Integral Bases of Number Fields Composed of Quadratic Extensions of $\mathbb{Q}$

D. Chatelain

1973
Ann. Univ. Besançon, Math. fasc. â 6.

This is a translation of *Bases des entiers des corps composés par des extensions quadratiques de* $\mathbb{Q}$. Translated and edited by Zack Baker (May 2016). Additional editing by Amy Feaver. Last updated June 2016.

Introduction

We study n-quadratic number fields, $n \geq 1$. Let $k_n = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})$ be a degree 2^n extension of $\mathbb{Q}$ obtained by joining the square root of n squarefree rational integers $a_1, ..., a_n$. In this paper, we seek to explicitly determine the integral bases of the rings of integers of k_n.

We will define these fields by their discriminant $(\Delta_\lambda)_{\lambda \in \Lambda}$. Define

$$\Lambda_1 = \{\lambda \in \Lambda : \Delta_\lambda \equiv 1 \pmod 4\}.$$

Any k_n has an associated subfield K given obtained by adjoining all of the elements in the set $\left\{\sqrt{\Delta_\lambda} : \lambda \in \Lambda_1\right\}$.

We know that the product of integral bases of two rings of integers with relatively prime discriminants is an integral basis made up of integers of the two subfields. This result allows us to determine the ring of integers of K and the ring of integers of any subfield K of k_n.

Recall that a normal integral basis is one that is comprised of conjugates of the same integer. We show that if k_n has a normal integral basis then this basis is unique. It is shown that in all cases the discriminant of k_n over K is equal to the product of discriminants of all in quadratic fields of k_n. These results generalize those obtained by Kenneth S. Williams in the case n=2 [1].

1 Construction and properties of the field k_n

1.1 How to define the field k_n

It is assumed that the n quadratic fields which generate k_n are given. The generator for each of these quadratic fields is given by $\alpha = \sqrt{a}$ for some squarefree

$a \in \mathbb{Z}$. We will denote these generators by α_{2^k}, $0 \le k \le n-1$. Also, for $0 \le k \le n-1$, let $A_{2^k} := \alpha_{2^k}^2$.

Of course, the numbers α_{2^k} must satisfy the condition:

$$\alpha_{2^k} \notin \mathbb{Q}(\alpha_{2^0}, \alpha_{2^1}, \dots \alpha_{2^{k-1}}), \quad 1 \le k \le n-1 \tag{1}$$

or the equivalent relationship:

$$\mathbb{Q}(\alpha_{2^k}) \cap \mathbb{Q}(\alpha_{2^0}, \dots, \alpha_{2^{k-1}}) = \mathbb{Q}, \quad 1 \le k \le n-1.$$

It follows that the field $k_n = \mathbb{Q}(\alpha_{2^0}, \dots, \alpha_{2^{n-1}})$ is a Galois extension of $\mathbb{Q}$ of degree 2^n whose Galois group G_n is isomorphic to the Cartesian product of n copies of $\mathbb{Z}_2$. All its components except the identity are of order 2 and G_n is abelian.

Conversely, if we define k_n as an abelian extension of $\mathbb{Q}$ of degree 2^n whose Galois group is equal to the direct product $g_0 \times g_1 \times \dots \times g_{n-1}$ n subgroups of order 2, k_n is spanned by the n generators quadratic extensions $\mathbb{Q}$ number field of $g_0 \times \dots \times id \times \dots \times g_{n-1}$ or id subgroups replace g_k for $0 \le k \le n-1$ [2].

1.2 Choosing a basis k over $\mathbb{Q}$

For j not a power of two with $1 \le j < 2^{n-1}$, we define by induction the numbers A_j from the numbers A_{2^k}. For $j = i + 2^k$, $0 < i < 2^k$, $1 \le k \le n-1$:

$$A_j = \frac{A_i \cdot A_{2^k}}{(d_{i,2^k})^2}, \tag{2}$$

where $d_{i,2^k} = \gcd(A_i, A_{2^k})$. It will be specified in Chapter 2 the choice of the sign of $d_{i,2^k}$. Therefore, for j $= i + 2^k$, $0 < i < 2^k$, $1 \le k \le n-1$:

$$\alpha_j = \frac{\alpha_i \cdot \alpha_{2^k}}{d_{i,2^k}} \quad . \tag{3}$$

Furthermore, it asks: $\alpha_0 = A_0 = 1$

A_j $0 \le j \le 2^n - 1$ are squarefree rational integers and the roots of the polynomial $X^2 - A_j$.

Lemma 1.

$$N = \{\alpha_j : 0 \le j \le 2^n - 1\} \textit{ is a basis for } k \textit{ over } \mathbb{Q}$$

The field k_n is composed of $\mathbb{Q}(\alpha_{2^k})$ and satisfies the condition (1). It therefore has a product of bases $\{1, \alpha_{2^k}\}$, $0 \le k \le n-1$. The elements of this basis are of the form $\lambda_j \alpha_j$, $0 \le j \le 2^n - 1$ with $\lambda_j \in \mathbb{Z} - \{0\}$; $\{\alpha_j : 0 \le j \le 2^n - 1\}$ together is also a basis of k_n over $\mathbb{Q}$

1.3 Galois group G of k_n over $\mathbb{Q}$

Let σ be any automorphism of k_n fixing $\mathbb{Q}$. We can define this automorphism by giving the values of $\sigma(\alpha_{2^k})$ for $0 \leq k \leq n-1$. The values of σ for other elements of the basis of N of k_n over $\mathbb{Q}$ are deduced by these relations

The numbers $\alpha_{2^k}^2 \in \mathbb{Z}$, are invariant under σ; therefore we have

$$\sigma(\alpha_{2^k}) = \pm\alpha_{2^k}.$$

Let σ_0 denote the identity automorphism of k_n and σ_{2^p}, $0 \leq p \leq n-1$, be the elements of G_n defined by

$$\sigma_{2^p}(\alpha_{2^p}) = -\alpha_{2^p}$$
$$\sigma_{2^p}(\alpha_{2^k}) = \alpha_{2^k} \text{ for } k \neq p \text{ and } 0 \leq k \leq n-1 \tag{4}$$

Let g_p be subgroup $\{\sigma_0, \sigma_{2^p}\}$ of G_n. Then G_n is equal to the direct product $g_0 \times g_1 \times \ldots \times g_{n-1}$ of its subgroups g_p.

This results from the isomorphism between G_n and the Cartesian product $h_0 \times h_1 \times \ldots \times h_{n-1}$ Galois groups $\mathbb{Q}(\alpha_{2^p})$, this isomorphism maps has an element of G_n, the n-tuple of its restrictions on the field $\mathbb{Q}(\alpha_{2^p})$, and the subgroup g_p the subgroup:

$$\{id\} \times \ldots \{id\} \times h_p \times \{id\} \times \ldots \times \{id\}$$

Then for $j = i + 2^k$, $0 < i < 2^k$, and $1 \leq k \leq n-1$,

$$\sigma_j = \sigma_i \circ \sigma_{2^k} \tag{5}$$

The Galois group G_n is equal to the set of all σ_i, for $0 \leq i \leq 2^n - 1$ and we have:

$$\sigma_i(\alpha_j) = \pm\alpha_j$$

Let $\sigma_i(\alpha_j) = a_{ij}\alpha_j$ $(0 \leq i \leq 2^n - 1$ and $0 \leq j \leq 2^n - 1)$, and let A_n be the square matrix of order 2^n whose general term is $a_{ij} = \dfrac{\sigma_i(\alpha_j)}{\alpha_j}$

Lemma 2. *The matrix A_n is defined by the recurrence relation:*

$$A_0 = (1)$$

$$A_n = \begin{Vmatrix} A_{n-1} & A_{n-1} \\ A_{n-1} & -A_{n-1} \end{Vmatrix}$$

Proof. The $\mathbb{Q}$-automorphisms of the subfield $k_{n-1} = \mathbb{Q}(\alpha_{2^0}, \ldots \alpha_{2^{n-2}})$ of k_n are the restrictions on k_{n-1} elements σ_i, $0 \leq i \leq 2^{n-1} - 1$, of some subgroup $g_0 \times \ldots \times g_{n-2}$ of G_n. We can therefore identify the Galois group G_{n-1} of k_{n-1} over $\mathbb{Q}$ with the subgroup $g_0 \times \ldots \times g_{n-2}$ of G_n. Under these conditions the entries of the matrix A_{n-1} are $\dfrac{\sigma_i \alpha_i}{\alpha_j}$ for $0 \leq i \leq 2^{n-1}$ and $0 \leq j \leq 2^{n-1} - 1$ and are coincident with the elements a_{ij} of A_n of even index.

It remains to show that one has the relationships

$$a_{i,j+2^n-1} = a_{i,j}$$

$$a_{i+2^n-1,j} = a_{i,j}$$

$$a_{i+2^n-1,j+2^n-1,j} = a_{i,j}$$

for $0 \leq i \leq 2^{n-1} - 1$ and $0 \leq j \leq 2^{n-1} - 1$

Just use the relationships

$$\sigma_{i+2^{n-1}} = \sigma_i \circ \sigma_{2^{n-1}}$$

$$\alpha_{j+2^{n-1}} = \frac{\alpha_j \alpha_2^{n-1}}{d_{j,2^{n-1}}} \text{ with } d_{j,2^{n-1}} \in \mathbb{Z}$$

$$\sigma_{2^{n-1}}(\alpha_j) = \alpha_j$$

$$\sigma_i(\alpha_{2^{n-1}}) = \alpha_{2^{n-1}}$$

$$\sigma_{2^{n-1}}(\alpha_{2^{n-1}}) = -\alpha_{2^{n-1}}$$

$$\sigma_i(\alpha_j) = a_{ij}$$

these relations are valid for $0 \leq i \leq 2^{n-1} - 1$ and $0 \leq j \leq 2^{n-1} - 1$

□

1.4 Quadratic subfields of k_n

An element $x = \sum_{i=0}^{2^{n-1}} Q_i \alpha_i$ of k_n (with $Q_i \in \mathbb{Q}$) is less than or equal to degree 2 over $\mathbb{Q}$ if an only if it has at most 2 distinct conjugates. That is to say, if there exists a $j \in \{1, \ldots, 2^n - 1\}$ such that $x = Q_0 + Q_j \alpha_j$.

k_n thus admits $2^n - 1$ distinct quadratic subfields: the fields $\mathbb{Q}(\alpha_j)$ for $1 \leq j \leq 2^n - 1$.

1.5 Group $\hat{G}_n$ of characters G_n

The characters of a finite abelian group G are homomorphisms of G in the multiplicative group of complex numbers of modulo 1. They form a group $\hat{G}$ under the operation

$$(\chi, \chi') \to \chi \cdot \chi' \text{ is defined by } \chi \cdot \chi'(\sigma) = \chi(\sigma) \cdot \chi'(\sigma)$$

.

The group is isomorphic to G. Let $\sigma_1, \sigma_2, \ldots, \sigma_h$ be the elements of G and $\chi_1, \chi_2, \ldots, \chi_h$, the elements of $\hat{G}$. Let A be the square matrix of order h whose general term is $\chi_i(\sigma_j)$.

The "orthogonality relations" characters can be written [3]:

$$A \cdot \overline{A}^t = h \cdot l_h = \overline{A}^t \cdot A$$

Where l_h denotes the unit matrice of order h and $\overline{A}$ the matrix of complex numbers $\overline{\chi_i(\sigma_j)}$ conjugates of $\chi_i(\sigma_j)$.

As $\|\chi_i(\sigma_j)\| = 1$ was :

$$\overline{\chi_i(\sigma_j)} = \chi_i^{-1}(\sigma_j) = \chi_i(\sigma_j^{-1})$$

Lemma 3. *The group $\hat{G_n}$ of the characters of G_n is all applications of χ_i, $0 \leq i \leq 2^n - 1$, in G_n in the group $\{-1, 1\}$ is defined by:*

$$\chi_i(\sigma_j) = \frac{\sigma_j(\alpha_i)}{\alpha_i} = a_{j,i}. \tag{6}$$

Proof. For $\sigma_i^2 = \sigma_0$ and for all $\sigma_i \in G_n$, the characters of G_n are the homomorphisms of G_n into the group $\{1, -1\}$. The map:

$$\chi_i : \sigma_j \longrightarrow \frac{\sigma_j(\alpha_i)}{\alpha_i} = a_{j,i}$$

is a mapping of G_n to $\{1, -1\}$. This is a homomorphism because

$$\chi_i(\sigma_j \circ \sigma_k) = \frac{\sigma_j[\sigma_k(\alpha_i)]}{\alpha_i} = \frac{\sigma_j(a_{ki}\alpha_i)}{\alpha_i} = a_{ki}a_{ji}$$

.

On the other hand, if $\chi_i = \chi_k$,

$$\frac{\sigma_j(\alpha_i)}{\alpha_i} = \frac{\sigma_j(\alpha_k)}{\alpha_k} \text{ for } 0 \leq j \leq 2^n - 1$$

.

Then:

$$\sigma_j\left(\frac{\alpha_i}{\alpha_k}\right) = \frac{\alpha_i}{\alpha_k} \text{ for } 0 \leq j \leq 2^n - 1$$

Therefore, $\dfrac{\alpha_i}{\alpha_k}$ is in $\mathbb{Q}$, the fixed group of G_n. If $i \neq k$, α_i and α_k are linearly independent over $\mathbb{Q}$, so if we have $\chi_i = \chi_k$ then we must have $i = k$ and the relation (6) defines the 2^n characters of G_n

□

Corollary 4. *The general term of the matrix A_n is*

$$a_{i,j} = \frac{\sigma_i(\alpha_j)}{\alpha_j}$$

verified relations:

$$A_n^t = A_n$$

$$A_n^{-1} = \frac{1}{2^n} A_n$$

$$\det A_1 = -2 \textit{ and } \det A_n = (2^n)^{2^{n-1}} \textit{ for } n > 1$$

Proof. The recurrence formula defining A_n from A_{n-1} with $A_0 = (1)$ (Lemma 2) shows that A_n is a symmetric matrix and $A_n = A_n^t = (\chi_i(\sigma_j))$

On the other hand, A_n is real. The characters of the orthogonality relations thus translate:

$$A_n^{-1} = \frac{1}{2_n} a_n \quad \text{and} \quad \| \det \ A_n \| = (2^n)^{2^{n-1}}.$$

To specify det A_n, we see for $n \geq 1$:

$$\det \ A_n = \det \begin{pmatrix} 2A_{n-1} & A_{n-1} \\ 0 & -A_{n-1} \end{pmatrix} = (-1)^{2^{n-1}} \cdot 2^{2^{n-1}} \cdot (\det \ A_{n-1})^2.$$

If $n \geq 2$ then det $A_n > 0$

For $n = 1$, $A_1 = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}$ where det $A_1 = -2$.

For $n = 0$, $A_0 = (1)$ where det $A_0 = 1$.

□

1.6 Calculation of the discriminants

We note $\Delta(x_i : 0 \leq i \leq 2^n - 1)$ is the discriminant over $\mathbb{Q}$ of a family $(x_i)_{0 \leq i \leq 2^n - 1}$ of k_n elements. We have:

$$\Delta = \Delta(\alpha_i : 0 \leq i \leq 2^n - 1) = \det(\sigma_k(\alpha_j))^2 = \det(a_{kj} a_j)^2$$

$$\Delta = \left[\det \ A_n \left\| \begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & a_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{2^n-1} \end{matrix} \right\| \right]^2$$

Then:

$$\Delta(\alpha_i : 0 \leq i \leq 2^n - 1) = (2^n)^{2^n} \cdot \prod_{i=1}^{2^n-1} A_i.$$

If $x_i = \sum_{j=0}^{2^n-1} P_{ij} \alpha_j$ for $0 \leq i \leq 2^n - 1$ with $P_{ij} \in \mathbb{Q}$, then:

$$\Delta(x_i : 0 \leq i \leq 2^n - 1) = \det(P_{ij})^2 \cdot \Delta(\alpha_i : 0 \leq i \leq 2^n - 1).$$

2 Determination of integers of $\mathbb{Z}$ of k_n and the discriminant of k_n over $\mathbb{Q}$

2.1 Choice of n generators for k_n

Let $S = \{A_{2^0}, \cdots, A_{2^{n-1}}\}$ be the set of squarefree rational integers n, square roots generate k_n. Also define:
$S_1 := \{A_{2^i} | A_{2^i} \equiv 1 \pmod 4, 0 \leq i \leq n-1\}$,
$S_2 := \{A_{2^i} | A_{2^i} \equiv 2 \pmod 4, 0 \leq i \leq n-1\}$, and
$S_3 := \{A_{2^i} | A_{2^i} \equiv 3 \pmod 4, 0 \leq i \leq n-1\}$.

We have: $S = S_1 \cup S_2 \cup S_3$

Let us show that we can reduce to the case $|S_2| \leq 1$ and $|S_3| \leq 1$.

Suppose we have $|S_2| \geq 1$. Let A and B be two distinct elements of S_2, and let $2c$ be the gcd of A and B. We have: $A = 2cb$, $B = 2ca$, with a and b being coprime and odd.

Let $C = ab$. Then:

$$C = \pm 1 \pmod 4 \text{ and } \mathbb{Q}(\sqrt{A}, \sqrt{B}) = \mathbb{Q}(\sqrt{A}, \sqrt{C})$$

Therefore B can be replaced by C throughout S to decrease the number of A_{2^j} congruent to 2 mod 4. This process can be repeated until $|S_2| \leq 1$.

We then consider the set S_3. Suppose it contains two distinct elements D and E (congruent to 3 mod 4). Let $F := \dfrac{DE}{(\gcd(D,E))^2}$. Then $F \equiv 1 \pmod 4$ and $\mathbb{Q}(\sqrt{D}, \sqrt{E}) = \mathbb{Q}(\sqrt{D}, \sqrt{F})$.

We can replace the number in S, E with F and ultimately reduce to the case or S contains at most one element congruent to $2 \pmod 4$ and an element congruent to $3 \pmod 4$.

We return to the study of

$$k_n = \mathbb{Q}(\alpha_{2^0}, \alpha_{2^1}, \ldots, \alpha_{2^{n-3}}, \delta\alpha_{2^{n-2}}, \delta'\alpha_{2^{n-1}}) \quad \text{with} \quad \{\delta, \delta', \delta{\cdot}\delta'\} \subset \{1, \sqrt{-1}, \sqrt{2}, \sqrt{-2}\}$$

and $A_{2^i} = (\alpha_{2^i})^2 \equiv 1 \pmod 4$ for $0 \leq i \leq n-1$.

Note:

We assume that the degree of k_n overs $\mathbb{Q}$ is 2^n and that for every index $k \in \{0, \ldots n-1\}$, the square A_{2^k} of α_{2^k} is a rational integer congruent to 1 (mod 4). The numbers $\alpha_{2^{n-2}}$ and $\alpha_{2^{n-1}}$ may possibly be congruent to 1.

For $0 \leq i \leq 2^n - 1$ we define by induction the numbers A_i by setting: $A_0 = 1$ and if $0 < j < 2^k$ and $0 \leq k \leq n-1$:

$$A_{j+2^k} = \frac{A_j A_{2^k}}{\|d_{j,2^k}\|} 2$$

The numbers A_{2^k} are all congruent to 1 (mod 4). It is the same for the numbers A_i for $0 \leq i \leq 2^n - 1$. We can then define $D_{j,2^k}$ as the gcd of A_j and A_{2^k}, congruent to $1 \pmod 4$.

We define:

$$\alpha_0 = 1$$
$$\text{if } 0 < j < 2 \text{ and } 0 \leq k \leq n-1, \quad \alpha_{j+2^k} = \frac{\alpha_j \alpha_{2^k}}{d_{j,2^k}}$$

For all $i \in \{0, \ldots, 2^n - 1\}$ and i not a power of 2, α_i is a root of the polynomial $X^2 - A_i$. It is completely determined by the numbers A_{2^k} and the choice of the root α_{2^k} of A_{2^k}

Note that if $\alpha_{2^{n-2}}$ is equal to 1, we have for $0 < i < 2^{n-2}$, $\alpha_{i+2^{n-2}} = \alpha_i$

The basis B of k_n over $\mathbb{Q}$ corresponds to the construction of this given in Section 1.2 is:

$$B = \{\beta_s : 0 < s < 2^n - 1\}$$

For $0 \leq 2^{n-2} - 1$:

$$\beta_i = \alpha_i$$
$$\beta_{i+2^{n-2}} = \delta \alpha_{i+2^{n-2}} = \frac{\delta \cdot \alpha_i \alpha_{2^{n-2}}}{d_{i,2^{n-2}}}$$
$$\beta_{i+2^{n-1}} = \delta' \alpha_{i+2^{n-1}} = \frac{\sigma' \cdot \alpha_i \cdot \alpha_{2^{n-1}}}{d_{i,2^{n-1}}}$$
$$\beta_{i+2^{n-1}+2^{n-2}} = \delta\delta' \alpha_{i+2^{n-1}+2^{n-2}} = \delta\delta' \frac{\alpha_i \cdot \alpha_{2^{n-2}} \cdot \alpha_{2^{n-1}}}{d_{i,2^{n-2}d} i + 2^{n-2}, 2^{n-1}}$$

2.2 Reminders

Many classical results of numbers theory are useful for this paper.

Theorem 5. *On the composition of number fields whose discriminants are relatively prime ([4], [5]) K and K' are two finite extensions of $\mathbb{Q}$ with degrees d and d', respectively. We note that KK' is the smallest subfield of $\mathbb{Q}$ containing K and K'.*

Let $\mathcal{O}_K, \mathcal{O}_{K'}, \mathcal{O}_{KK'}$ be the rings of integers of K, K' and KK'. Let $\Delta_K, \Delta_{K'}$, and $\Delta_{KK'}$, the discriminants of $\mathbb{Q}$. Assume that Δ_K and $\Delta_{K'}$ are coprime, so:

1. *K and K' are linearly disjoint, i.e.:*
   $[K : \mathbb{Q}] \cdot [K' : \mathbb{Q}] = [KK' : \mathbb{Q}]$
2. *If $\{e_1, \ldots, e_d\}$ and $\{e'_1, \ldots, e'_{d'}\}$ are integral bases of $\mathcal{O}_K$ and $\mathcal{O}_{K'}$, then $\{e_i \cdot e'_j : 1 \leq i \leq d; 1 \leq j \leq d'\}$ is a basis of $\mathcal{O}_{KK'}$*
3. *$\Delta_{KK'} = (\Delta_K)^{d'} \cdot (\Delta_{K'})^d$*

Rings of integers and discriminants of quadratic extensions of $\mathbb{Q}$:

If A is a rational integer, the ring of integers over $\mathbb{Q}(\sqrt{A})$ admits a basis over $\mathbb{Z}$:

1. $\{1, \sqrt{A}\}$ if $A \equiv 2 \pmod 4$ or $A \equiv -1 \pmod 4$). The discriminant of $\mathbb{Q}(\sqrt{A})$ over $\mathbb{Q}$ is then $\Delta = 4A$.
2. $\left\{\dfrac{1+\sqrt{A}}{2}, \dfrac{1-\sqrt{A}}{2}\right\}$ if $A \equiv 1 \pmod 4$. The discriminiant of $\mathbb{Q}(\sqrt{A})$ over $\mathbb{Q}$ is then $\Delta = A$.

Rings of integers and discriminants of the field $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$:

This field is the field with the 8^{th} root of unity. Apply the results concerning the index of the cyclotomic field p^r with p the first case $p = 2; r = 3$ [5].

The ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ has integral basis $\{1, \theta, \theta^2, \theta^3\}$ where θ is the $8th$ primitive root of unity. One can take the basis $\left\{1, \delta, \sqrt{-1}, \dfrac{\delta + \sqrt{-1}\delta}{2}\right\}$ with $\delta \in \{\sqrt{2}, \sqrt{-2}\}$. The discriminant of $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ over $\mathbb{Q}$ is:

$$\Delta = p^{p^{r-1}(pr-r-1)} = 2^8$$

Lemma 6. *Let K and K' be finite abelian extentions of $\mathbb{Q}$ such that $K \subset K'$. Let $\mathcal{O}$ and $\mathcal{O}'$ be rings of integers over $\mathbb{Z}$, G and G' their Galois groups over $\mathbb{Q}$ and H the subgroup of G whose number field is K. If the $\mathbb{Z}$-module $\mathcal{O}'$ admits a normal basis, that is to say, a basis formed of an integer ϵ' and its conjugates with respect to $\mathbb{Q}$, then $\mathcal{O}$ has a basis consisting of $\epsilon = \sum_{\tau \in H} \tau(\epsilon')$ and its conjugate with respect to $\mathbb{Q}$*

Proof. Let ϵ be invariant under the elements of H, $\epsilon \in K \cap \mathcal{O}' - \mathcal{O}$. The $\mathbb{Z}$-module is generated by ϵ and its conjugates are included in $\mathcal{O}$. Conversely, if $x \in \mathcal{O} \subseteq \mathcal{O}'$, then for $\tau \in H$:

$$x = \sum_{\sigma' \in G'} \lambda_{\sigma'} \cdot \sigma'(\epsilon') = \tau(x) = \sum_{\sigma' \in G'} \lambda_{\sigma'} \cdot \tau \circ \sigma'(\epsilon') = \sum_{\sigma' \in G'} \lambda_{\sigma' \circ \tau} - 1 \cdot \sigma'(\epsilon')$$

where $\lambda'_{\sigma} = \lambda_{\sigma' \circ \tau} - 1$ for all $\tau \in H$

$$\sum_{t \in H} \tau(x) = (|H|)x = \sum_{\sigma' \in G} \lambda_{\sigma'} \cdot \sigma' \left(\sum_{\tau \in H} \tau(\epsilon') \right) = \sum_{\sigma' \in G'} \lambda_{\sigma'} \cdot \sigma'(\epsilon)$$

C is an equivalence class of G' mod H. Let $\lambda_{\sigma_c}$and $\sigma_c(\epsilon)$ be values of $\lambda_{\sigma'}$, and $\sigma'(\epsilon)$ when σ' describes c.

$$(|H|)x = \sum_{C \in G'/H} \left(\sum_{\sigma' \in C} \lambda_{\sigma'} \cdot \sigma'(\epsilon) \right) = \sum_{C \in G'/H} (|H|)\lambda_{\sigma_c} \cdot \sigma_c(\epsilon)$$

G and G'/H are isomorphic to $\sigma_c(\epsilon)$ for $C \in G'/H$ and are equal to $\sigma(\epsilon)$ for $\sigma \in G$.

Therefore, x is a $\mathbb{Z}$-module generated by the conjugates of ϵ with respect to $\mathbb{Q}$ □

Lemma 7. *Let $\mathcal{O}$ and $\mathcal{O}'$ be rings of integers of number fields K and K' such that $K \subset K'$. We denote d and d' over the degrees over $\mathbb{Q}$ of K and K'. If $\{e_1, \dots, e_d, e_{d+1}, \dots, e_{d'}\}$ is a basis of $\mathcal{O}'$ over $\mathbb{Z}$ such that $e_1, \dots, e_d$ belongs to $\mathcal{O}$, then $\{e_1, \dots, e_d\}$ is an integral basis of $\mathcal{O}$. There is also an integral basis for $\mathcal{O}'$ satisfying these conditions.*

Proof. $\{e_1, \dots, e_q, e_{q+1}, \dots, e_{q'}\}$ is also a basis of K' over $\mathbb{Q}$ containing the basis $\{e_1, \dots, e_q\}$. On the other hand we have $\mathcal{O} = K \cap \mathcal{O}'$.So if $x \in \mathcal{O}$ was:

$$x = \sum_{i=1}^{q} \lambda_i e_i \quad \text{with} \quad \lambda_i \in \mathbb{Q}$$

$$x = \sum_{j=1}^{q'} \mu_j e_j \quad \text{with} \quad \mu_j \in \mathbb{Z}$$

Where $\lambda_i = \mu_i \in \mathbb{Z}$ for $1 \leq i \leq q$ and x belongs to $\mathbb{Z}$-module free basis $\{e_1, \dots, e_q\}$. Since $e_1, \dots, e_q$ belongs to $\mathcal{O}$, they form a basis of $\mathcal{O}$. □

Existence of the basis $\{e_1, \dots, e_q, e_{q+1}, \dots, e_{q'}\}$:

$\mathcal{O}$ is a submodule of $\mathcal{O}'$ of rank q, free module of rank q' over the main ring $\mathbb{Z}$. So there is a basis of $\{e_1, \dots, e_q, e_{q+1}, \dots, e_{q'}\}$ of $\mathcal{O}'$ and nonzero elements $a_1, \dots, a_q$, such that $\{a_1 e_1, \dots, a_q e_q\}$ is a basis of $\mathcal{O}$; $e_1, \dots, e_q$ therefore belongs to K, therefore $K \cap \mathcal{O}' = \mathcal{O}$ forms a basis for $\mathcal{O}$.

2.3 Rings of integers and discriminants of $k_n = \mathbb{Q}(\alpha_{2^0}, \dots, \alpha_{2^{n-1}})$ with $(\alpha_{2^k})^2 = A_{2^k} \equiv 1 \pmod 4$ for $0 \leq k \leq n-1$

Compared with results from Section 2.1, we study the field k_n corresponding to $\delta = \delta' = 1$. First study the special case where the A_{2^k} are distinct primes and are congruent to $1 \pmod 4$.

Proposition 8. *Let $p_{2^0}, \dots, p_{2^{m-1}}$, be distinct prime numbers in $\mathbb{Z}$, and congruent to 1 $\pmod 4$. Let π_{2^k} be the square roots of p_{2^k} and let:*

$$\ell_m = \mathbb{Q}(\pi_{2^0}, \dots, \pi_{2^{m-1}})$$

Then ℓ is an extension of $\mathbb{Q}$ of degree 2^m, the discriminant with respect to $\mathbb{Q}$ is:

$$\Delta_m = \left(\prod_{k=0}^{m-1} p_{2^k}\right)^{2^{m-1}}$$

The ring $\mathcal{O}_m$ of integers of ℓ_m is the free $\mathbb{Z}$-module of rank 2^m admits a basis built of the conjugates with respect to the element of $\mathbb{Q}$:

$$\theta_m = \prod_{k=0}^{m-1} \frac{(1 + \pi_{2^k})}{2}$$

Proof. This proof is by induction on m. The proposition is true for $m = 1$ (results on quadratic fields). Suppose it is true for $m-1$. The discriminant Δ_{m-1} of $\mathcal{L}_{m-1}$ is relatively prime to the discriminant of $\mathbb{Q}(\pi_{2^{m-1}})$ which is equal to $p_{2^{m-1}}$.

We have $\mathcal{L}_m = \mathcal{L}_{m-1} \cdot \mathbb{Q}(\pi_{2^{m-1}})$. The theorem on the composition of the field of prime discriminants applies: $\mathcal{L}_m$ is of degree 2, admitting the discriminant:

$$\Delta_m = (\Delta_{m-1})^2 (p_{2^{m-1}})^{2^{m-1}} = \left(\prod_{k=0}^{m-1} p_{2^k}\right)^{2^{m-1}}$$

$\mathcal{O}_m$ admits to basis the product of the basis formed of $\mathcal{O}_{m-1}$ formed of θ_{m-1} and conjugate with respect to $\mathbb{Q}$ and the basis $\{\dfrac{1+\pi_{2^{m-1}}}{2}, \dfrac{1-\pi_{2^{m-1}}}{2}\}$ of the ring of integers of $\mathbb{Q}(\pi_{2^{m-1}})$

It is the basis consisting of θ_m and its conjugates relative to $\mathbb{Q}$. Indeed $\theta_m = \theta_{m-1} \cdot \dfrac{1+\pi_{2^{m-1}}}{2}$. □

Theorem 9. *Let $k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$.*

(a) The following conditions are equivalent:

(i) The ring of integers $\mathcal{O}_n$ of $k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$ has a normal basis over $\mathbb{Z}$.

(ii) The n quadradic subfields of $\mathbb{Q}(\alpha_{2^k})$ composing k_n have discriminant congruent to 1 $\pmod 4$.

(iii) The rings of the number field $\mathbb{Q}(\alpha_{2^k})$ admits normal bases over $\mathbb{Z}$.

(b) When there conditions are met, the normal basis of $\mathcal{O}_n$ is unique to the order almost entirely and the sign near one of its generators; generators can be taken to be:

$$\epsilon_n = \sum_{i=0}^{2^n-1} \frac{\alpha_i}{2^n}$$

and the discriminant of k_n over $\mathbb{Q}$ is equal to the product of the discriminants of all the quadratic subfields of k_n; we have:

$$\Delta_{k_n/\mathbb{Q}} = \prod_{i=1}^{2^n-1} A_i$$

Proof. **2.3.1 Part (a)**

Conditions (ii) and (iii) are equivalent according to the classical results on quadratic fields. Also, according to Lemma 1, condition (i) implies condition(ii) according to Lemma 1. Thus it only remains to show that (ii) implies (i):

Let $p_{2^0}, p_{2^1}, \ldots, p_{2^{m-1}}$ be the set of distinct prime numbers congruent to 1 $\pmod 4$ and divide the discriminants A_{2^k} of the field $\mathbb{Q}(\alpha_{2^k})$.

For $0 \leq k \leq n-1$, each rational number A_{2^k} is equal to the product of some of these numbers (each being a high power 1 because A_{2^k} is squarefree).

k_n is a subfield of the field $\mathcal{L}_m = \mathbb{Q}(\pi_{2^0}, \ldots, \pi_{2^{m-1}})$ held by adjoining to $\mathbb{Q}$ the square roots π_{2^k} of the numbers p_{2^k}. Using Proposition 1 and Lemma 1, we deduced that in the ring of integers $\mathcal{O}_n$ of k_n, it admits a normal basis consisting of all conjugates with respect to $\mathbb{Q}$:

$$\epsilon_n = \sum_{\tau \in H} \tau(\prod_{k=0}^{m-1} \frac{1+\pi_{2^k}}{2})$$

,

Here H denotes the subgroup of the Galois group of $\mathcal{L}$ over $\mathbb{Q}$ whose fixed field is k_n.
Note: The equivalence of (i) and (iii) is a special case of the more general result of the theory of Abelian extensions K of $\mathbb{Q}$: The Galois group G of K over $\mathbb{Q}$ being a direct product of cyclic groups $g_1, g_2, \ldots, g_s$, the ring of integers of K has a basis over $\mathbb{Z}$, which is normal if and only if it is the same for rings of number fields with fixed sub-groups:

$$g_1 \times \ldots \times g_{i-1} \times \{id\} \times g_{i+1} \times \ldots \times g_1$$

of G, for $1 \leq i \leq s$.

2.3.2 Demonstrating the uniqueness of the normal basis $\mathcal{O}_n$

Let $B = \{\sigma_i(\epsilon) : \sigma_i \in G_n\}$ and $B' = \{\sigma_i(\epsilon') : \sigma_i \in G_n\}$ be normal bases of $\mathcal{O}_n$.

We have:

$$\epsilon' = \sum_{i=0}^{2^n-1} \lambda_{\sigma_i \cdot \sigma_i(\epsilon)} \text{ with } \lambda_{\sigma_i} \in \mathbb{Z},$$

where

$$\sigma_k(\epsilon') = \sum_{i=0}^{2^n-1} \lambda_{\sigma_i} \cdot \sigma_i(\epsilon) = \sum_{j=0}^{2^n-1} \lambda_{\sigma_k-1 \circ \sigma_j} \cdot \sigma_j(\epsilon).$$

Let M be the transition matrix of the basis B to the basis B'. We have:

$$M = \|\lambda_{\sigma_k-1_\circ \sigma_j}\|.$$

As defined in Chapter 1 §5 the matrix A_n's general term is $a_{i,j}$. Recall that we have:

$$a_{i,j} = \frac{\sigma_i(\alpha_j)}{\alpha_j} = \chi_j(\sigma_i) \text{ and } A_n^{-1} = \frac{1}{2^n} A_n = \frac{1}{2^n}(\chi_i(\sigma_j))$$

While it was verified:

$$A_nMA_n^{-1}=\begin{Vmatrix} r_0 & 0 & \dots & 0\\ 0 & r_1 & \dots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & & r_{2^n-1}\end{Vmatrix}$$

with:

$$r_i=\sum_{k=0}^{2^n-1}\chi_i(\sigma_k)\cdot\lambda_k.$$

(This calculation uses only the properties of orthogonality of the characters of a finite abelian group.)

Therefore:

$$\det M=\prod_{i=0}^{2^n-1}r_i.$$

Let B and B' be two bases of $\mathcal{O}_n$, $\det M$ is equal to ± 1. In the case of the field studied, the numbers $\chi_i(\sigma_n)$ are 1, the numbers r_i are therefore rational integers. They must divide 1, so the are qual to $\pm$ 1.

Relationship (1) may be present in matricies by:

$$A_n\cdot\begin{Vmatrix}\lambda_{\sigma_0}\\ \vdots\\ \lambda_{\sigma_{2^n-1}}\end{Vmatrix}=\begin{Vmatrix} r_0\\ \vdots\\ r_{2^{n-1}}\end{Vmatrix}$$

Where:

$$\begin{Vmatrix}\lambda_0\\ \vdots\\ \lambda_{\sigma_{2^n-1}}\end{Vmatrix}=A_n^{-1}\cdot\begin{Vmatrix} r_0\\ \vdots\\ r_{2^{n-1}}\end{Vmatrix}=\frac{1}{2^n}(a_{ij})\cdot\begin{Vmatrix} r_0\\ \vdots\\ r_{2^n-1}\end{Vmatrix}$$

if:

$$\lambda_{\sigma_j}\frac{\sum_{j=0}^{2^n-1}a_{ij}r_j}{2^n}$$

Relation (2) permits us to write the inequality:

$$|\lambda_{\sigma_i}|\leq\frac{\sum_{j=0}^{2^n-1}|a_{ij}r_j|}{2^n}=\pm 1$$

because $|a_{ij}|=|r_j|=1$

The numbers therefore can take the values: -1, 0, and 1; ϵ' is different from 0, there exists an index k such that λ_{σ_k} is non-zero. Let:

$$\lambda_{\sigma_k}=\delta \text{ with } \delta=\pm 1$$

The equality

$$\lambda_{\sigma_k} = \delta = \sum_{j=0}^{2^{n-1}} \frac{a_{kj} r_j}{2^n} \text{ with } |a_{kj} r_j| = 1$$

implies that we have:

$$a_{kj} r_j = \delta \text{ for } 0 \leq j \leq 2^n - 1$$

or:

$$(a_{kj})^2 r_j = r_j = a_{kj} \delta$$

Relation (2) writes:

$$\lambda_{\sigma_i} = \sum_{j=0}^{2^n-1} \frac{a_{ij} \cdot a_{kj} \cdot \delta}{2^n}$$

Orthogonality relationships of the characters we have deduced give us:

$$\lambda_{\sigma_i} = 0 \text{ for } i \neq k$$

where $\epsilon' = \lambda_{\sigma_k} \cdot \sigma_k(\epsilon) = \delta \sigma_k(\epsilon)$ with $\delta = \pm 1$

The bases B and B' have the same order and the sign near one of their generators. □

Expression of the generator $\epsilon_n = \sum_{\tau \in H} \tau(\prod_{k=0}^{m-1} \frac{1 + \pi_{2^k}}{2})$ of the normal basis of $\mathcal{O}_n$ in terms of the numbers α_i

Note for $j = i + 2^k, 0 < i < 2^k$ and $1 \leq k \leq n-1$:

$$\pi_j = \pi_i \cdot \pi_2^k$$

if $2^k \leq j \leq 2^{k+1}$, then

$$\pi_j = \pi_{2^0}^{\lambda_0} \cdot \pi_{2^1}^{\lambda_1} \cdot \ldots \cdot \pi_{2^{k-1}}^{\lambda_{k-1}} \cdot \pi_{2^k}$$

with $\lambda_i = 0$ or $\lambda_i = 1$

Let $\pi_0 = 1$. We have:

$$\theta_m = \prod_{k=0}^{m-1} \frac{1 + \pi_{2^k}}{2} = \sum_{i=0}^{2^m-1} \frac{\pi^i}{2^m}$$

Let $\pi_j^2 = p_j$. We have:

$$p_j = p_{2^0}^{\lambda_0} \cdot p_{2^1}^{\lambda_1} \cdot \ldots \cdot p_{2^{k-1}}^{\lambda_{k-1}} \cdot p_{2^k}$$

The numbers p_j (for $1 \leq j \leq 2^m - 1$) are squarefree rational integers and is the discriminant of $2^m - 1$ quadratic subfields of $\mathcal{L}_m$. The set of numbers A_i (for $0 \leq ileq 2^n - 1$) is the set of discriminants of the $2^n - 1$ quadratic subfields of k_n and is included in $\{p_j : 0 \leq j \leq 2^m - 1\}$ and for all $i \in \{0, \ldots, 2^n - 1\}$, there is one and only one $\lambda_i \in \{0, \ldots, 2^m - 1\}$ such that $A_i = p_{\lambda_i}$

In particular we have: $A_0 = p_{\lambda_0} = p_0 = 1$.

All invariant numbers $\pi_j (j \in K \subseteq \{0, \ldots, 2^m - 1\})$ by $\mathbb{Q}$- automorphisms of $\mathcal{L}_m$ contained in the subgroup H is the set of π_{λ_i} for $(0 \leq i \leq 2^n - 1)$ and:

$$\epsilon_n = \sum_{\tau \in H} \tau \left[\frac{\sum_{j=0} \pi_j}{2^m} \right] = \frac{1}{2^n} \left[\sum_{i=0}^{2^n - 1} \pi_{\lambda_i} \right]$$

Indeed $|H| = 2^{m-n}$ and if π_j does not belong to the number field of H, all invariant elements H' of$H$ are a subgroup of H with index 2. We therefore have:

$$\sum_{\tau \in H} \tau(H_j) = \sum_{\tau \in H'} \pi_j + \sum_{\tau \in H - H'} (-\pi_j) = 0$$

Now compare the signs of α_i and $\pi_{\lambda_i} (0 \leq i \leq 2^n - 1)$ and show that ϵ_n and $\sum_{i=0}^{2^n-1} \dfrac{\alpha_i}{2^n}$ are conjugates.

The numbers α_{2^k} were defined as any root of $X^2 - A_{2^k}$; so for $0 \leq k \leq n-1$ we have:

$$\alpha_{2^k} = \delta_{2^k} \cdot \pi_{\lambda_{2^k}} \text{ for } \delta_{2^k} = \pm 1$$

When $\delta_{2^k} (0 \leq k \leq n-1)$ numbers are chosen there is one and only one $\mathbb{Q}$-automorphism σ of k_n such that:

$$\sigma(\alpha_{2^k}) = \delta_{2^k} \cdot \alpha_{2^k} = \pi_{\lambda_{2^k}} \ (0 \leq k \leq n-1)$$

Let's check $\sigma(\epsilon_n) = \sum_{i=0}^{2^n-1} \dfrac{\alpha_i}{2^n}$

$d_{i,2^k}$ is the product of prime numbers belonging to $\{p_{2^0}, \ldots, p_{2^{m-1}}\}$ and divides $A_i = p_{\lambda_i}$ and A_{2^k} and $p_{\lambda_{2^k}}$; $d_{i,2^k}$ is the gcd of A_i and A_{2^k} congruent to $1 \pmod 4$ and $0 < i < 2^k$ has:

$$\pi_{\lambda_i} \cdot \pi_{\lambda_{2^k}} = d_{i,2^k} \pi_{\lambda_{i+2^k}}$$
$$\alpha_i \cdot \alpha_{2^k} = A_{i,2^k} \cdot \alpha_{i+2^k}$$

We deduced that if the relationship

$$\sigma(\alpha_i) = \pi_{\lambda_i}$$

is true for $i \leq 2^k - 1$, it is true also for:

$$j = i + 2^k \leq 2^{k+1} - 1$$

As this relation is true for $i \leq 2^1 - 1$, it is true for $0 \leq i \leq 2^n - 1$.

The normal basis of $\mathbb{Z}$-module is therefore formed by $\sum_{i=0}^{2^n-1} \dfrac{\alpha_i}{2^n}$ and its conjugates with respect to $\mathbb{Q}$

Discriminant calculation of k_n over $\mathbb{Q}$

Presumably, $\epsilon_n = \sum_{j=0}^{2^n-1} \dfrac{\alpha_j}{2^n}$ where

$$\sigma_i(\epsilon_n) = \sum_{j=0}^{2^n-1} \frac{\sigma_i(\alpha_j)}{2^n} = \sum_{j=0}^{2^n-1} \frac{a_{ij}\alpha_j}{2^n}$$

$$\Delta_{k_n}/\mathbb{Q} = \Delta(\sigma_i(\epsilon_n)); 0 \leq i \leq 2^n - 1 = \det P^2 \Delta(\alpha_i : 0 \leq i \leq 2^n - 1)$$

, where P is the transition matrix of the basis $\{\sigma_i(\epsilon_n)\}$ of the basis $\{\alpha_i\}$. we have $P = \dfrac{A_n}{2^n}$ where (Ch. 1 §5):

$$\Delta_{k_n/\mathbb{Q}} = \text{ det } (\frac{A_n}{2^n})^2 \cdot (2^n)^{2^n} \cdot \prod_{i=1}^{2^n-1} A_i = \prod_{i=1}^{2^n-1} A_i$$

For $1 \leq i \leq 2^n - 1$, A_i is the discriminant of the field $\mathbb{Q}(\alpha_i)$

Example: $k_3 = \mathbb{Q}(\sqrt{-15}, \sqrt{21}, \sqrt{-39})$, $\alpha_0 = 1$ $\alpha_1 = \sqrt{-35}$ $\alpha_2 = \sqrt{21}$ $\alpha_3 = \dfrac{\alpha_1\alpha_2}{-3} = -\sqrt{-35}$ $\alpha_4 = \sqrt{-39}$ $\alpha_5 = \dfrac{\alpha_1\alpha_4}{-3} = \sqrt{65}$ $\alpha_6 = \dfrac{\alpha_2\alpha_4}{-3} = -\sqrt{-91}$ $\alpha_7 = \dfrac{\alpha_3\alpha_4}{2} = \sqrt{1365}$

The normal basis of $\mathcal{O}_3$ consists of all the conjugates of:

$$\epsilon_3 = \frac{1 + \sqrt{-15} + \sqrt{21} - \sqrt{-35} + \sqrt{-39} + \sqrt{65} - \sqrt{-95} + \sqrt{1356}}{8}$$

The matrix $A_3 = \left(\dfrac{\sigma_i(\alpha_j)}{\alpha_j}\right)$ to calculate the expression of $\sigma_i(\epsilon_3)$ is:

$$A_3 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{Vmatrix}.$$

The discriminant is:

$$\Delta_{k_3/\mathbb{Q}} = 3^4 \cdot 5^4 \cdot 7^4 \cdot 13^4.$$

2.4 Rings of integers and discriminants of $k_n = \mathbb{Q}(\alpha_{2^0}, \dots, \alpha_{2^{n-3}}, \delta\alpha_{2^{n-2}}, \sqrt{-1}\ \alpha_{2^{n-1}})$ with $\delta \in \{\sqrt{2}, \sqrt{-2}\}$ and $(\alpha_2^k)^2 = A_{2^k} \equiv 1 \pmod 4$ for $0 \leq k \leq n-1$

We have for $0 \leq i \leq 2^{n-2} - 1$ (2.1)

$$\beta_i = \alpha_i$$

$$\beta_{i+2^{n-2}} = \delta\frac{\alpha_i\alpha_{2^{n-2}}}{d_{i,2^{n-2}}} = \delta\alpha_{i+2^{n-2}}$$

$$\beta_{i+2^{n-1}} = \sqrt{-1}\frac{\alpha_i\alpha_{2^{n-1}}}{d_{i,2^{n-1}}} = \sqrt{-1}\alpha_{i+2^{n-1}}$$

$$\beta_{i+2^{n-2}+2^{n-1}} = \sqrt{-1}\delta\frac{\alpha_i\alpha_{2^{n-2}}\alpha_{2^{n-1}}}{d_{i,2^{n-2}\cdot d_{i+2^{n-2},2^{n-1}}}} = \sqrt{-1}\delta\alpha_{i+2^{n-2}+2^{n-1}}$$

$\alpha_{2^{n-2}}$ and $\alpha_{2^{n-1}}$ can take the value $+1$.

Theorem 10. *The ring of integers $\mathcal{O}_n$ of k_n is the Z-module of rank 2^n which admits a basis of all conjugates with respect to $\mathbb{Q}(\delta\alpha_{2^{n-2}}, \sqrt{-1}\alpha_{2^{n-1}})$ of the elements:*

$$\sum_{i=0}^{2^{n-2}-1}\frac{\beta_i}{2^{n-2}};\ \sum_{j=2^{n-2}}^{2^{n-1}-1}\frac{\beta_j}{2^{n-2}};\ \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}}\frac{\beta_k}{2^{n-2}};$$

$$\sum_{j=2^{n-2}}^{2^{n-1}-1}\frac{\beta_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1}\frac{\beta_l}{2^{n-1}}$$

The discriminant of k_n over $\mathbb{Q}$ is equal to the product of $2^n - 1$ quadratic subfields of k_n and is:

$$\Delta_{k_n}/\mathbb{Q} = \prod_{i=1}^{2^{n-2}-1}(\beta_i)^2 \cdot \prod_{j=2^{n-2}}^{2^{n-1}-1}(2\beta_j)^2 \cdot \prod_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1}(2\beta_j)^2 \cdot \prod_{l=2^{n-1}+2^{n-2}}^{2^{n-1}}(\beta_l)^2$$

Proof. This theorem is applied to the composition of fields whose discriminants are relatively prime to the field

$$K = [\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})] \cdot \left[\mathbb{Q}(\delta, \sqrt{-1})\right]$$

We obtain a basis over $\mathbb{Z}$ for the ring of integers $\mathcal{O}$ of K by the product of the integral bases of $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$ and $\mathbb{Q}(\delta, \sqrt{-1})$

This is followed by a basic change, a way to get a basis of $\mathcal{O}$ containing 2^n elements of the subfield k_n of K; by Lemma 2, these elements are a basis of $\mathcal{O}_n$.

The degree of $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$ over $\mathbb{Q}$ is 2^n, 2^{n-1}, or 2^{n-2} depending on whether $\alpha_{2^{n-2}}$ or $\alpha_{2^{n-1}}$ belong to $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}})$ and $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}})$.

First Case:

$\alpha_{2^{n-2}} \notin \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}})$ and $\alpha_{2^{n-1}} \notin \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}})$

Let $h_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$. We have $[h_n : \mathbb{Q}] = 2^n$

Let $h_{n+2} = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}}, \delta, \sqrt{-1})$

Note $\mathcal{O}_{n+2}$ as the ring of integers of h_{n+2} and the Galois group G_{n+2} over $\mathbb{Q}$ of h_{n+2}.

We have:

$$G_{n+2} = \{\sigma_0, \sigma_{2^0}\} \times \ldots \times \{\sigma_0, \sigma_{2^{n-1}}\} \times \{\sigma_0, \tau_1\} \times \{\sigma_0, \tau_2\}$$

with σ_0 mapping to the identity of h_{n+2} and for $0 \leq j \leq n-1$:

$$\sigma_{2^j}(\alpha_{2^j}) = -\alpha_{2^j};\ \sigma_{2^j}(\alpha_j) = \alpha_{2^k} \text{ for } k \neq j \text{ and } 0 \leq k \leq n-1$$

$$\sigma_{2^j}(\delta) = \delta;\ \sigma_{2^j}(\sqrt{-1}) = \sqrt{-1};\ \tau_1(\alpha_{2^j}) = \tau_2(\alpha_{2^j}) = \alpha_{2^j}$$

$$\tau_1(\delta) = -\delta;\ \tau_1(\sqrt{-1}) = \sqrt{-1};\ \tau_2(\delta) = \delta;\ \tau_2(\sqrt{-1}) = -\sqrt{-1}$$

According to Theorem 1 after the ring of integers $\mathcal{O}_n$ of $h_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-1}})$ admits the set β_1 of 2^n conjugates with respect to $\mathbb{Q}$ of $\epsilon_n = \sum_{i=0}^{2^n-1} \frac{\alpha_i}{2^n}$.

So: $\beta_1 = \{\delta_j(\epsilon_n) : 0 \leq j \leq 2^n - 1\}$.

Let:

$$(R) = \begin{cases} x_1 = \epsilon_n : x_2 = \epsilon_n + \sigma_{2^{n-2}}(\epsilon_n); x_3 = \epsilon_n + \sigma_{2^{n-1}}(\epsilon_n) \\ x_4 = \epsilon_n + \sigma_{2^{n-2}}(\epsilon_n) + \sigma_{2^{n-1}}(\epsilon_n) + \sigma_{2^{n-2}} \circ \sigma_{2^{n-1}}(\epsilon_n) \end{cases}$$

and $\beta_1' = \{\sigma_i(x_s); 0 \leq i \leq 2^{n-2} - 1; 1 \leq s \leq 4$

The relation (R) shows that β_1' is also a $\mathbb{Z}$-basis of $\mathcal{O}_n$. Note β_2 as a basis of $\mathcal{O}_{n+2}$ obtained by multiplying the elements of β_1' by the elemnts of $\{1, \delta, \sqrt{-1}, \frac{\delta + \sqrt{-1}\delta}{2}\}$

$$B_2 = \{\sigma_i(x_s); \delta\sigma_i(x_s); \sqrt{-1}\sigma_i(x_s); \frac{\delta + \sqrt{-1}\delta}{2}\sigma_i(x_s); 0 \leq i \leq 2^{n-2}; 1 \leq s \leq 4\}$$

Expression of x_s: We have:

$$\alpha_i = \sigma_{2^{n-2}}(\alpha_i) = \sigma_{2^{n-1}}(\alpha_i) = \sigma_{2^{n-1}} \circ \sigma_{2^{n-2}}(\alpha_i),\ 0 \leq i \leq 2^{n-2} - 1$$

$$\alpha_j = -\sigma_{2^{n-2}}(\alpha_j) = \sigma_{2^{n-1}}(\alpha_j) = -\sigma_{2^{n-1}} \circ \sigma_{2^{n-2}}(\alpha_j),\ 2^{n-2} \leq j \leq 2^{n-1} - 1$$

$$\alpha_k = \sigma_{2^{n-2}}(\alpha_k) = -\sigma_{2^{n-1}}(\alpha_k) = -\sigma_{2^{n-1}} \circ \sigma_{2^{n-2}}(\alpha_k),\ 2^{n-1} \leq k \leq 2^{n-1} + 2^{n-2} - 1$$

$$\alpha_l = \sigma_{2^{n-2}}(\alpha_l) = -\sigma_{2^{n-1}}(\alpha_l) = \sigma_{2^{n-1}} \circ \sigma_{2^{n-2}}(\alpha_l),\ 2^{n-1} + 2^{n-2} \leq l \leq 2^n - 1$$

Where:

$$x_2 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-1}} + \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\alpha_k}{2^{n-1}}$$

$$x_3 = \sum_{i=0}^{2^{n-1}-1} \frac{\alpha_i}{2^{n-1}}$$

$$x_4 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-2}} = \sum_{i=0}^{2^{n-2}-1} \frac{\beta_i}{2^{n-2}}$$

The basis $\beta_2$of $\mathcal{O}_{n+2}$ already contains 2^{n-2} elements of k_n (the elements $\sigma_i(x_4)$ for $0 \leq i \leq 2^{n-2} - 1$).

We look for another basis β'_2 of $\mathcal{O}_{n+2}$ containing 2^n elements of k_n: Let:

$$(1) \quad y_2 = 2(\delta x_3) - (\delta x_4)$$

We have:

$$y_2 = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\delta\alpha_j}{2^{n-2}} = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-2}} \in k_n \cap \mathcal{O}_{n+2} = \mathcal{O}_n$$

$$(2) \quad y_3 = 2(\sqrt{-1}x_2) - 2(\sqrt{-1}x_2) - (\sqrt{-1}x_4)$$

We have

$$y_3 = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\sqrt{-1}}{2^{n-2}} = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\beta_k}{2^{n-2}} \in k_n \cap \mathcal{O}_{n+2} = \mathcal{O}_n$$

Let:

$$y_4 = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1} \frac{\beta_l}{2^{n-1}}$$

$$y_4 = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\delta\alpha_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1} \frac{\sqrt{-1}\delta\alpha_l}{2^{n-1}}$$

We have $y_4 \in k_n$ and the equality

$$2x_1 - x_2 = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\alpha_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1} \frac{\alpha_l}{2^{n-1}}$$

we deduced the relationship:

$$(3) \quad y_4 = 2(\delta x_3) - (\delta x_4) - 2(\delta x_1) + (\delta x_2) - 2(\frac{\delta + \sqrt{-1}\delta}{2} x_2)$$
$$+4(\frac{\delta + \sqrt{-1}\delta}{2} x_1) - 2(\frac{\delta + \sqrt{-1}\delta}{2} x_3) + (\frac{\delta + \sqrt{-1}\delta}{2} x_2)$$

where $y_4 \in \mathcal{O}_{n+2}$ and so $y_4 \in \mathcal{O}_{n+2} \cap k_n = \mathcal{O}_n$.

If we replace the basis B_2, the elements $\delta\sigma_i(x_4)$ for $\sigma_i(y_2)$, the elements $\sqrt{-1}\sigma_i(x_4)$ for $\sigma_i(y_3)$, the elements $\frac{\delta + \sqrt{-1}\delta}{2}\sigma_i(x_4)$ for $\sigma_i(y_3)$ and the elements $\frac{\delta + \sqrt{-1}\delta}{2}\sigma_i(x_4)$ for $\sigma_i(y_4)$ a set β'_2 is obtained from elements of $\mathcal{O}_{n+2}$ and is still a $\mathbb{Z}$-basis of $\mathcal{O}_{n+2}$ (this is immediately deduced from relations (1),(2), and (3)). β'_2 contains 2^n elements of $\mathcal{O}_n : \sigma_i(x_4); \sigma_i(y_2); \sigma_i(y_3); \sigma_i(y_4)$ for $0 \leq i \leq 2^{n-2}-1$ thus form a $\mathbb{Z}$-basis B of $\mathcal{O}_n$ after Lemma 2. If $x \in k_n$, $\sigma_i(x)$ for $0 \leq i \leq 2^{n-2}-1$ represent the conjugate of x from the subfield $\mathbb{Q}(\delta\alpha_{2^{n-2}}, \sqrt{-1}\alpha_{2^{n-1}})$ of k_n. B is therefore the basis cited in Theorem 2.

Second case:

$$\alpha_{2^{n-2}} \notin \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_2^{n-3}) \text{ and } \alpha_{2^{n-1}} \in \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}})$$

We can bring $\alpha_{2^{n-1}} = 1$, what is assumed in the rest of the paragraph. Therefore:

$$k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}}, \delta\alpha_{2^{n-2}}, \sqrt{-1})$$

It verifies that the ring of integers $\mathcal{O}_{n+1}$:

$$h_{n+1} = \mathbb{Q}(\alpha_{2^{n-2}}, \ldots, \alpha_{2^{n-2}}, \delta, \sqrt{-1})$$

admits for a $\mathbb{Z}$ basis B_q we can assemble it with conjugates with respect to:

$$k = \mathbb{Q}(\alpha_{2^{n-2}}, \delta, \sqrt{-1})$$

of the elements:

$$z_1 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-2}}; \quad z_2 = \sum_{j=0}^{2^{n-1}-1} \frac{\alpha_j}{2^{n-1}}$$

$$z_3 = \delta z_1; z_4 = \delta z_2; z_5 = \sqrt{-1}z_1; z_6 = \sqrt{-1}z_2; z_7 = \frac{\delta + \sqrt{-1}\delta}{2} z_1 \text{ and } z_8 = \frac{\delta + \sqrt{-1}\delta}{2} z_2$$

It replaces B_1, z_3 and its conjugates with respect to k by $z_3' = 2z_4 - z_3$ and its conjugates with respect to k and z_7 and its conjugates with respect to k by $z_7' = 2z_8 - z_7$ and its conjugates with respect to k.

This provides a new basis B_1' of $\mathcal{O}_{n+1}$ which contains 2^n elements of k_n and their conjugates with respect to k or with respect to the subfield $\mathbb{Q}(\sqrt{2}\alpha_{2^{n-1}}, \sqrt{-1})$ of k_n of the 4 elements:

$$z_1 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-1}} = \sum_{i=0}^{2^{n-2}-1} \frac{\beta_i}{2^{n-2}}$$

$$z_3' = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\delta\alpha_j}{2^{n-2}} = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-2}}$$

$$z_5 = \sum_{i=0}^{2^{n-2}-1} \frac{\sqrt{-1}\alpha_i}{2^{n-2}} = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-} \frac{\beta_k}{2^{n-2}}$$

$$z_7' = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{(\delta\sqrt{-1}\delta)}{2^{n-1}}\alpha_j = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1} \frac{\beta_l}{2^{n-1}}$$

These 2^n elements form an integral basis for $\mathcal{O}_n$, according to Lemma 2

Third case:

$$\alpha_{2^{n-2}} \in \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}})$$
$$\alpha_{2^{n-1}} \notin \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}})$$

It reduces to $\alpha_{2^{n-2}} = 1$ and we study:

$$k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}}, \delta, \sqrt{-1}\alpha_{2^{n-1}})$$

It verifies that the ring of integers L'_{n+1}:

$$h'_{n+1} = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}}, \alpha_{2^{n-1}}, \delta, \sqrt{-1})$$

admits an integral basis based over the set B_2 and its conjugates with respect to

$$k' = \mathbb{Q}(\alpha_{2^{n-1}}.\delta, \sqrt{-1})$$

of the elements

$$t_1 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-2}};\ t_2 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-1}} + \sum_{2^n-1}^{2^{n-1}+2^{n-2}-1} \frac{\alpha_k}{2^{n-1}};\ t_3 = \delta t_1;$$

$$t_4 = \delta t_2;\ t_5 = \sqrt{-1};\ t_6 = \sqrt{-1}t_2;\ t_7 = \frac{\delta + \sqrt{-1}\delta}{2} t_1;\ t_8 = \frac{\delta + \sqrt{-1}\delta}{2} t_2$$

It relplaces B_2,t_5 and its conjugates wiht respect to k' by $t'_5 = 2t_6 - t_5$ and its conjugates with respect to k', t_7 and its conjugates with respect to k' by $t'_7 = t_8 - t_7 t_4 + t_3$and its conjugates with respect to k'.

This provides a new basis B'_2 of L'_{n+1} which contains 2^n elements of k_n, namely the conjugates with respect to k', or with respect to the subfield $\mathbb{Q}(\delta, \sqrt{-1}\alpha_{2^{n-1}})$ of k_n of the four elements:

$$t_1 = \sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-2}} = \sum_{i=0}^{2^{n-2}-1} \frac{\beta_i}{2^{n-2}}$$

$$t_3 = \sum_{i=0}^{2^{n-2}-1} \frac{\delta\alpha_i}{2^{n-2}} = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-2}}$$

$$t'_5 = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\sqrt{-1}\alpha_k}{2^{n-2}} = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\beta_k}{2^{n-2}}$$

$$t'_7 = \sum_{i=0}^{2^{n-2}-1} \frac{\delta\alpha_i}{2^{n-1}} + \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\delta\sqrt{-1}\alpha_k}{2^{n-1}}$$

$$t'_7 = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-1}} + \sum_{2^{n-1}+2^{n-2}}^{2^n-1} \frac{\beta_l}{2^{n-1}}$$

These 2^n elements form an integral basis for the ring of integers $\mathcal{O}_n$
Fourth Case:
$\alpha_{2^{n-2}}$ and $\alpha_{2^{n-1}}$ belong to $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_2^{n-3})$
We can reduce $\alpha_{2^{n-2}} = \alpha_{2^{n-1}} = 1$. Let:

$$k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-3}}, \delta, \sqrt{-1})$$

An integral basis of k_n is formed from the conjugates with respect to $\mathbb{Q}(\delta, \sqrt{-1})$ of the numbers:

$$\sum_{i=0}^{2^{n-2}-1} \frac{\alpha_i}{2^{n-2}} = \sum_{i=0}^{2^{n-2}-1} \frac{\beta_i}{2^{n-2}}$$

$$\sum_{i=0}^{2^{n-2}-2} \frac{\sqrt{-1}\ \alpha_i}{2^{n-2}} = \sum_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} \frac{\beta_k}{2^{n-2}}$$

$$\sum_{i=0}^{2^{n-2}-1} \frac{\delta + \sqrt{-1}}{2} \frac{\alpha_i}{2^{n-2}} = \sum_{j=2^{n-2}}^{2^{n-1}-1} \frac{\beta_j}{2^{n-1}} + \sum_{l=2^{n-1}+2^{n-2}}^{2^n-1} \frac{\beta_l}{2^{n-1}}$$

Calculating the Discriminants
The transition matrix of the basis $N = \{\beta_s : 0 \leq s \leq 2^n - 1\}$ of k_n over $\mathbb{Q}$ of the integral basis B is:

$$P = \begin{Vmatrix} \frac{A_{n-2}}{2^{n-2}} & 0 & 0 & 0 \\ 0 & \frac{A_{n-2}}{2^{n-2}} & 0 & \frac{A_{n-2}}{2^{n-1}} \\ 0 & 0 & \frac{A_{n-2}}{2^{n-2}} & 0 \\ 0 & 0 & 0 & \frac{A_{n-2}}{2^{n-1}} \end{Vmatrix}$$

Δ designates the discriminant over $\mathbb{Q}$ of $\beta_s(0 \leq s \leq 2^n - 1)$, therefore:

$$\Delta_{k_n/\mathbb{Q}} = det\ P^2 \cdot \Delta = (\frac{1}{2^{n-2}})^{2^{n-1}} (\frac{1}{2^{n-1}})^{2^{n-1}} (2n)^{2^n} \prod_{s=1}^{2^n-1} \beta_s$$

for the calculation of det P, use the relation:

$$A_{n-2} \cdot \frac{A_{n-2}}{2^{n-2}} = l_{n-2}$$

where

$$\Delta_{k_n/\mathbb{Q}} = \prod_{i=1}^{2^n-2} -1(\beta_i)^2 \cdot \prod_{j=2^{n-2}}^{2^{n-1}-1} (2\beta_j)^2 \cdot \prod_{k=2^{n-1}}^{2^{n-1}+2^{n-2}-1} (2\beta_k)^2 \cdot \prod_{l=2^{n-1}+2^{n-2}}^{2^n-1} (\beta_l)^2$$

□

Example: $k_3 = \mathbb{Q}(\sqrt{-15}, \sqrt{-6}, \sqrt{7})$

Let: $k_3 = \mathbb{Q}(\alpha_{2^0}, \sqrt{2}, \alpha_{2^1}\sqrt{-1}\cdot\alpha_{2^2}) = \mathbb{Q}(\alpha_{2^0}, \sqrt{2}\,\alpha_{2^1}, i\alpha_{2^2})$ with $\alpha_{2^0} = i\sqrt{15}$, $\alpha_{2^1} = \sqrt{-3}, \alpha_{2^2} = \sqrt{-7}, \beta_0 = 1, \beta_1 = \sqrt{-15}, \beta_2 = \sqrt{-6}, \beta_3 = \sqrt{10}, \beta_4 = -\sqrt{7}, \beta_5 = -\sqrt{-105}, \beta_6 = -\sqrt{-42}, \beta_7 = -\sqrt{70}$

The ring of integers of k_3 admits the basis formed by the numbers:

$$\frac{1+\sqrt{-5}}{2}; \frac{1-i\sqrt{15}}{2}; \frac{i\sqrt{6}+\sqrt{10}}{2}; \frac{i\sqrt{6}-\sqrt{10}}{2}; \frac{-7-i\sqrt{105}}{2}; \frac{-7+i\sqrt{105}}{2};$$

$$\frac{i\sqrt{6}+\sqrt{10}-i\sqrt{42}-\sqrt{70}}{4}; \frac{i\sqrt{6}-\sqrt{10}-i\sqrt{42}+\sqrt{70}}{4}$$

$$\Delta_{k_3/\mathbb{Q}} = 2^{16}\cdot 3^4 \cdot 5^4 \cdot 7^4$$

2.5 The ring of integers and discriminant of $k_n = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}}, \delta\alpha_{2^{n-1}})$ with $\delta \in \{\sqrt{-2}, \sqrt{-1}, \sqrt{2}\}$ and $(\alpha_{2^k})^2 = A_{2^k} \equiv 1 \pmod 4$ for $(0 \le k \le n-1)$

$\alpha_{2^{n-1}}$ may possibly belong to $\mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}})$. The basis N of k_n is given by $\{\beta_s : 0 \le s \le 2^n - 1\}$ with:

$$\beta_i = \alpha_i$$

$$\beta_i = \delta\frac{\alpha_i\alpha_{2^{n-1}}}{d_{i,2^{n-1}}} = \delta\alpha_{i+2^{n-1}}$$

for $0 \le i \le 2^{n-1} - 1$.

Theorem 11. *The ring of integers $\mathcal{O}_n$ of k_n is the free module of rank 2^n admitting a basis of all conjugates with respect to $\mathbb{Q}(\alpha_{2^{n-1}}, \delta)$ of the two elements:*

$$\epsilon_{n-1} = \sum_{i=0}^{2^{n-1}-1}\frac{\beta_i}{2^n} \text{ and } \sum_{j=2^{n-1}}^{2^n-1} = \frac{\beta_j}{2^{n-1}}$$

The discriminant of k_n over $\mathbb{Q}$ is the product of the discriminants of $2^n - 1$ quadratic subfields $\mathbb{Q}(\beta_i)$ (for $1 \le i \le 2^n - 1$) of k_n:

$$\Delta_{k_n/\mathbb{Q}} = \prod_{i=0}^{2^{n-1}-1}(\beta_i)^2 \prod_{j=2^{n-1}}^{2^n-1}(2\beta_j)^2$$

Proof. After paragraph 4, we know an integral basis of $k_{n+1} = \mathbb{Q}(\alpha_{2^0}, \ldots, \alpha_{2^{n-2}}, \delta\alpha_{2^{n-1}}, \delta')$ with $\{\delta, \delta'\} = \{\sqrt{2}, \sqrt{-1}\}$ or $\{\delta, \delta'\} = \{\sqrt{-2}\sqrt{-1}\}$; It is formed with the conjugates with respect to $\mathbb{Q}(\delta\alpha_{2^{n-1}}, \delta')$ of the four elements:

$$\sum_{i=0}^{2^{n-1}-1}\frac{\beta_i}{2^{n-1}}; \sum_{j=2^{n-1}}^{2^n-1}\frac{\beta_j}{2^{n-1}}; \sum_{i=0}^{2^{n-1}-1}\frac{\delta'\alpha_i}{2^{n-1}}; x$$

The expression of x differs depending on whether $\delta \in \{\sqrt{2}, \sqrt{-2}\}$, or $\delta = \sqrt{-1}$. This basis contains 2^n elements of k_n; they are the conjugates relative to $\mathbb{Q}(\delta\alpha_{2^{n-1}}, \delta')$ of the elements:

$$\sum_{i=0}^{2^{n-1}-1} \frac{\beta_i}{2^{n-1}} \text{ and } \sum_{j=2^{n-1}}^{2^{n-1}} \frac{\beta_j}{2^{n-1}}$$

These elements thus form from Lemma 2 a basis B of $\mathcal{O}_n$

Calculation of the discriminant of k_n over $\mathbb{Q}$

The transition matrix of the basis of N of k_n to the basis B is:

$$P = \left\| \begin{matrix} \frac{A_{n-1}}{2^{n-1}} & 0 \\ 0 & \frac{A_{n-1}}{2^{n-1}} \end{matrix} \right\|$$

Where:

$$\Delta_{k_n/\mathbb{Q}} = detP^2 \cdot \Delta(\beta_s; 0 \leq s \leq 2^n - 1) = (\frac{1}{2^{n-1}})2^n(2n)^{2^n} \prod_{s=1}^{2^n-1} (\beta_s^2)$$

Therefore:

$$\Delta_{k_n/\mathbb{Q}} = \prod_{i=1}^{2^{n-1}-1} (\beta_i)^2 \cdot \prod_{j=2^{n-1}}^{2^n-1} (2\beta_j)^2$$

□

Example: $k_3 = \mathbb{Q}(\sqrt{5}, i\sqrt{3}, i\sqrt{2}) = \mathbb{Q}(\alpha_{2^0}, \alpha_{2^1}, \delta)$

$$\alpha_0 = 1 = \beta_0; \alpha_{2^0} = \sqrt{5} = \beta_1; \alpha_{2^1} = i\sqrt{3} = \beta_2; \alpha_3 = i\sqrt{15} = \beta_3;$$
$$\beta_4 = i\sqrt{2}; \beta_5 = i\sqrt{10}; \beta_6 = -\sqrt{6}; \beta_7 = -\sqrt{30}$$

The ring of integers of k_3 admits a basis:

$$\frac{1+\sqrt{5}+i\sqrt{3}+i\sqrt{15}}{4}, \frac{1-\sqrt{5}+i\sqrt{3}-i\sqrt{15}}{4},$$
$$\frac{1+\sqrt{5}-i\sqrt{3}-i\sqrt{15}}{4}, \frac{1-\sqrt{5}-i\sqrt{3}+i\sqrt{15}}{4},$$
$$\frac{i\sqrt{2}+i\sqrt{10}-\sqrt{6}-\sqrt{30}}{4}, \frac{i\sqrt{2}-i\sqrt{10}-\sqrt{6}+\sqrt{30}}{4},$$
$$\frac{i\sqrt{2}+i\sqrt{10}+\sqrt{6}+\sqrt{30}}{4}, \frac{i\sqrt{2}+i\sqrt{10}+\sqrt{6}-\sqrt{30}}{4}$$
$$\Delta_{k_n/\mathbb{Q}} = 2^{12} \cdot 15^4$$

References

[1] Williams, K., *Integers of biquadratic .*, Canadian Mathematical Bulletin **13** (1970).

[2] Lang, S. *Algebra - VII -§1.*

[3] Van Der Waerden. *Modern Algebra - Vol. II §126*

[4] Hilbert. *Théorie des corps de nombres algébriques (thêorèmes 87 and 88)*

[5] Lang, S. *Algebraic Number - IV - §1 and 2*