K \). Then

\[
K(\sqrt[n]{a'}) \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})
\]

if and only if there exist \( j_1, \ldots, j_k \in \mathbb{N} \) and \( c \in K^* \) such that

\[
a' = a_1^{j_1} \cdot \cdots \cdot a_k^{j_k} \cdot c^n.
\]

Proof. One implication is trivial. For the other we proceed by induction on \( k \). The case \( k = 1 \) is exactly the previous theorem. Suppose that the result is true for \( k \) and prove it for \( k + 1 \). So, let \( K(\sqrt[n]{a'}) \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}) \). If we denote \( K' = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \), then \( K' \) satisfies clearly the condition \( C(n; a', a_{k+1}) \) or \( \mu_n(\Omega) \subseteq K' \). Since \( K'(\sqrt[n]{a'}) \subseteq K'(\sqrt[n]{a_{k+1}}) \) we can apply the previous theorem to obtain \( b \in K' \) and \( j_{k+1} \in \mathbb{N} \) with \( a' = a_1^{j_1} \cdot b^n \). Then

\[
b^n = a' \cdot a_{k+1}^{-j_{k+1}} = (\sqrt[n]{a'} \cdot a_{k+1}^{-j_{k+1}})^n.
\]

It follows that

\[
\sqrt[n]{a'} \cdot a_{k+1}^{-j_{k+1}} = \omega b
\]

for some \( \omega \in \mu_n(\Omega) \); if \( \mu_n(\Omega) \subseteq K \) one gets

\[
\sqrt[n]{a'} \cdot a_{k+1}^{-j_{k+1}} \in K',
\]

and if \( K \) satisfies the condition \( C(n; a', a_1, \ldots, a_{k+1}) \) then \( \omega \in \mu_n(\Omega) \cap K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}, \sqrt[n]{a'}) \subseteq \{1, -1\} \), and so

\[
\sqrt[n]{a'} \cdot a_{k+1}^{-j_{k+1}} \in K'.
\]

By the inductive hypothesis, there exist \( j_1, \ldots, j_k \in \mathbb{N} \) and \( c \in K^* \) such that

\[
a' \cdot a_{k+1}^{-j_{k+1}} = a_1^{j_1} \cdot \cdots \cdot a_k^{j_k} \cdot c^n;
\]

that is

\[
a' = a_1^{j_1} \cdot \cdots \cdot a_k^{j_k} \cdot a_{k+1}^{j_{k+1}} \cdot c^n.
\]
4.5. Remark. If $K$ satisfies neither the condition $C(n; a, a')$ nor $\mu_n(\Omega) \subseteq K$, then the result of 4.3 fails. For instance, we have
\[ \mathbb{Q}(\sqrt[4]{6^2}) \subseteq \mathbb{Q}(\sqrt[4]{-9}), \]
where $\sqrt[4]{-9}$ is any of the complex roots of the polynomial $X^4 + 9 \in \mathbb{Q}[X]$, but there exist no $j \in \mathbb{N}$ and $c \in \mathbb{Q}$ such that
\[ \sqrt[4]{6^2} = (\sqrt[4]{-9})^j \cdot c. \]

5. THE MAIN RESULTS: APPLICATIONS

The aim of this section is to establish two main results holding for both kinds of finite Kummer extensions, with few or with many roots of unity, to present some of the consequences of these results, and to connect them with certain known particular results appearing in the literature.

The first one shows that the classical result concerning the degree of a finite Kummer extension of exponent $n$, $K \subseteq K(x_1, \ldots, x_k)$, with many roots of unity (recall that this means that $\mu_n(\Omega) \subseteq K$) and such that $(n, e(K)) = 1$ (see 3.4) also holds for a finite Kummer extension of exponent $n$ with few roots of unity (this means that $\mu_n(K(x_1, \ldots, x_k)) \subseteq \{1, -1\}$). The main component of our proof of this result is 4.4. Note that a proof in the case when the exponent $n$ is odd, without using 4.4, was given in Sect. 3.

The second main result of this section establishes that any finite Kummer extension of exponent $n$, $K \subseteq K(x_1, \ldots, x_k)$, with few or with many roots of unity such that $(n, e(K)) = 1$ and $[K(x_1, \ldots, x_k) : K] = \prod_{1 \leq i \leq k} [K(x_i) : K]$ has $x_1 + \ldots + x_k$ as a primitive element.

5.1. Theorem. Let $n \in \mathbb{N}$, $n \geq 2$, $k \in \mathbb{N}^*$, $K$ a field with $(n, e(K)) = 1$, and $a_1, \ldots, a_k \in K^*$. Suppose that either $K$ satisfies the condition $C(n; a_1, \ldots, a_k)$ or $\mu_n(\Omega) \subseteq K$. Then

\[ [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = \langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle = \langle \hat{a}_1, \ldots, \hat{a}_k \rangle, \]

where $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$ (resp., $\langle \hat{a}_1, \ldots, \hat{a}_k \rangle$) is the subgroup of $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})/K^*$ (resp., $K^*/K^*$) generated by the cosets $\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}$ in the quotient group $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})/K^*$ (resp., by the cosets $\hat{a}_1, \ldots, \hat{a}_k$ in the quotient group $K^*/K^*$).

Moreover, any set of representatives of the cosets of the group $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$ is a vector space basis of the extension $K \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$. 
Proof. First, we shall prove that

\[ \{ \sqrt[n]{a_1^{i_1}} \cdots \sqrt[n]{a_k^{i_k}} \mid 0 \leq i_1 < d_1, \ldots, 0 \leq i_k < d_k \} = d_1 d_2 \cdots d_k, \quad (*) \]

where \( d_1 = [K(\sqrt[n]{a_1}) : K] \), \( d_2 = [K(\sqrt[n]{a_1}, \sqrt[n]{a_2}) : K(\sqrt[n]{a_1})] \), and so on, \( d_k = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}})] \).

For this, we proceed by induction on \( k \). If \( k = 1 \), then according to 1.1, we have

\[ \{ \sqrt[n]{a_1^{i_1}} \mid 0 \leq i_1 < d_1 \} = \text{ord}(\sqrt[n]{a_1}) = [K(\sqrt[n]{a_1}) : K] = d_1. \]

Suppose now that (*) is satisfied for an arbitrary \( k \in \mathbb{N}^* \), and we prove it for \( k + 1 \). Since \( K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \) satisfies the condition \( C(n; a_{k+1}) \) whenever \( K \) satisfies the condition \( C(n; a_1, \ldots, a_k, a_{k+1}) \), we can apply 1.1; hence

\[ d_{k+1} = \text{ord}(\sqrt[n]{a_{k+1}}) \]

in the quotient group \( \Omega_2^*/K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})^* \), where \( x \) denotes the coset of \( x \in \Omega \) in this group. Hence

\[ d_{k+1} = \text{Min}\{d \mid d \in \mathbb{N}^*, \sqrt[n]{a_{k+1}}^d \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})\}. \]

Now let

\[ \sqrt[n]{a_1^{i_1}} \cdots \sqrt[n]{a_k^{i_k}} \sqrt[n]{a_{k+1}^{i_{k+1}}} = \sqrt[n]{a_1^{j_1}} \cdots \sqrt[n]{a_k^{j_k}} \sqrt[n]{a_{k+1}^{j_{k+1}}} \]

where \( 0 \leq i_s, j_s < d_s \) for all \( s, 1 \leq s \leq k + 1 \), and assume that \( i_{k+1} > j_{k+1} \).

Then

\[ \sqrt[n]{a_{k+1}^{i_{k+1} - j_{k+1}}} = \sqrt[n]{a_1^{j_1 - i_1}} \cdots \sqrt[n]{a_k^{j_k - i_k}}; \]

hence there exists \( b \in K^* \) with

\[ \sqrt[n]{a_{k+1}^{i_{k+1} - j_{k+1}}} = b \cdot \sqrt[n]{a_1^{j_1 - i_1}} \cdots \sqrt[n]{a_k^{j_k - i_k}} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \]

and \( 0 < i_{k+1} - j_{k+1} < d_{k+1} \), in contradiction with the definition of \( d_{k+1} \).

Thus, we must have \( i_{k+1} = j_{k+1} \), and so, by cancelling with \( \sqrt[n]{a_{k+1}^{i_{k+1}}} \) in the above equality one finds

\[ \sqrt[n]{a_1^{i_1}} \cdots \sqrt[n]{a_k^{i_k}} \sqrt[n]{a_{k+1}^{i_{k+1}}} = \sqrt[n]{a_1^{j_1}} \cdots \sqrt[n]{a_k^{j_k}}. \]

By the inductive hypothesis, we get \( i_1 = j_1, \ldots, i_k = j_k \), and consequently the relation (*) follows.

We shall prove now by induction on \( k \) that

\[ \langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle = \{ \sqrt[n]{a_1^{i_1}} \cdots \sqrt[n]{a_k^{i_k}} \mid 0 \leq i_1 < d_1, \ldots, 0 \leq i_k < d_k \}. \quad (***) \]

Clearly, (***') is true for \( k = 1 \). Suppose that (***') is true for \( k \) and prove it for \( k + 1 \). Let \( z \in \langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}} \rangle \). Then \( z = \sqrt[n]{a_1^{j_1}} \cdots \sqrt[n]{a_k^{j_k}} \).
\( \sqrt[1]{a_{k+1}} \) for some \( j_1, \ldots, j_k, j_{k+1} \in \mathbb{N} \). But \( \sqrt[n]{a_{k+1}^{j_{k+1}}} = \sqrt[n]{a_{k+1}^{j_{k+1}}} \) in the group \( \Omega^*/K(\sqrt[1]{a_1}, \ldots, \sqrt[1]{a_k})^* \), where \( 0 \leq i_{k+1} < d_{k+1} \) because\\ord(\sqrt[1]{a_{k+1}}) = d_{k+1}. \) Hence \( \sqrt[n]{a_{k+1}^{j_{k+1}}} = \sqrt[n]{a_{k+1}^{j_{k+1}}} = \sqrt[n]{a_{k+1}^{j_{k+1}}} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}). \) Let \( \sqrt[n]{a_{k+1}^{j_{k+1}}} \) be by definition \( \sqrt[n]{a_{k+1}^{j_{k+1}}} \). According to 4.4 there exist \( p_1, \ldots, p_k \in \mathbb{N} \) and \( c \in K^* \) such that
\[
\sqrt[n]{a_{k+1}^{j_{k+1}}} = \sqrt[n]{a_1^{p_1}} \cdots \sqrt[n]{a_k^{p_k}} \cdot c^n.
\]
It follows that
\[
\sqrt[n]{a_{k+1}^{j_{k+1} - i_{k+1}}} = \sqrt[n]{a_1^{p_1}} \cdots \sqrt[n]{a_k^{p_k}} \cdot c^n,
\]
where \( c' = \pm 1 \) if \( K \) satisfies the condition \( C(n; a_1, \ldots, a_{k+1}) \) and \( c' = \zeta \in K \) with \( \zeta^n = 1 \) in the case \( \mu_n(\Omega) \subseteq K \). So \( c' = \hat{1} \) in both cases, and therefore \( \sqrt[n]{a_{k+1}^{j_{k+1} - i_{k+1}}} = \sqrt[n]{a_1^{p_1}} \cdots \sqrt[n]{a_k^{p_k}} \cdot \sqrt[n]{a_{k+1}^{j_{k+1} - i_{k+1}}} \). Consequently \( z = \sqrt[n]{a_1^{p_1}} \cdots \sqrt[n]{a_k^{p_k}} \cdot \sqrt[n]{a_{k+1}^{j_{k+1} - i_{k+1}}} \). Apply now the inductive hypothesis to obtain
\[
z = \sqrt[n]{a_1^{n_i}} \cdots \sqrt[n]{a_k^{n_i}} \cdot \sqrt[n]{a_{k+1}^{n_i}} \]
for some \( 0 \leq i_1 < d_1, \ldots, 0 \leq i_k < d_k \).

Combining (*) and (**) and taking into account that
\[
[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = d_1 \cdots d_k
\]
we get
\[
[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = \langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle.
\]

The other equality from the statement of the theorem follows from some more general considerations: let
\[
\varphi : \Omega^* \to \Omega^*
\]
\[
\varphi(x) = x^n.
\]

Clearly, \( \varphi \) is a group epimorphism; hence \( \varphi \) induces a group epimorphism
\[
\bar{\varphi} : \Omega^*/K^* \to \Omega^*/K^*
\]
\[
\bar{\varphi}(\hat{x}) = \hat{x}^n.
\]

If \( \mu_n(\Omega) \subseteq K \), then \( \bar{\varphi} \) is also injective because \( \hat{x} \in \ker(\bar{\varphi}) \) entails \( \hat{x}^n = \hat{1} \); hence \( x^n = y^n \) for some \( y \in K^* \). Thus \( x = y\zeta \) with \( \zeta \in \mu_n(\Omega) \subseteq K \), and so \( x \in K^* \), i.e., \( \bar{x} = \hat{1} \).

If \( E \) is now an arbitrary subfield of \( \Omega \) such that \( K \subseteq E \) and \( \mu_n(E) \subseteq K \), then for any subgroup \( G \) of \( E^*/K^* \), \( \bar{\varphi} \) induces an isomorphism \( G \simeq \bar{\varphi}(G) \).
Indeed, if $\hat{x} \in \text{Ker}(\varphi) \cap G$, then $x \in E$ and $\hat{x}^n = \hat{1}$; hence $x^n = y^n$ for some $y \in K^*$. Thus $xy^{-1} \in E$ and $(xy^{-1})^n = 1$, and so $xy^{-1} \in K^*$, i.e., $\hat{x} = \hat{y} = \hat{1}$.

By using these facts, we deduce that the mapping $x \mapsto x^n$ induces an isomorphism of groups $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle \cong \langle \hat{a}_1, \ldots, \hat{a}_k \rangle$. The last assertion from the statement of the theorem now follows immediately. 

Note that neither condition $C(n; a_1, \ldots, a_k)$ nor $\mu_n(\Omega) \subseteq K$ can be left out. To see this, take $K = \mathbb{Q}$ and denote by $\sqrt[4]{-4}$ one of the complex roots $1+i, 1-i, -1+i, -1-i$ of the polynomial $X^4 + 4 \in \mathbb{Q}[X]$. Then $[\mathbb{Q}(:\sqrt[4]{-4} : \mathbb{Q}) = 2$, while $|\sqrt[4]{-4}| = 4$.

5.2. COROLLARY. With the hypotheses and notations of 5.1, the following three assertions are equivalent:

(i) $[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K]$.

(ii) The family $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$ of subgroups of $\Omega^*/K^*$ is independent, i.e., if $i_1, \ldots, i_k \in \mathbb{N}$, then

$$\sqrt[n]{a_1}^{i_1} \cdots \sqrt[n]{a_k}^{i_k} \in K^* \Rightarrow n_1 | i_1, \ldots, n_k | i_k,$$

where $n_j = \text{ord}(\sqrt[n]{a_j}) = \text{ord}(\hat{a}_j)$ for each $j, 1 \leq j \leq k$.

(iii) The family $\langle \hat{a}_1 \rangle, \ldots, \langle \hat{a}_k \rangle$ of subgroups of $K^*/K^{**}$ is independent, i.e., if $i_1, \ldots, i_k \in \mathbb{N}$, then

$$a_1^{i_1} \cdots a_k^{i_k} \in K^{**} \Rightarrow n_1 | i_1, \ldots, n_k | i_k.$$

Proof. (ii) $\iff$ (iii) in view of the isomorphism

$$\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle \rightarrow \langle \hat{a}_1, \ldots, \hat{a}_k \rangle$$

described in the proof of 5.1.

(ii) $\Rightarrow$ (i): Denote $d_1 = [K(\sqrt[n]{a_1}) : K], d_2 = [K(\sqrt[n]{a_1}, \sqrt[n]{a_2}) : K(\sqrt[n]{a_1})], \ldots, d_k = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}})]$. Then $d_1 = n_1$ and $d_j \leq n_j$.

Since (ii) implies that the group $\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$ is the internal direct product $\langle \sqrt[n]{a_1} \rangle \times \cdots \times \langle \sqrt[n]{a_k} \rangle$, it follows that

$$|\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle| = n_1 \cdots n_k.$$

On the other hand, by 5.1 we have

$$|\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle| = d_1 \cdots d_k;$$

hence necessarily $d_j = n_j$ for all $j, 1 \leq j \leq k$, and consequently (ii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): With the same notations, if $[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K]$, then $d_1 \cdots d_k = n_1 \cdots n_k$, hence the group
TOMA ALBU

\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle$, which is isomorphic to a quotient group of the group \langle \sqrt[n]{a_1} \times \cdots \times \sqrt[n]{a_k} \rangle of order \( n_1 \cdot \cdots \cdot n_k \), has the same order as the later one. Therefore they are isomorphic, and so

\langle \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k} \rangle = \langle \sqrt[n]{a_1} \rangle \times \cdots \times \langle \sqrt[n]{a_k} \rangle.

5.3. COROLLARY. Let \( K \) be a subfield of \( \mathbb{R} \), \( n \geq 2 \), \( k \geq 2 \) natural numbers, and \( a_1, \ldots, a_k \in K \) such that \( a_i > 0 \) for all \( i \), \( 1 \leq i \leq k \). Then

\sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} \in K \iff \sqrt[n]{a_i} \in K \quad \text{for all} \quad i, 1 \leq i \leq k,

where \( \sqrt[n]{a_i} \) denotes for each \( i, 1 \leq i \leq k \), the positive real root of the binomial \( X^n - a_i \).

Proof. The nontrivial implication is \( \Rightarrow \). Suppose that \( \sqrt[n]{a_i} \notin K \) for an \( i \), say \( i = 1 \), and \( \sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} \in K \). Then \( \sqrt[n]{a_k} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}}) \). Since \( K \) satisfies the condition \( C(n; a_1, \ldots, a_k) \), by applying 4.4 one gets

\[ \sqrt[n]{a_k} = \sqrt[n]{a_1^{-j_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{-j_{k-1}}} \cdot b \]

for some \( j_1, \ldots, j_{k-1} \in \mathbb{N} \) and \( b \in K, \ b > 0 \). According to the proof of 5.1, there exists \( 0 \leq i_1 < d_1, \ldots, \ 0 \leq i_{k-1} < d_{k-1} \) and \( c \in K, \ c > 0 \), such that

\[ \sqrt[n]{a_1^{-j_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{-j_{k-1}}} \cdot b = \sqrt[n]{a_1^{-i_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{-i_{k-1}}} \cdot c, \]

where \( d_1 = [K(\sqrt[n]{a_1}) : K], \ d_2 = [K(\sqrt[n]{a_1}, \sqrt[n]{a_2}) : K(\sqrt[n]{a_1})], \ldots, d_{k-1} = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}}) : K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-2}})]. \) Moreover, the set

\[ \{ \sqrt[n]{a_1^{m_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{m_{k-1}}} \mid 0 \leq m_1 < d_1, \ldots, 0 \leq m_{k-1} < d_{k-1} \} \]

is a vector space basis of \( K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}}) \) over \( K \).

Hence

\[ \sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} = \sqrt[n]{a_1^{-i_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{-i_{k-1}}} \cdot c = d \in K. \quad (\ast) \]

Clearly \( d_i \geq 2 \) because \( \sqrt[n]{a_1} \notin K \), but it is possible to have \( d_j = 1 \) for some \( j, \ 2 \leq j \leq k-1 \); in this case \( \sqrt[n]{a_j} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{j-1}}) \), and again by 4.4 we may write \( \sqrt[n]{a_j} \) as

\[ \sqrt[n]{a_j} = \sqrt[n]{a_1^{-m_1}} \cdot \cdots \cdot \sqrt[n]{a_{j-1}^{-m_{j-1}}} \cdot c_j \quad (\ast\ast) \]

for some \( c_j \in K, \ c_j > 0, \ 0 \leq m_1 < d_1, \ldots, 0 \leq m_{j-1} < d_{j-1} \). If we replace in \( (\ast) \) each \( \sqrt[n]{a_j}, \ 2 \leq j \leq k-1 \) for which \( d_j = 1 \) by the right side of the equality \( (\ast\ast) \) one gets a sum of the type

\[ \sqrt[n]{a_1} + \cdots + \sqrt[n]{a_1^{m_1}} \cdot \cdots \cdot \sqrt[n]{a_{j-1}^{m_{j-1}}} \cdot c_j + \cdots \]

\[ + \sqrt[n]{a_1^{-i_1}} \cdot \cdots \cdot \sqrt[n]{a_{k-1}^{-i_{k-1}}} \cdot c = d. \quad (\ast\ast\ast) \]
where all the coefficients $c, c_j$ are strictly positive. Note that it is possible to have in (***), two terms

$$
\lambda \sqrt[n]{a_1^{s_1}} \cdots \sqrt[n]{a_{k-1}^{s_{k-1}}} + \mu \sqrt[n]{a_1^{t_1}} \cdots \sqrt[n]{a_{k-1}^{t_{k-1}}}
$$

with $(s_1, \ldots, s_{k-1}) = (t_1, \ldots, t_{k-1})$, $0 \leq s_i = t_i < d_i$, and $\lambda > 0$, $\mu > 0$. Then $\lambda + \mu > 0$; hence these terms cannot be reduced. In this way we have contradicted the fact that

$$\{\sqrt[n]{a_1^{m_1}} \cdots \sqrt[n]{a_{k-1}^{m_{k-1}}} | 0 \leq m_1 < d_1, \ldots, 0 \leq m_{k-1} < d_{k-1}\}$$

is a vector space basis of $K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}})$ over $K$. □

5.4. Corollary. Let $k \in \mathbb{N}$, $k \geq 2$, $n_1, \ldots, n_k$ be natural numbers $\geq 2$, and $a_1, \ldots, a_k$ be strictly positive real numbers. Then

$$\sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} \in \mathbb{Q} \iff \sqrt[n]{a_i} \in \mathbb{Q} \quad \text{for all } i, 1 \leq i \leq k.$$

Proof. If $n$ is the least common multiple of $n_1, \ldots, n_k$ then $n = nf_i f_i$ for some $f_i \in \mathbb{N}$; hence $\sqrt[n]{a_i} = \sqrt[n]{a_i f_i}$ for all $i, 1 \leq i \leq k$. Apply now 5.3. □

5.5. Corollary (Mordell [9]). Let $K$ be an algebraic number field, $k \in \mathbb{N}^*$, $n_1, \ldots, n_k \in \mathbb{N}^*$, $a_1, \ldots, a_k \in K^*$, and $x_1, \ldots, x_k \in \mathbb{C}$ such that $x_i^n = a_i$ for all $i, 1 \leq i \leq k$. Suppose that either

(i) $K \subseteq \mathbb{R}$ and $x_1, \ldots, x_k$ are all real or

(ii) $\mu_{n_1}(C) \cup \cdots \cup \mu_{n_k}(C) \subseteq K$.

Then

$$[K(x_1, \ldots, x_k) : K] = n_1 \cdots n_k$$

provided the following condition is satisfied:

$$m_1, \ldots, m_k \in \mathbb{N} \text{ and } x_1^{m_1} \cdots x_k^{m_k} \in K \Rightarrow m_i \text{ for all } i, 1 \leq i \leq k. \quad (M)$$

Proof. Fix an arbitrary $i, 1 \leq i \leq k$, and take $m_j = n_j$ for all $j, 1 \leq j \leq k, j \neq i$. If $m_i \in \mathbb{N}$ is such that $x_i^{m_i} \in K$, then $x_1^{m_1} \cdots x_i^{m_i - 1} \cdots x_k^{m_k} \in K$; hence the condition (M) entails $n_i \mid m_i$. Therefore $\text{ord}(\hat{x}_i)$ in $C^* / K^*$ is exactly $n_i$. Consequently, the condition (M) is nothing else than the condition that the family $\langle \hat{x}_1 \rangle, \ldots, \langle \hat{x}_k \rangle$ of subgroups of the quotient group $C^* / K^*$ is independent, i.e., $\langle \hat{x}_1 \rangle, \ldots, \langle \hat{x}_k \rangle$ is the internal direct product $\langle \hat{x}_1 \rangle \times \cdots \times \langle \hat{x}_k \rangle$ of the subgroups $\langle \hat{x}_1 \rangle, \ldots, \langle \hat{x}_k \rangle$.

Denote by $n$ the least common multiple of the numbers $n_1, \ldots, n_k$. Then, condition (i) from the statement of the corollary entails that $C$ satisfies the condition $C(n; b_1, \ldots, b_k)$, where $b_i = x_i^n$ for each $i, 1 \leq i \leq k$, while condition
(ii) can be expressed as \( \mu_n(C) \subseteq K \). Apply now 5.2, and remark that, again by 5.2, the converse of the Mordell's result is also true: if \( [K(x_1, \ldots, x_k) : K] = n_1 \cdots n_k \), then condition (M) holds.

A related result is the following.

**Theorem (Ursell [13]).** Let \( k \in \mathbb{N}, k \geq 2, n_1, \ldots, n_k, a_1, \ldots, a_k \in \mathbb{N}^* \), and denote by \( x_i \) the positive real root \( \sqrt[n]{a_i}, \ 1 \leq i \leq k \). Suppose that for each \( i, \ 1 \leq i \leq k \), \( n_i \) is the least strictly positive integer such that \( x_i^{n_i} \in \mathbb{N} \) (i.e., \( \text{ord}(x_i) \) in \( \mathbb{R}^*/\mathbb{Q}^* \) is \( n_i \)). If \( a_1, \ldots, a_k \) are relatively prime in pairs, then

\[
[\mathbb{Q}(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k}) : \mathbb{Q}] = n_1 \cdots n_k.
\]

In order to extend this result to a unique factorization domain we need some preparation. Suppose that the field \( K \) is the field of fractions of a unique factorization domain \( A \) which is not a field. By \( U(A) \) we shall denote the group of units of \( A \). If \( S \) is a nonempty subset of \( A^* = A \setminus \{0\} \), we shall denote in the sequel by \( [S] \) the subsemigroup generated by \( S \) of the multiplicative monoid \( (A, \cdot) \), i.e.,

\[
[S] = \{ s_1 \cdots s_k \mid k \in \mathbb{N}^*, s_i \in S \text{ for all } 1 \leq i \leq k \}.
\]

Denote by \( P(A) \) a representative set of mutually nonassociated in divisibility nonzero prime elements of \( A \).

Let \( a \in [P(A)] \); then \( a = p_1^{a_1} \cdots p_t^{a_t} \), where \( s \in \mathbb{N}^*, \ p_i \in P(A), \ \alpha_i \in \mathbb{N}^* \) for all \( i, \ 1 \leq i \leq s \), and \( p_i \neq p_j \) for \( i \neq j \) in \( \{1, \ldots, s\} \). Suppose that \( K \) satisfies the condition \( C(n; p_1, \ldots, p_s) \), where \( n \in \mathbb{N}, \ n \geq 2 \); then clearly \( K \) also satisfies the condition \( C(n; a) \). Remark that \( x = \sqrt[n]{a} \) is an integral element over \( A \); hence

\[
\text{ord}(x) = \text{Min}\{m \mid m \in \mathbb{N}^*, \ x^m \in K\} = \text{Min}\{m \mid m \in \mathbb{N}^*, \ x^m \in A\}.
\]

Denote by \( d = (\alpha_1, \ldots, \alpha_s, n) \) the greatest common divisor of the numbers \( \alpha_1, \ldots, \alpha_s, n \). We assert that

\[
\text{ord}(\sqrt[n]{a}) = n/d.
\]

Indeed, denote \( \beta_i = \alpha_i/d \) for each \( i, \ 1 \leq i \leq k \). Then

\[
a = (\sqrt[n]{a^{n/d}})^d = p_1^{d\beta_1} \cdots p_t^{d\beta_t} = (p_1^{\beta_1} \cdots p_t^{\beta_t})^d,
\]

hence \( \sqrt[n]{a^{n/d}} = p_1^{\beta_1} \cdots p_t^{\beta_t} \in A \), because \( K \) satisfies the condition \( C(n; a) \) and so \( \mu_d(K(\sqrt[n]{a})) \subseteq \mu_n(K(\sqrt[n]{a})) \subseteq \{1, -1\} \). If \( m \in \mathbb{N}^* \) is such that \( \sqrt[m]{a} \in A \) then \( a^m = b^n \) for some \( b \in A \). Let \( b = u p_1^{\gamma_1} \cdots p_t^{\gamma_t} \), where \( u \in U(A) \) and \( \gamma_1, \ldots, \gamma_s \in \mathbb{N} \). Then

\[
p_1^{\gamma_1 m} \cdots p_t^{\gamma_t m} = u^n \cdot p_1^{\gamma_1} \cdots p_t^{\gamma_t}.
and so \( n | mx_i \) for all \( i, 1 \leq i \leq s \). Thus \( n | (mx_1, ..., mx_s) \), i.e., \( n | m(x_1, ..., x_s) \).

But \( ((x_1, ..., x_s)/d, n/d) = 1 \); hence \( n/d | m \). Consequently \( \text{ord}(\sqrt[n]{a}) = n/d \).

Note that the above equality also follows from 1.2.

5.6. THEOREM. Let \( A \) be a unique factorization domain which is not a field, \( K \) its field of fractions, \( \Omega \) an algebraically closed field containing \( K \) as a subfield, \( k \in \mathbb{N}, k \geq 2, n_1, ..., n_k \in \mathbb{N}^*, a_1, ..., a_k \in [\mathbf{P}(A)] \cup \mathbf{U}(A) \), and \( x_1, ..., x_k \in \Omega \) such that \( x_i^{n_i} = a_i \) and \( \text{ord}(x_i) = n_i \) in \( \Omega^*/K^* \) for all \( i, 1 \leq i \leq k \).

Suppose that \( (n, e(K)) = 1 \), where \( n \) is the least common multiple of \( n_1, ..., n_k \), and either

(i) \( \mu_n(K(x_1, ..., x_k)) \subseteq \{1, -1\} \) or

(ii) \( \mu_n(\Omega) \subseteq K \).

Then \( [K(x_1, ..., x_k) : K] = n_1 \cdots n_k \) provided the following condition is satisfied:

The elements \( a_1, ..., a_k \) are relatively prime in pairs. (U)

Proof. Using 1.1, the proof can be achieved by following the proof from Ursell [13].

Another way to prove the above theorem is to show that the condition (U) implies the condition (M). More precisely, we have the following.

5.7. PROPOSITION. Let \( A \) be a unique factorization domain and \( K \) its field of fractions. With the notations of 5.6, suppose that the field \( K \) satisfies either condition (i) or (ii). Then condition (U) from 5.6 implies condition (M) from 5.5.

Proof. Since \( n \) is the least common multiple of \( n_1, ..., n_k \), for each \( i, 1 \leq i \leq k \), there exists \( f_i \in \mathbb{N} \) such that \( n = n_i f_i \). Let \( m_1, ..., m_k \in \mathbb{N} \) such that \( x_i^{n_i} \cdots x_k^{n_k} \in K \). Since \( x_i, 1 \leq i \leq k \), are integral elements over \( A \) and \( A \) is integrally closed, it follows that \( x_i^{m_i} \cdots x_k^{m_k} \in A \). But \( x_i^{n_i} = a_i \); hence \( x_i^{m_i} = a_i^{f_i} \), and so

\[
x_i^{m_i} \cdots x_k^{m_k} = a_1^{m_1 f_1} \cdots a_k^{m_k f_k} = a^n
\]

for some \( a \in A \setminus U(A) \).

But \( a = u \cdot p_1^{e_1} \cdots p_r^{e_r} \), where \( u \in U(A), p_1, ..., p_r \) are distinct elements of \( \mathbf{P}(A) \), and \( \alpha_i \in \mathbb{N}^*, 1 \leq i \leq r \). Since \( a_i \in [\mathbf{P}(A)] \cup \mathbf{U}(A) \), we have \( a_i = q_1^{f_1} \cdots q_s^{f_s} \), where \( q_1, ..., q_s \) are distinct elements of \( \mathbf{P}(A) \) and \( \beta_1, ..., \beta_s \in \mathbb{N}^* \). But \( a_1, ..., a_k \) are relatively prime in pairs; hence \( \{q_1, ..., q_s\} \subseteq \{p_1, ..., p_r\} \) and \( n \mid m_i f_i \beta_j \) for all \( j, 1 \leq j \leq s \), and so \( n_1 \mid m_i \beta_j \) for all \( j, 1 \leq j \leq s \). Thus \( a_i^{m_i} \in A^{n_i} \). But \( n_1 = \text{ord}(x_i) = \text{Min}\{m \mid m \in \mathbb{N}^* \} \).
\[ x_m^t \in A \} = \text{Min} \{ m | m \in \mathbb{N}^*, \ a_n^m \in A^n \}, \text{ and consequently } n_1 | m_1. \text{ In a similar manner one shows that } n_j | m_j \text{ for all } j, 2 \leq j \leq k, \text{ and the proof is complete.} \]

5.8. Remark. Condition (M) from 5.5 does not imply condition (U) from 5.6, as the following simple example shows:

\[ Q \subseteq Q(\sqrt{2}, \sqrt{6}). \]

Indeed, we have \([Q(\sqrt{2}, \sqrt{6}) : Q]\) = 4, and if \(m_1, m_2 \in \mathbb{N}\) are such that \(\sqrt{2}^{m_1} \cdot \sqrt{6}^{m_2} \in Q\), then \(m_2\) and consequently \(m_1\) must be even; however, \((2, 6) \neq 1\).

5.9. Theorem. Let \(n \in \mathbb{N}\), \(n \geq 2, k \in \mathbb{N}^*, K\) a field with \((n, e(K)) = 1, \text{ and } a_1, ..., a_k \in K^*. \text{ Suppose that either } K \text{ satisfies the condition } C(n; a_1, ..., a_k) \text{ or } K_n(\Omega) \subseteq K. \text{ If } [K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K], \text{ then}

\[ K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) = K(\sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k}). \]

Proof. For each \(i, 1 \leq i \leq k\), denote \(n_i = [K(\sqrt[n]{a_i}) : K]\) and let \(X^n - b_i = \text{Irr}(\sqrt[n]{a_i}, K); \text{ then } \sqrt[n]{a_i} = \sqrt[n]{b_i}. \text{ We proceed by induction on } k. \)

If \(k = 1\) we have nothing to prove. Suppose that the theorem is true for \(k\) and prove it for \(k + 1\). Clearly we can assume that \(n_j > 1\) for all \(j, 1 \leq j \leq k + 1\). Let \(\omega\) be a primitive \(n\)th root of unity and denote

\[ F = K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_{k+1}}, \omega) \]

\[ x = \sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} \]

\[ \beta = \sqrt[n]{a_{k+1}}. \]

Since \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] \leq \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K]\) and \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) : K] = \prod_{1 \leq i \leq k+1} [K(\sqrt[n]{a_i}) : K]\), it follows that \([K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K]\).

By the inductive hypothesis, \(K(\sqrt[n]{a_1}, ..., \sqrt[n]{a_k}) = K(\alpha)\); hence \(\alpha\) has exactly \(n_1 \cdot \cdots \cdot n_k\) conjugates \(\alpha_1, \alpha_2, ..., \alpha_{n_1} \cdot \cdots \cdot n_k\) over \(K\) contained in \(F\). On the other hand, \(\beta\) has exactly \(n_{k+1}\) conjugates \(\beta_1, \beta_2, ..., \beta_{n_{k+1}}\) over \(K\) contained in \(F\).

Consider an arbitrary \(i, 1 \leq i \leq n_1 \cdot \cdots \cdot n_k\), and an arbitrary \(j, 1 \leq j \leq n_{k+1}\). Then, there exists \(\varphi \in \text{Gal}(F/K)\) such that \(\varphi(\alpha_i) = \alpha; \text{ since } \varphi(\beta_j) \text{ is a conjugate of } \beta \text{ over } K, \text{ there exists } s, 1 \leq s \leq n_{k+1}, \text{ such that } \varphi(\beta_j) = \beta_s. \text{ But } [K(\alpha, \beta) : K(\alpha)] = n_{k+1}; \text{ hence the degree of } \text{Irr}(\beta, K(\alpha)) \text{ is } n_{k+1}; \text{ in other words, } \beta_1, ..., \beta_{n_{k+1}}, \text{ are all the conjugates of } \beta \text{ over } K(\alpha). \text{ It follows that there exists } \psi \in \text{Gal}(F/K(\alpha)) \text{ such that } \psi(\beta_j) = \beta. \text{ Denote } \chi = \psi \circ \varphi. \text{ Then } \chi \in \text{Gal}(F/K) \text{ and } \chi(\alpha_i) = \alpha, \chi(\beta_j) = \beta. \text{ Consequently, all the} \]
elements $\alpha_i + \beta_j$, $1 \leq i \leq n_1 \cdot \ldots \cdot n_k$, $1 \leq j \leq n_{k+1}$, are the conjugates of $\alpha + \beta$ over $K$. If all these elements are distinct, we can conclude that $[K(\alpha + \beta) : K] = n_1 \cdot \ldots \cdot n_{k+1}$; hence

$$K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) = K(\alpha, \beta) = K(\alpha + \beta) = K(\sqrt[n]{a_1 + \ldots + \sqrt[n]{a_k + \sqrt[n]{a_{k+1}}}}),$$

and we are done.

So, it is sufficient to show that no difference of two conjugates of $\alpha$ equals a difference of two conjugates of $\beta$. Let

$$\alpha = \varepsilon_1 \sqrt[n]{a_1} + \ldots + \varepsilon_k \sqrt[n]{a_k}, \quad \beta = \varepsilon'_1 \sqrt[n]{a_{k+1}}, \quad \alpha_p = \varepsilon'_1 \sqrt[n]{a_1} + \ldots + \varepsilon'_k \sqrt[n]{a_k},$$

be two conjugates of $\alpha$ over $K$, and

$$\beta_j = e \sqrt[n]{a_{k+1}}, \quad \beta_q = e' \sqrt[n]{a_{k+1}}$$

be two conjugates of $\beta$ over $K$, such that

$$\alpha_i - \alpha_p = \beta_q - \beta_j,$$

where $\varepsilon, \varepsilon', e, e' \in \mu_n(\Omega)$.

Suppose that $\beta_q \neq \beta_j$, i.e., $e \neq e'$; then

$$\sqrt[n]{a_{k+1}} = \left[1/(e' - e)\right] \left[(\varepsilon_1 - \varepsilon'_1) \sqrt[n]{a_1} + \ldots + (\varepsilon_k - \varepsilon'_k) \sqrt[n]{a_k}\right],$$

and so, $\sqrt[n]{a_{k+1}} \in K(\omega, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$. To finish the proof, we shall show that this leads to a contradiction. Two cases arise as follows.

**Case 1.** $n$ is odd. Then, according to 3.2, one has

$$[K(\omega, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) : K(\omega)] = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) : K] = n_1 \cdot \ldots \cdot n_k \cdot n_{k+1}.$$ 

On the other hand, $K(\omega, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$; hence

$$[K(\omega, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) : K(\omega)] = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = n_1 \cdot \ldots \cdot n_k.$$
We deduce that \( n_1 \cdot \cdots \cdot n_k \cdot n_{k+1} = n_1 \cdot \cdots \cdot n_k \), and so, \( n_{k+1} = 1 \), contrary to our assumption.

*Case 2.* \( n \) is even. First of all, note that if \( n = 2 \) then \( \omega = 1 \); hence the same arguments as above, but without making appeal to 3.2, yield the desired contradiction.

If all \( n_i, 1 \leq i \leq k + 1 \), are odd, then we proceed as above, but applying 3.3(iii) instead of 3.2. We can therefore assume, by renumbering the \( a_i's \) that \( n_1, \ldots, n_r \) are all even numbers, \( r \geq 1 \), and \( n_{r+1}, \ldots, n_{k+1} \) are all odd.

We consider first the case when \( r = k + 1 \). Then \( n_i = 2m_i \) for all \( i, 1 \leq i \leq k + 1 \). If we denote \( x_i = \sqrt[n]{a_i} \), then \( x_i^{2m_i} = \sqrt[n]{b_i} \). Recall that \( \text{Irr}(\sqrt[n]{a_i}, K) = X^{n_i} - b_i \) and \( \sqrt[n]{b_i} = \sqrt[n]{a_i} \).

Let \( j_1, \ldots, j_{k+1} \in \mathbb{N} \) such that \( \sqrt[n]{b_1} \cdot \cdots \cdot \sqrt[n]{b_{k+1}} \in K^* \). Then \( x_i^{j_1m_i} \cdot \cdots \cdot x_{k+1}^{j_{k+1}m_{k+1}} \in K^* \); hence \( n_1 | j_1m_1, \ldots, n_{k+1} | j_{k+1}m_{k+1} \) by 5.2, and so \( 2 | j_1, \ldots, 2 | j_{k+1} \). Applying 5.2 again, we find

\[
[K(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_{k+1}}) : K] = 2^{k+1},
\]

and consequently \( K(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_{k+1}}) = K(\sqrt[n]{b_1} + \cdots + \sqrt[n]{b_{k+1}}) \), as we have just seen above.

We prove now that

\[
K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) = K(\sqrt[n]{a_1} + \cdots + \sqrt[n]{a_k} + \sqrt[n]{a_{k+1}})
\]

in the case \( n_i = 2m_i \) for all \( i, 1 \leq i \leq k + 1 \).

If we denote \( L = K(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_k}, \sqrt[n]{b_{k+1}}) \), then, by Lemma 5.10 which will be proved below, we have

\[
[L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}) : L] = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}) : K(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_{k+1}})] = n_1 \cdot \cdots \cdot n_k \cdot n_{k+1} / 2^{k+1}.
\]

But \( \sqrt[n]{a_{k+1}} \in K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \); hence \( L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \sqrt[n]{a_{k+1}}) = L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \). On the other hand, by the same lemma, we have

\[
[L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L] = [K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_k})] = n_1 \cdot \cdots \cdot n_k / 2^k.
\]

It follows that \( n_1 \cdot \cdots \cdot n_k \cdot n_{k+1} / 2^{k+1} = n_1 \cdot \cdots \cdot n_k / 2^k \), and so \( n_{k+1} = 2 \). But we can suppose that at least one of the even numbers \( n_1, \ldots, n_k, n_{k+1} \), say \( n_r \), is \( > 2 \), for otherwise, if \( n_1 = \cdots = n_k = n_{k+1} = 2 \), then
Kummer Extensions

355

\( K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}) = K(\sqrt[n]{a_1} + \cdots + \sqrt[n]{a_{k+1}}) \) as we have already seen. By a convenient renumbering we can suppose that this \( n_j \) is exactly \( n_{k+1} \). We thus got a contradiction.

We consider now the following case:

- \( n_1, \ldots, n_r \) are all even numbers, and \( r \geq 1 \)
- \( n_{r+1}, \ldots, n_{k+1} \) are all odd numbers, and \( r + 1 \leq k + 1 \).

According to 3.3(iii), by taking instead of \( K \) the field \( K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k+1}}) \), which satisfies clearly the condition \( C(n; a_1, \ldots, a_{k+1}) \), one has

\[
\begin{align*}
&[K(\omega, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}}) : K(\omega, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}})] \\
&= [K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}}) : K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}})] \\
&= [K(\omega, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}}) : K(\omega, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}})] \\
&= [K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}}) : K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k+1}]{a_{k+1}})].
\end{align*}
\]

Consequently \( n_1, \ldots, n_{k+1} = n_{r+1}, \ldots, n_k \), which implies \( n_{k+1} = 1 \), a contradiction, since we have assumed that all the \( n_i \)'s are \( > 1 \).

And now we shall state and prove the lemma used in the proof of the above theorem.

5.10. Lemma. Let \( n \geq 4 \) be an even number, \( k \in \mathbb{N} \), \( k \geq 2 \), and \( a_1, \ldots, a_k \in K^* \). Suppose that \( K \) satisfies the condition \( C(n; a_1, \ldots, a_k) \), \( [K(\sqrt[n]{a_i}) : K] = 2m_i \), \( m_i \in \mathbb{N} \) for each \( i, 1 \leq i \leq k \), and

\[
[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt[n]{a_i}) : K].
\]

Then, for any abelian extension \( L \) of \( K \) with \( \mu_n(\Omega) \subseteq L \subseteq \Omega \) or \( L \subseteq K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) \), one has

\[
[K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : K(\sqrt[n]{a_1^s_1}, \ldots, \sqrt[n]{a_k^s_k})] = [L(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) : L(\sqrt[n]{a_1^s_1}, \ldots, \sqrt[n]{a_k^s_k})].
\]

where \( s_1, \ldots, s_k \in \mathbb{N} \) are such that \( s_i | n \) and \( [K(\sqrt[n]{a_i^s_i}) : K] = 2 \) for all \( i, 1 \leq i \leq k \).

Proof. By 1.1, \( \text{Irr}(\sqrt[n]{a_i}, K) = X^n - b_i \); hence \( n_i = 2m_i \), \( \sqrt[n]{b_i} = \sqrt[n]{a_i} \), and \( \sqrt[b_i]{m_i} \in K(\sqrt[n]{a_i}) \) for each \( i, 1 \leq i \leq k \).

We proceed by induction on \( k \). If \( k = 1 \) we obtain exactly 4.1. Suppose that the lemma is true for \( k - 1 \) and prove it for \( k \geq 2 \). Denote \( K' = K(\sqrt[k]{b_k}) \), \( F = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_{k-1}}) \), and consider the following diagram:
As we have already seen in the proof of the above theorem, 
\([K(\sqrt{b_1}, \ldots, \sqrt{b_k}) : K] = 2^k\); hence 
\([K(\sqrt{b_1}, \ldots, \sqrt{b_k}) : K(\sqrt{b_1}, \ldots, \sqrt{b_{k-1}})] = 2\). By the inductive hypothesis, taking as \(L\) the abelian extension \(K(\sqrt{b_k})\) of \(K\), one deduces

\[ [F(\sqrt{b_k}) : K'(\sqrt{b_1}, \ldots, \sqrt{b_{k-1}})] = [F : K(\sqrt{b_1}, \ldots, \sqrt{b_{k-1}})]; \]

hence, from the commutative diagram (1) one gets \([F(\sqrt{b_k}) : F] = 2\). On the other hand, \([K'(\sqrt{b_i}) : K'] = 2\) for all \(i, 1 \leq i \leq k - 1\); hence, again by the inductive hypothesis applied to the field \(K'(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}})\) and to the abelian extension \(K' \subseteq L(\sqrt{b_k})\), one finds

\[ [L(\sqrt{b_k})(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}}) : L(\sqrt{b_1}, \ldots, \sqrt{b_{k-1}})] = [K'(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}}) : K'(\sqrt{b_1}, \ldots, \sqrt{b_{k-1}})]. \]  

Consider now the diagram

\[ L(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}})(\sqrt{b_k}) \quad - \quad L(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}}, \sqrt{a_k}) \]

\[ F(\sqrt{b_k}) \quad - \quad F(\sqrt{a_k}) \]

Since \([F(\sqrt{b_k}) : F] = 2\), we can apply 4.1 to the abelian extension \(F \subseteq L(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}})\) to deduce

\[ [F(\sqrt{a_k}) : F(\sqrt{b_k})] = [L(\sqrt{a_1}, \ldots, \sqrt{a_k}) : L(\sqrt{a_1}, \ldots, \sqrt{a_{k-1}}, \sqrt{b_k})] \]  

(\text{**})

From (\text{*}) and (\text{**}) we conclude

\[ [K(\sqrt{a_1}, \ldots, \sqrt{a_k}) : K(\sqrt{b_1}, \ldots, \sqrt{b_k})] = [L(\sqrt{a_1}, \ldots, \sqrt{a_k}) : L(\sqrt{b_1}, \ldots, \sqrt{b_k})], \]

and the proof is complete.

\[ \text{5.11. Problem. Does 5.9 hold without the condition} \]

\[ [K(\sqrt{a_1}, \ldots, \sqrt{a_k}) : K] = \prod_{1 \leq i \leq k} [K(\sqrt{a_i}) : K]? \]
5.12. **Remark.** The condition \((n, e(K)) = 1\) is essential for the validity of 5.9. Indeed, let \(K = F_p(X^p, Y^p)\), where \(p\) is a prime number and \(X, Y\) are two algebraically independent indeterminates. Denoting \(a = X^p, b = Y^p, \sqrt[p]{a} = X, \sqrt[p]{b} = Y\), then \(K\) satisfies the condition \(C(p; a, b)\) (see 3.1(ii)) and \([K(\sqrt[p]{a}, \sqrt[p]{b}) : K] = p^2\), but \(K(\sqrt[p]{a}, \sqrt[p]{b}) \neq K(\sqrt[p]{a + \sqrt[p]{b}})\) because \((\sqrt[p]{a + \sqrt[p]{b}})^p = a + b \in K\).

5.13. **COROLLARY.** Let \(K\) be an arbitrary field and \(p > 0\) a prime number, other than the characteristic of \(K\). Let \(k \in \mathbb{N}^*, a_1, ..., a_k \in K^*\), and let \(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k}\) denote fixed \(p\)th roots. Then

\[
[K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k}) : K] = |\left< \sqrt[p]{a_1}, ..., \sqrt[p]{a_k} \right>| = |\left< a_1, ..., a_k \right>|
\]

where \(\left< \sqrt[p]{a_1}, ..., \sqrt[p]{a_k} \right>\) (resp., \(\left< a_1, ..., a_k \right>\)) is the subgroup of \(K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k})^*/K^*\) (resp., \(K^*/K^p\)) generated by the cosets \(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k}\) in the quotient group \(K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k})^*/K^*\) (resp., by the cosets \(a_1, ..., a_k\) in the quotient group \(K^*/K^p\)).

Moreover, if \(a_i \notin K^p\) for all \(i\), \(1 \leq i \leq k\), then

\[
[K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k}) : K] = p^k
\]

if and only if the following condition is satisfied:

\[
i_1, ..., i_k \in \mathbb{N} \quad \text{and} \quad a_1^{i_1} \cdot \cdots \cdot a_k^{i_k} \in K^p \Rightarrow p \mid i_s \quad \text{for all} \quad s, 1 \leq s \leq k.
\]

In this case \(K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k}) = K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_k})\).

**Proof.** According to 3.1(ii) \(K\) satisfies either the condition \(C(p; a_1, ..., a_k)\) or \(\mu_p(\Omega) \subseteq K\). Apply now 5.1, 5.2, and 5.9.

We end this paper by showing how 5.1 can be used for the computation of the degrees of the extensions of the type

\[Q \subseteq Q(a_1^{i_1}, ..., a_k^{i_k}),\]

where \(k, n_1, ..., n_k \in \mathbb{N}^*\) and \(a_1, ..., a_k\) are strictly positive rational numbers.

For example, we want to find \([Q(\sqrt[12]{12}, \sqrt[108]{108}) : Q]\). We have \(\sqrt[12]{12} = \sqrt[12]{2^{5}3^3}\) and \(\sqrt[108]{108} = \sqrt[12]{2^{4}3^6}\). By 5.1, \([Q(\sqrt[12]{12}, \sqrt[108]{108}) : Q]\) is exactly the order of the subgroup of \(Q^*/Q^*12\) generated by the cosets \(\sqrt[12]{2^{5}3^3}\) and \(\sqrt[12]{2^{4}3^6}\).

We have

\[
\left< \sqrt[12]{2^{4}3^6}, \sqrt[12]{2^{5}3^3} \right> = \left< \sqrt[12]{2^{4}3^6}, \sqrt[12]{2^{5}3^3}, \sqrt[12]{2^{4}3^6}, \sqrt[12]{2^{5}3^3}, \sqrt[12]{2^{4}3^6}, \sqrt[12]{2^{5}3^3}, \sqrt[12]{2^{4}3^6}, \sqrt[12]{2^{5}3^3} \right>.
\]
and $|\langle 2^{\sqrt{3}}, 2^{\sqrt{3}} \rangle| = 12$. Consequently, $[\mathbb{Q}(\sqrt[4]{12}, \sqrt[4]{108}) : \mathbb{Q}] = 12$, and
\[
\{1, 2^{\sqrt{3}}, 2^{\sqrt{3}^2}, 2^{\sqrt{3}^3}, 2^{\sqrt{3}^4}, 2^{\sqrt{3}^5}, 2^{\sqrt{3}^6}, 2^{\sqrt{3}^7}, 2^{\sqrt{3}^8}, 2^{\sqrt{3}^9}, 2^{\sqrt{3}^{10}}, 2^{\sqrt{3}^{11}}, 2^{\sqrt{3}^{12}} \}
\]
is a vector space basis of the considered extension.

In a similar way one finds $[\mathbb{Q}(\sqrt[4]{12}, \sqrt[4]{3}) : \mathbb{Q}] = 8$ and $[\mathbb{Q}(\sqrt[6]{18}, \sqrt[6]{162}) : \mathbb{Q}] = 18$.

Note added in proof: After this paper was finished we found that the book by G. Karpilovsky, "Field Theory," Dekker, New York, 1988, contains additional references and results on the subject under consideration.

REFERENCES