ON INTEGRAL BASIS OF PURE NUMBER FIELDS

ANUJ JAKHAR, SUDESH K. KHANDUJA AND NEERAJ SANGWAN

Abstract. Let $K = \mathbb{Q}(\sqrt[n]{a})$ be an extension of degree $n$ of the field $\mathbb{Q}$ of rational numbers, where the integer $a$ is such that for each prime $p$ dividing $n$ either $p \nmid a$ or the exponent of $p$ in $a$ is coprime to $p$; this condition is clearly satisfied when $a, n$ are coprime or $a$ is squarefree. The present paper gives explicit construction of an integral basis of $K$ along with applications. This construction of an integral basis of $K$ extends a result proved in [Gaál and Remete, J. Number Theory 173 (2017), 129–146] regarding periodicity of integral bases of $\mathbb{Q}(\sqrt[n]{a})$ when $a$ is squarefree.

§1. Introduction and statement of results. Discriminant is a valuable tool to find a $\mathbb{Z}$-basis for the ring $A_K$ of algebraic integers in an algebraic number field $K$. To describe a $\mathbb{Z}$-basis of $A_K$ (called an integral basis of $K$) is in general a difficult task in an infinite parametric family of algebraic number fields. The problem of computation of integral basis especially for pure algebraic number fields has attracted the attention of several mathematicians. In 1900, Dedekind [1] described an integral basis of pure cubic fields. Westlund [9] in 1910 gave an integral basis for all fields of the type $\mathbb{Q}(\sqrt[n]{a})$ having prime degree $p$ over $\mathbb{Q}$. In 1984, Funakura [2] determined an integral basis of all pure quartic fields. In 2015, Hameed and Nakahara [5] provided an integral basis of those pure octic fields $\mathbb{Q}(\sqrt[n]{a})$, where $a$ is a squarefree integer. In 2017, Gaál and Remete [3] gave a construction of integral basis of $K = \mathbb{Q}(\sqrt[n]{a})$ where the integer $a$ is squarefree and $3 \leq n \leq 9$; they further proved that if $a, a'$ are squarefree integers which are congruent modulo $n_0^\epsilon$, $n_0$ being the largest square dividing $n$ and if $\theta, \theta'$ are roots of the irreducible polynomials $x^n - a, x^n - a'$, respectively, then an element $\frac{1}{q} (c_0 + c_1 \theta + \cdots + c_{n-1} \theta^{n-1})$ with $c_i, q \in \mathbb{Z}$, is an algebraic integer if and only if so is $\frac{1}{q} (c_0 + c_1 \theta' + \cdots + c_{n-1} \theta'^{n-1})$. This result they expressed by saying that the integral bases of the fields $\mathbb{Q}(\sqrt[n]{a})$ are periodic in $a$ with period $n_0^\epsilon$ when $a$ is squarefree.

In the present paper, our aim is to give an explicit construction of an integral basis of pure fields of the type $K = \mathbb{Q}(\sqrt[n]{a})$ where for each prime $p$ dividing $n$, either $p$ does not divide $a$ or the exponent of $p$ in $a$ (to be denoted by $v_p(a)$) is coprime to $p$; this condition is satisfied when either $\gcd(a, n) = 1$ or $a$ is squarefree. Moreover, we shall quickly deduce from our construction that the integral bases of the fields $\mathbb{Q}(\sqrt[n]{a})$, $a$ being squarefree, are periodic in $a$ with period $np_1 \cdots p_k$, where $p_1, \ldots, p_k$ are the distinct primes dividing $n$. We shall use the following theorem proved in [4, 6].

Theorem 1. A. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with discriminant $d_K$, where $\theta$ is a root of an irreducible polynomial $f(x) = x^n - a$ belonging to $\mathbb{Z}[x]$. Let $\prod_{i=1}^{l} p_i^{\epsilon_i}, \prod_{j=1}^{l'} q_j^{\epsilon_j}$ be the prime factorizations of $n, |a|$, respectively. Let $m_j = \gcd(n, t_j), n_i = \frac{n}{p_i^{\epsilon_i}}$ and
\[ r_i = v_p(a^{p^i} - 1) - 1. \] Assume that \( a \) is \( n \)th power free and for each \( i \), either \( v_p(a) = 0 \) or \( v_p(a) \) is coprime to \( p_i \). Then

\[ d_K = (-1)^{(n-1)(n-2)} \frac{\text{sgn}(a^{n-1})}{\left( \prod_{i=1}^{k} p_i^{v_i} \right) \prod_{j=1}^{l} a_j^{n-m_j}}, \]

where \( v_i \) equals \( n s_i - 2n_i \sum_{j=1}^{\min(\{r_i, s_i\})} p_i^{s_i-j} \) or \( ns_i \) according to \( r_i > 0 \) or not.

The basic idea of our construction of integral basis \( \mathbb{Q}(\sqrt[n]{a}) \) has been derived from two lemmas which are stated below and will be proved in the next section. These lemmas lead to a method to construct certain algebraic integers in \( K \) which play a significant role in the formation of integral basis of \( K \). The proofs of all our results in the paper are based on elementary algebraic number theory and are self contained. In what follows, \( \theta \) is a root of an irreducible polynomial \( x^n - a \in \mathbb{Z}[x] \), where \( |a| \) is \( n \)th power free which is expressed as \( \prod_{j=1}^{n-1} a_j \) where \( a_1, a_2, \ldots, a_{n-1} \) are squarefree numbers which are relatively prime in pairs. For a real number \( \lambda \), \( [\lambda] \) will stand for the greatest integer not exceeding \( \lambda \). For \( 0 \leq m \leq n-1 \), \( C_m \) will stand for the number \( \prod_{j=1}^{n-1} a_j^{\lfloor \frac{m}{n} \rfloor} \). Keeping in mind that \( \theta^n = a \), it can be easily seen that the element \( \frac{\theta^n}{C_m} \) satisfies the polynomial \( x^n - \text{sgn}(a)^m \prod_{j=1}^{n-1} a_j^{jm-n \lfloor \frac{m}{n} \rfloor} \) and hence is an algebraic integer.

With above notation, we shall prove the following two lemmas in the next section.

**Lemma 1.1.** Let \( K = \mathbb{Q}(\theta) \) with \( \theta \) be a root of an irreducible polynomial \( x^n - a \) belonging to \( \mathbb{Z}[x] \). Let \( p \) be a prime factor of \( n \), \( s = v_p(n) \) and \( r = v_p(a^{p^s} - 1) - 1 \). Assume that \( r \) is positive. Corresponding to a number \( k \), \( 1 \leq k \leq \min(r, s) \), let \( b' \) be an integer satisfying \( ab' \equiv 1 \pmod{p^{k+1}} \) and \( a' \) be given by \( (b')^{p^{-k-1}} \) or \( b' \) according to \( k < s \) or not. Let \( n' = \frac{n}{p} \).

If \( \eta_k \) is the element \( \sum_{j=0}^{p^s-1} (a' \theta^n)^j \) of \( K \), then \( \frac{\eta_k}{p} \) is an algebraic integer.

**Lemma 1.2.** Let \( x^n - a, p, s \) and \( r \) be as in Lemma 1.1. For any given integer \( m \), \( 0 \leq m \leq n-1 \), let \( k_m \) be the largest non-negative integer not exceeding \( \min(r, s) \) such that \( m = n - \frac{n}{p^{k_m}} + j_m \) with \( j_m > 0 \). Let \( b'_m \) be an integer satisfying \( ab'_m \equiv 1 \pmod{p^{k_m+1}} \) and \( a'_m \) be given by \( (b'_m)^{p^{-k_m}-1} \) or \( b'_m \) according to \( k_m < s \) or not. Let \( n'_m = \frac{n}{p^{k_m}} \) and \( w_m \) be an integer such that \( w_m C_m (a'_m)^{p^{k_m}n-1} \equiv 1 \pmod{p^{k_m}} \). Let \( \delta_m \) stand for the element \( w_m C_m \theta^{j_m} \sum_{j=0}^{p^{k_m}-2} (a'_m \theta^{n'_m})^j \).

If \( \delta_m \) of \( \mathbb{Z}[\theta] \) according to \( k_m > 0 \) or \( k_m = 0 \), then \( \frac{\delta_m + \delta_m}{p^{k_m} C_m} \) is an algebraic integer.

For reader’s convenience, we first describe an explicit integral basis of \( K \) (with \( K \) as in Theorem 1) when its degree is power of a prime.

**Theorem 1.3.** Let \( K = \mathbb{Q}(\theta) \) with \( \theta \) a root of an irreducible polynomial \( x^{p^s} - a \) belonging to \( \mathbb{Z}[x] \) of degree power of a prime \( p \), where \( |a| \) is \( p^s \)-th power free which is expressed as \( \prod_{j=1}^{p^s-1} a_j \) functions \( a_j \) being squarefree numbers relatively prime in pairs. Assume \( p \nmid \gcd(a, v_p(a)) \). Let \( r = v_p(a^{p^s} - 1) - 1 \) and \( d = \min(r, s) \). For \( 0 \leq m < p^s \), let \( k_m \) stand for the largest non-negative integer not exceeding \( d \) such that \( m \geq p^s - p^{s-k_m} \) and \( j_m \) be given by \( m = p^s - p^{s-k_m} + j_m \). Let \( C_m = \prod_{j=1}^{p^s-1} a_j^{\lfloor \frac{m}{p^{s-k_m}} \rfloor} \). When \( m \geq \phi(p^s)^2 \), fix any integer

---

2 Note that \( m \geq \phi(p^s)^2 \) if and only if \( k_m \geq 1 \).
a'_m congruent to a^{(p-2)(p^r-k_m-1)} or a^{p-2} modulo p^{k_m+1} according to k_m < s or k_m = s. Let w_m belong to \mathbb{Z} be such that w_mC_m(a'_m)^{p^r-1} \equiv 1 (mod p^{k_m}) and \delta_m denote the element w_mC_m \sum_{i=0}^r p^{r-i}(a'_m \theta^{p^r-i}) when m \geq \phi(p^r). Then the following hold.

(i) If r = 0 or -1, then \{\theta/ C_0, \theta^2/ C_1, \ldots, \theta^{p^r-1}/ C_{p^r-1}\} is an integral basis of K.

(ii) If r \geq 1, then \{\theta/ C_0, \theta^2/ C_1, \ldots, \theta^{p^r-1}/ C_{p^r-1}\} \cup \{\theta^{n+k}/ C_{p^m} \mid \phi(p^s) \leq m \leq p^s - 1\} is an integral basis of K.

Theorem 1.3 will be deduced as a corollary to our main theorem which will be stated after giving some examples illustrating Theorem 1.3.

Example 1.4. Let K = \mathbb{Q}(\theta), where \theta is a root of x^8 - 17 \cdot 7^2 and \mathbb{A}_K be the ring of algebraic integers of K. We retain the notations of Theorem 1.3. Here a = 17 \cdot 7^2, p = 2, s = 3, r \geq 5 as a \equiv 1 (mod 2^6). One can verify that C_m = 1 or 7 according to 0 \leq m \leq 3 or 4 \leq m \leq 7. It can be easily checked that k_0 = k_1 = k_2 = k_3 = 0, k_4 = k_5 = 1, k_6 = 2, k_7 = 3. j_4 = 0, j_5 = 1, j_6 = 0 and j_7 = 0. Keeping in mind a \equiv 1 (mod 2^6), we see that a'_m = 1 works for 0 \leq m \leq 7. Accordingly one can choose w_4 = w_5 = 1, w_6 = 3 and w_7 = 7. Therefore with \delta_m as defined in Theorem 1.3, we have \delta_4 = 7, \delta_5 = 7\theta, \delta_6 = 21(\theta^4 + \theta^2 + 1) and \delta_7 = 49(\sum_{j=0}^6 \theta^j). Substituting for C_m, k_m and \delta_m in the integral basis described in Theorem 1.3, we see that the set \{1, \theta, \theta^2, \theta^3, \theta^{4+7n/14}, \theta^{57+7n/14}, \theta^{6+21(\theta^4+\theta^2+1)/28}, \theta^{7+49(\sum_{j=0}^6 \theta^j)/56}\} is an integral basis of K.

Example 1.5. Let K = \mathbb{Q}(\theta) with \theta a root of x^9 - 26. With notations as in Theorem 1.3, here \theta = a_1 and hence C_m = a_1^{\frac{p_m}{p^r}} = 1 for each m \leq 8. It can be easily checked that k_0 = 0 for 0 \leq m \leq 5, k_6 = k_7 = 1, k_8 = 2, j_6 = 0, j_7 = 1 and j_8 = 0. Here a'_m = -1 works for m = 6, 7, 8 and accordingly we may choose w_m = 1 for these values of m. Thus we have \delta_6 = -\theta^3 + 1, \delta_7 = -\theta^4 + \theta and \delta_8 = \sum_{j=0}^7 (-\theta)^j. Therefore by Theorem 1.3, \{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^{6-\theta+1}/3, \theta^{7-\theta^4+\theta}/3, \theta^{8+\sum_{j=0}^7 (-\theta)^j}/9\} is an integral basis of K.

Before explicitly stating an integral basis of \mathbb{Q}(\sqrt{a}), we introduce some notation.

Let K = \mathbb{Q}(\theta) be an algebraic number field with \theta a root of an irreducible polynomial x^n - a belonging to \mathbb{Z}[x] where |a| is a nth power free integer which is expressed as \prod_{j=1}^{n-1} a_j, a_j being squarefree relatively prime in pairs. Let n = \prod_{i=1}^k p_i^{d_i}, |a| = \prod_{j=1}^l q_j be the prime factorizations of n, |a| and let r_i be as in Theorem 1.1. For 0 < m \leq n - 1, C_m will stand for the number \prod_{j=1}^{n-1} a_j^{m/p^{d_i-1}}. We shall denote by S the set \{i \mid 1 \leq i \leq k, r_i \geq 1\}. For i \in S, denote d_i = \min(r_i, s_i). Note that for such an index i, p_i does not divide a, for otherwise r_i = v_{p_i}(a^{p_i-1} - 1) = 1 < 0. Since the interval [0, n - 1] can be partitioned into the union \bigcup_{k=0}^{n-1} [n - \frac{n}{p_i^k}, n - \frac{n}{p_i^k}] \cup [n - \frac{n}{p_i^k}, n - 1] of pairwise disjoint intervals, it follows that there exists a largest integer k_i,m, 0 \leq k_i,m \leq d_i and a non-negative integer j_i,m such that m = n - \frac{n}{p_i^k} + j_i,m. For 0 < m \leq n - 1, let S_m denote the subset of S defined by S_m = \{i \in S \mid k_i,m \geq 1\}. Fix a pair (i, m) with i \in S_m. Choose an integer b_i,m such that ab_i,m \equiv 1 mod(p_i^k) and set a'_i,m = (b_i,m)^{p_i^k-1-k_i,m} or b_i,m according to 1 \leq k_i,m < s_i or k_i,m = s_i. Corresponding to the pair (i, m), denote the integer \frac{n}{p_i^k} by n_i,m. Let w_{i,m} be an integer
such that $w_{i,m}C_m(a'_{i,m})^{p_{i,m}^{-1}} \equiv 1 \pmod {p_i^{k_{i,m}}}$; such $w_{i,m}$ exists because $p_i \nmid C_m a'_{i,m}$. Define $\delta_{i,m}$ belonging to $\mathbb{Z}[\theta]$ by $\delta_{i,m} = w_{i,m}C_m \theta^{j_{i,m}} \sum_{r=0}^{p_{i,m}^{-2}} (a'_{i,m})^r \theta^{n_{i,m}}$. Let $z_{i,m} = \prod_{j \in S_m \setminus \{i\}} p_j^{k_{j,m}}$ for $i \in S_m$. Since $\gcd(z_{i,m} | i \in S_m) = 1$, there exist integers $u_{i,m}$ such that $\sum_{i \in S_m} u_{i,m}z_{i,m} = 1$. Let $\beta_m$ equal $\sum_{i \in S_m} u_{i,m}z_{i,m} \delta_{i,m}$ or 0 according as $S_m \neq \emptyset$ or $S_m = \emptyset$. Observe that the highest power of $\theta$ occurring in $z_{i,m}$ is $j_{i,m} + n - 2n_{i,m} = m - n_{i,m} < m$ and hence the same holds for $\beta_m$. Note that when $S_m$ is a singleton set consisting of $\{i\}$, then $z_{i,m}$ being an empty product is 1 and $\beta_m = \delta_{i,m}$.

With the above notations, we shall prove the following theorem.

**Theorem 1.6.** Let $K = \mathbb{Q}(\theta)$ with $\theta$ having minimal polynomial $x^n - a$ over $\mathbb{Q}$ where $a$ is an $n$th power free integer and for every prime $p_i$ dividing $n$ either $p_i \nmid a$ or $v_{p_i}(a)$ is coprime to $p_i$. Let $n = \prod_{i=1}^{k} p_i^{q_i}$, $S, C_m, k_i, m$ and $\beta_m$ be as in the above paragraph. Then the following hold.

(i) If $S = \emptyset$, then $\left\{ \frac{\theta_m}{C_m} | 0 \leq m \leq n - 1 \right\}$ is an integral basis of $K$.

(ii) If $S \neq \emptyset$, then $\left\{ \frac{\theta_m + \beta_m}{C_m} | 1 \leq m \leq n - 1 \right\}$ is an integral basis of $K$.

**Remark 1.7.** In the paragraph preceding Theorem 1.6, note that $b'_{i,m}$ can be chosen to be any integer which is congruent to $a^{p_i-2}$ modulo $p_i^{k_{i,m}+1}$ because $a^{p_i-1} \equiv 1 \pmod {p_i^{r+1}}$ and $k_{i,m} \leq r$.

The following theorem which improves the results of [3, Theorems 2 and 3] will be quickly deduced from the above theorem.

**Theorem 1.8.** Let $n \geq 2$ be an integer with prime divisors $p_1, \ldots, p_k$. Let $K = \mathbb{Q}(\theta)$, $K' = \mathbb{Q}(\theta')$ be algebraic number fields of degree $n$, where $\theta, \theta'$ satisfy, respectively, the polynomials $x^n - a, x^n - a'$ with integers $a, a'$ squarefree which are congruent modulo $np_1 \cdots p_k$, then an element $\frac{1}{q}(c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1})$ with $c_i, q \in \mathbb{Z}$ is in $A_K$ if and only if $\frac{1}{q}(c_0 + c_1\theta' + \cdots + c_{n-1}\theta'^{n-1})$ is in $A_K$.

We now provide some examples to illustrate Theorem 1.6.

**Example 1.9.** Let $\theta$ be a root of $x^{10} - 150$ and $K = \mathbb{Q}(\theta)$. With notations as in Theorem 1.6, it can be easily seen that here $S = \emptyset$, $C_m = 1$ for $0 \leq m \leq 4$ and $C_m = 5$ for $5 \leq m \leq 9$. Hence $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7, \theta^8, \theta^9\}$ is an integral basis of $K$ by Theorem 1.6(i).

**Example 1.10.** Let $K = \mathbb{Q}(\theta)$, where $\theta$ is a root of $x^{10} - 2 \cdot 5^2 \cdot 13^5$. We retain the notations introduced in the paragraph preceding Theorem 1.6 and take $p_1 = 3, p_2 = 2, a = 2 \cdot 5^2 \cdot 13^5$. One can verify that $C_1 = 1, C_2 = 13, C_3 = 5 \cdot 13^2, C_4 = 5 \cdot 13^3, C_5 = 5 \cdot 13^4$. It can be easily seen $v_3(a^2 - 1) = r_1 + 1 \geq 2$ and $v_2(a - 1) = r_2 + 1 = 0$. Therefore $S = \{1\}$. One can quickly verify that $k_{1,m} = 0$ for $0 \leq m \leq 3$ and $k_{1,m} = 1$ for $m = 4, 5$; also $j_{1,4} = 0, j_{1,5} = 1$. Here $b'_{1,m} = -1$ works for $m = 4, 5$ and in view of this choice we may take $a'_{1,m} = -1$ for $m = 4, 5$. We may take $w_{1,m} = 2$ for $m = 4, 5$. Since $S = \{1\}$ is a singleton, we have $\beta_m = \delta_{1,m}$ for $m = 4, 5$. Substituting these values, we see that $\beta_4 = 10 \cdot 13^3(-\theta^2 + 1)$ and $\beta_5 = 10 \cdot 13^4(-\theta^3 + \theta)$. Therefore by Theorem 1.6(ii), $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7, \theta^8, \theta^9\}$ is an integral basis of $K$. 
Example 1.11. Let \( \theta \) be a root of \( x^6 - 37 \) and \( K = \mathbb{Q}(\theta) \). We retain the notations introduced in the paragraph preceding Theorem 1.6 and we take \( p_1 = 3 \), \( p_2 = 2 \) and \( a = 37 \). It is clear that \( v_3(a^2 - 1) = r_1 + 1 = 2 \) and \( v_2(a - 1) = r_2 + 1 = 2 \). Therefore \( S = \{1, 2\} \). One can easily verify that \( k_{1,m} = 0 \) for \( 0 \leq m \leq 3, k_{1,m} = 1 \) for \( m = 4, 5, j_{1,4} = 0 \) and \( j_{1,5} = 1 \). Here \( b_{1,m}' = 1 \) works for \( m = 4, 5 \) and so we may choose \( a_{1,m}' = 1 \) for \( m = 4, 5 \). Since \( a \) is squarefree, \( C_m = 1 \) for all \( m \); we may take \( w_{1,m}' = 1 \) for \( m = 4, 5 \). So \( \delta_{1,4} = \theta^2 + 1 \) and \( \delta_{1,5} = \theta^3 + \theta \). Further \( k_{2,m} = 0 \) for \( 0 \leq m \leq 2, k_{2,m}' = 1 \) for \( m = 3, 4, 5, j_{2,3} = 0, j_{2,4} = 1 \) and \( j_{2,5} = 2 \). Here \( b_{2,m}' = 1 \) works for \( m = 3, 4, 5 \) and in view of this choice \( a_{2,m}' = 1 \) for \( m = 3, 4, 5 \).

As \( C_m = 1 \) for all \( m \), we may take \( w_{2,m}' = 1 \) for \( m = 3, 4, 5 \). Thus \( \delta_{2,3} = 1, \delta_{2,4} = \theta \) and \( \delta_{2,5} = \theta^2 \). Note that \( S_m = \emptyset \) for \( 0 \leq m \leq 2 \), \( S_3 = \{2\} \) and \( S_4 = \{1, 2\} \) for \( m = 4, 5 \). Here \( z_{2,3} = 1, z_{1,m} = 2 \) for \( m = 4, 5 \) and \( z_{2,3} = 3 \) for \( m = 4, 5 \), therefore we can take \( u_{2,3} = 1 \) and \( u_{1,m}' = -1, u_{2,m}' = 1 \) for \( m = 4, 5 \). Note that \( \beta_1 = \beta_2 = 0, \beta_3 = \delta_{2,3} \) and \( \beta_m = u_{1,m} z_{1,m} \delta_{1,m} + u_{2,m} z_{2,m} \delta_{2,m} \) for \( m = 4, 5 \). Substituting these values, it follows quickly from Theorem 1.6(ii) that \( \{1, \theta, \theta^2, \frac{\theta^3+1}{2}, \frac{\theta^5-2\theta^2+3\theta-2}{6}, \frac{\theta^5-2\theta^3+3\theta^2-2\theta}{6}\} \) is an integral basis of \( K \).

§2. Proof of Lemmas 1.1 and 1.2.

Proof of Lemma 1.1. Multiplying \( \eta_k = 1 + (a'\theta'^n) + \cdots + (a'\theta'^n)^{p^k-1} \) by \((a'\theta'^n - 1)\) on both sides and using the fact that \( \theta'^n p^k = a \), we see that

\[
a'\theta'^n \eta_k = \eta_k + a(a')^{p^k} - 1.
\]

Now taking \( p^k \)-th power on both sides, we obtain

\[
a(a')^{p^k} \eta_k^{p^k} = \sum_{j=0}^{p^k} \left( \binom{p^k}{j} \right) \eta_k^{p^k-j} (a(a')^{p^k} - 1)^j,
\]

which can be rewritten as

\[
(a(a')^{p^k} - 1) \eta_k^{p^k} = \sum_{j=1}^{p^k} \left( \binom{p^k}{j} \right) (a(a')^{p^k} - 1)^j \eta_k^{p^k-j}.
\]

Note that \( a(a')^{p^k} \neq 1 \), for otherwise \( a = \pm 1 \) when \( p \) is odd and \( a = 1 \) when \( p = 2 \) which is impossible in view of irreducibility of \( x^n - a \) over \( \mathbb{Q} \). On dividing (1) by \( a(a')^{p^k} - 1 \), we have

\[
\eta_k^{p^k} = \sum_{j=1}^{p^k} \left( \binom{p^k}{j} \right) (a(a')^{p^k} - 1)^{j-1} \eta_k^{p^k-j}.
\]

Thus \( \eta_k \) satisfies the polynomial \( x^{p^k} - \sum_{j=1}^{p^k} \left( \binom{p^k}{j} \right) (a(a')^{p^k} - 1)^{j-1} x^{p^k-j} \); consequently, \( \frac{\eta_k}{p^k} \) satisfies the polynomial \( x^{p^k} - \sum_{j=1}^{p^k} \left( \binom{p^k}{j} \right) (a(a')^{p^k} - 1)^{j-1} x^{p^k-j} = h(x) \) (say). In view of the following Lemma 2.1, \( h(x) \in \mathbb{Z}[x] \) and so \( \frac{\eta_k}{p^k} \) is an algebraic integer as desired. \( \square \)

Lemma 2.1. Let \( x^n - a, p, s, r, k \) and \( a' \) be as in the above lemma. Then \( p^k \) divides \( \binom{p^k}{j} (a(a')^{p^k} - 1)^{j-1} \) for \( 1 \leq j \leq p^k \).

Proof. We first prove that

\[
a(a')^{p^k} \equiv 1 \pmod{p^{k+1}}.
\]

(2)
Keeping in mind that \( r + 1 = v_p(a^p - a) \) and the fact that \( k \leq r \), we have
\[
a^p \equiv a \pmod{p^{k+1}}. \tag{3}
\]

The proof of (2) is split into two cases. Consider first the case when \( k < s \). It follows from (3) that \( a^{p^{s-1}} \equiv a \pmod{p^{k+1}} \). Multiplying the last congruence by \((b')^{p^{s-1}} \) on both sides, we have \((ab')^{p^{s-1}} \equiv a(b')^{p^{s-1}} \pmod{p^{k+1}}\). By choice, \( ab' \equiv 1 \pmod{p^{k+1}} \); consequently using the last two congruences, we see that \( 1 \equiv a'(b')^{p^{s-1}}b^k \pmod{p^{k+1}} \). Recall that in the present case \( a' = (b')^{p^{s-1}} \). So \( a(a')^k \equiv 1 \pmod{p^{k+1}} \) proving (2) in this case. When \( k = s \), then by choice \( a' = b' \) which in view of the hypothesis \( ab' \equiv 1 \pmod{p^{k+1}} \) and (3) implies that \( 1 \equiv (ab')^k \equiv a(a')^k \pmod{p^{k+1}} \) and hence (2) is proved.

Let \( j \) be an integer such that \( 1 \leq j < p^k \). Fix a non-negative integer \( w \) for which \( p^w \leq j < p^{w+1} \). By a basic result, \( v_p(\binom{p}{j}) = k - v_p(j) \) (cf. [6, Lemma 2.D]). So \( p^{k-w} \) divides \( \binom{p}{j} \); consequently by virtue of (2) the lemma is proved once we show that \( jk \leq k - w + (j - 1)(k + 1) \), that is, \( 0 \leq j - w - 1 \), which clearly holds in view of the choice of \( w \).

\[ \square \]

Proof of Lemma 1.2. As pointed out in the paragraph preceding Lemma 1.1, \( \frac{\theta_m}{C_m} \) is an algebraic integer and hence the lemma is proved when \( k_m = 0 \). From now on, it may be assumed that \( k_m \geq 1 \). Denote \( \sum_{j=0}^{p^{k_m}-1} (a_m^{\theta_m})^j \) by \( \eta_m \). By hypothesis, \( p \nmid a \) so \( p \nmid C_m a_m \). Let \( w'_m \) be an integer such that
\[
w_m C_m (a_m')^{p^{k_m}-1} + w'_m p^{k_m} = 1. \tag{4}
\]

By Lemma 1.1, \( \frac{\eta_m}{p^{k_m}} \) is an algebraic integer and hence so is \( w_m \theta_m (\frac{\eta_m}{p^{k_m}}) + w'_m (\frac{\theta_m}{C_m}) = \beta \) (say). Using (4) together with the fact that \( j_m + n_m (p^m - 1) = j_m + (n - \frac{n}{p^{k_m}}) = m \), a simple calculation shows that
\[
\beta = \frac{\theta^m + \delta_m}{p^{k_m} C_m},
\]
where \( \delta_m = w_m C_m \theta_m \sum_{j=0}^{p^{k_m}-2} (a_m^{\theta_m})^j \). This proves the lemma.

\[ \square \]

§3. Proof of Theorems 1.3, 1.6 and 1.8. For algebraic integers \( \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n \) in \( K \) which are linearly independent over \( \mathbb{Q} \), \( D_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) \) will stand for the determinant of the \( n \times n \) matrix with \((i, j)\)-th entry \( T_{R_{K/\mathbb{Q}}}(\alpha_i \alpha_j) \). If \( M \) denotes the subgroup of \( \mathbb{C} \) with basis \( \alpha_1, \alpha_2, \ldots, \alpha_n \), then as is well known \( D_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = [A_K : M]^2 d_K \). So the problem of finding an integral basis of \( K \) is same as finding algebraic integers \( \gamma_1, \gamma_2, \ldots, \gamma_n \) in \( K \) such that \( D_{K/\mathbb{Q}}(\gamma_1, \gamma_2, \ldots, \gamma_n) = d_K \). We shall use the following elementary result proved in [7, Problem 435].

Lemma 3.A. Let \( t, n \) be positive integers. Then
\[
\sum_{m=1}^{n-1} \left\lfloor \frac{tm}{n} \right\rfloor = \frac{1}{2} [(n - 1)(t - 1) + \gcd(t, n) - 1].
\]

Proof of Theorem 1.6. We first prove the theorem when \( S = \emptyset \). As pointed out in the paragraph preceding Lemma 1.1, \( \frac{\theta_m}{C_m} \) is an algebraic integer for \( 1 \leq m \leq n - 1 \). The transition matrix from \( \{1, \frac{\theta}{C_1}, \frac{\theta^2}{C_2}, \ldots, \frac{\theta^{n-1}}{C_{n-1}}\} \) to \( \{1, \theta, \ldots, \theta^{n-1}\} \) has determinant \( \prod_{m=1}^{n-1} C_m = C \) (say). As is well known
\[
D_{K/\mathbb{Q}}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(n\theta^{n-1}) = (-1)^{\frac{(n-1)(n-2)}{2}} n^n d^{n-1}.
\]
Consequently using a basic result (cf. [8, Proposition 2.9]) and the above equation, we see that
\[
D_{K/Q}\left(1, \frac{\theta}{C_1}, \frac{\theta^2}{C_2}, \ldots, \frac{\theta^{n-1}}{C_{n-1}}\right) = \frac{1}{C^2} D_{K/Q}(1, \theta, \ldots, \theta^{n-1}) = \frac{(-1)^{(n-1)(n-2)}}{C^n a^{n-1}}.\tag{5}
\]
Applying Lemma 3.A, we have
\[
C = \prod_{m=1}^{n-1} \prod_{i=1}^{d_i} a_i^{\left\lfloor \frac{m}{d_i} \right\rfloor} = \prod_{i=1}^{n-1} \sum_{m=1}^{\frac{\lfloor n/d_i \rfloor}{d_i}} = \prod_{i=1}^{n-1} a_i^{\left\lfloor \frac{(n-1)(n-2)}{2} \right\rfloor a^{n-1}}.\tag{6}
\]
Substituting for \(C\) in (5), we obtain
\[
D_{K/Q}\left(1, \frac{\theta}{C_1}, \frac{\theta^2}{C_2}, \ldots, \frac{\theta^{n-1}}{C_{n-1}}\right) = \frac{(-1)^{(n-1)(n-2)}}{\prod_{i=1}^{n-1} a_i^{(n-1)(i-1)+\gcd(i,n)-1}}.\tag{7}
\]
Keeping in mind that \(a = \text{sgn}(a) \prod_{i=1}^{n-1} a_i^{l_i}\), a simple calculation shows that the above equation can be rewritten as
\[
D_{K/Q}\left(1, \frac{\theta}{C_1}, \frac{\theta^2}{C_2}, \ldots, \frac{\theta^{n-1}}{C_{n-1}}\right) = (-1)^{(n-1)(n-2)} \prod_{i=1}^{n-1} a_i^{n-\gcd(i,n)}.\tag{8}
\]
If \(\prod_{j=1}^{l_i} q_{ij}^{l_j}\) is the prime factorization of \(|a|\), then it can be easily seen that
\[
\prod_{i=1}^{n-1} a_i^{n-\gcd(i,n)} = \prod_{j=1}^{l_i} q_{ij}^{n-\gcd(i,n)}.\tag{9}
\]
It is immediate from (8) and Theorem 1.A that the right-hand side of (7) equals \(d_K\). So we conclude that \(\{1, \theta, \theta^2, \ldots, \theta^{n-1}\} = a^{n-1}\) is an integral basis of \(K\) in the present case. \(\square\)

We now deal with the case \(S \neq \emptyset\). Retaining the notation introduced in the paragraph preceding Theorem 1.6, we first show that \(\frac{\theta^m + \beta_m}{C_m} = \gamma_m\) (say) is an algebraic integer for \(1 \leq m \leq n - 1\). Fix any \(m, 1 \leq m \leq n - 1\). If \(S_m = \emptyset\), then by definition \(\beta_m = 0\) and \(\prod_{i \in S} \frac{k_i}{a_i}\) = 1 and so \(\gamma_m = \frac{\gamma_m}{C_m}\) is an algebraic integer. Consider now the situation when \(S_m \neq \emptyset\). Recall that when \(i \in S_m\), then \(z_{i,m} = \prod_{j \in S_m \setminus \{i\}} p_i^{k_{j,m}}\) and \(u_{i,m}\) are integers such that \(\sum_{i \in S_m} u_{i,m} z_{i,m} = 1\). Further by Lemma 1.2, the element \(\frac{\theta^m + \beta_m}{C_m}\) of \(K\) is an algebraic integer; consequently keeping in mind \(\sum_{i \in S_m} u_{i,m} z_{i,m} = 1\), we see that
\[
\sum_{i \in S_m} u_{i,m} \frac{C_m p_i^{k_{j,m}}}{C_m p_i^{k_{j,m}}} = \frac{\theta^m + \sum_{i \in S_m} u_{i,m} z_{i,m} \delta_{i,m}}{C_m \prod_{i \in S_m} p_i^{k_{j,m}}} = \frac{\theta^m + \beta_m}{C_m \prod_{i \in S_m} p_i^{k_{j,m}}} = \frac{\theta^m + \beta_m}{C_m \prod_{i \in S_m} p_i^{k_{j,m}}} = \gamma_m
\]
is an algebraic integer.

Taking \(\gamma_0 = 1\), it remains to be shown that \(D_{K/Q}(\gamma_0, \gamma_1, \ldots, \gamma_{n-1}) = d_K\). As pointed out at the end of the paragraph preceding Theorem 1.6, the power of \(\theta\) occurring in \(\beta_m\) is less than \(m\). So it is clear that the transition matrix from \(\{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}\) to \(\{1, \theta, \ldots, \theta^{n-1}\}\) has determinant \(\prod_{m=1}^{n-1}(C_m \prod_{i \in S} p_i^{k_{j,m}}) = C \prod_{i \in S} p_i^{\sum_{m=1}^{n-1} k_{i,m}}\), where \(C = \prod_{m=1}^{n-1} C_m\). Recall that \(k_{i,m}\) is the largest integer less than or equal to \(d_i\) such that \(m \geq n - \frac{n}{p_i^{d_i}}\). So when
1 \leq j \leq d_i - 1 \text{ and } n - \frac{n}{p_i'} \leq m < n - \frac{n}{p_i''}, \text{ we have } k_{i,m} = j \text{ and } k_{i,m} = d_i \text{ when } n - \frac{n}{p_i'} \leq m < n; \text{ consequently }

\sum_{m=1}^{n-1} k_{i,m} = \sum_{j=1}^{d_i-1} j \left( \frac{n}{p_i'} - \frac{n}{p_i''} \right) + d_i \frac{n}{p_i'} = \sum_{j=1}^{d_i} n \frac{n}{p_i'} = n \sum_{j=1}^{d_i} p_i^{q_j - j}.

Using the above equation together with (6), we see that the determinant of transition matrix from \{y_0, y_1, \ldots, y_{n-1}\} to \{1, \theta, \ldots, \theta^{n-1}\} equals \prod_{j=1}^{n-1} a_j \prod_{s \in S} p_i^{q_j - j}.

Now arguing exactly as in the previous case, it can be easily seen that

\[ D_{K/Q}(y_0, y_1, \ldots, y_{n-1}) = (-1)^{(n-1)(n-2)/2} \text{sgn}(a^{n-1}) \left( \prod_{s \in S} p_i^{v_j} \right) \prod_{j=1}^{n-1} a_j^{n - \text{gcd}(j,n)}, \]

where \( v_j \) equals \( ns_j - 2n_i \sum_{j=1}^{d_i} p_i^{q_j - j} \) or \( ns_j \) according to \( i \in S \) or not. In view of (8) and Theorem 1.6, the right-hand side of the above equation equals \( d_K \). Therefore \{y_0, y_1, \ldots, y_{n-1}\} is an integral basis of \( K \).

**Proof of Theorem 1.3.** It is immediate from the definition of \( k_m \) that \( k_m \geq 1 \) if and only if \( m \geq \Phi(p') \); consequently (with notations as in Theorem 1.6) \( \beta_m = 0 \) for \( 0 \leq m < \Phi(p') \) and hence the corollary follows at once from Theorem 1.6 and Remark 1.7. \( \square \)

**Proof of Theorem 1.8.** We retain the notation of Theorem 1.6 and adopt the convention that \( \beta_m = 0 \) for each \( m \) if \( S \) is empty. Since \( a \) is squarefree, \( C_m = 1 \) for \( 1 \leq m \leq n - 1 \). So in view of Theorem 1.6, \( \{1, \theta, \ldots, \theta^{n-1}\} \) is an integral basis of \( K \). Let \( \beta'_m \) denote the element of \( K' \) obtained on replacing \( \theta \) by \( \theta' \) in the expression for \( \beta_m \). The theorem is proved once we show that \( \{1, \theta^m + \beta'_m \mid 1 \leq m \leq n - 1\} \) is an integral basis of \( K' \). Fix any prime \( p \) dividing \( n \) and let \( s = v_p(n) \). Let \( r, r' \) stand, respectively, for \( v_p(a^{p-1} - 1) - 1, v_p(a'^{p-1} - 1) - 1 \). In view of the definition of \( \beta_m \), the desired assertion is proved once we show that

\[ \min\{r, s\} = \min\{r', s\}. \tag{9} \]

By hypothesis, \( a' \equiv a \mod np \). Note that (9) needs to be verified when \( p \nmid a \). Write \( a' = a + p^{r+1}b, b \in \mathbb{Z} \). So there exists \( c \in \mathbb{Z} \) such that

\[ r' + 1 = v_p(a'^{p-1} - a') = v_p(a^{p-1} - a + p^{r+1}c). \tag{10} \]

If \( r < s \), then the above equation shows that \( r' + 1 = r + 1 \), which proves (9) in this case. If \( r \geq s \), then by (10), \( r' + 1 \geq s + 1 \) and hence (9) is verified. This completes the proof of the theorem. \( \square \)

**References**

1. R. Dedekind, Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. *J. reine angew. Math.* **121** (1900), 40–123.
2. T. Funakura, On integral bases of pure quartic fields. *Math. J. Okayama Univ.* **26** (1984), 27–41.
3. I. Gałd and L. Remete, Integral basis and monogeneity of pure number fields. *J. Number Theory* **173** (2017), 129–146.
4. T. A. Gassert, A note on the monogeneity of power maps. *Albanian J. Math.* **11** (2017), 3–12.
5. A. Hameed and T. Nakahara, Integral bases and relative monogeneity of pure octic fields. *Bull. Math. Soc. Sci. Math. Roumanie* **58** (106) (2015), 419–433.
6. A. Jakhar, S. K. Khanduja and N. Sangwan, On the discriminant of pure number fields. *Colloq. Math.* (to appear).
7. J. M. de Koninck and A. Mercier, 1001 *Problems in Classical Number Theory*, American Mathematical Society (Providence, RI, 2007).
8. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer (Berlin–Heidelberg, 2004).
9. J. Westlund, On the fundamental number of the algebraic number field $k(\sqrt{m})$. *Trans. Amer. Math. Soc.* 11 (1910), 388–392.

Anuj Jakhar,
Department of Mathematics,
Indian Institute of Technology (IIT) Bhilai,
GEC Campus,
Raipur, 492015,
India
Email: anujjakhar@iisermohali.ac.in
anujjakhar@iithbilai.ac.in

Sudesh K. Khanduja,
Indian Institute of Science Education and Research
Mohali,
Sector 81, Knowledge City, SAS Nagar, Punjab 140306,
India
and
Department of Mathematics,
Panjab University, Chandigarh, 160014,
India
Email: skhanduja@iisermohali.ac.in

Neeraj Sangwan,
Indian Institute of Technology (IIT) Bombay,
Mumbai, 400076,
India
Email: neerajsan@iisermohali.ac.in