Bases whole body composed by quadratic extensions of $\mathbb{Q}$

May 2, 2016

Introduction

The bodies studied are extensions of $k_n$of the field of rationals composed of n quadratic extensions of $\mathbb{Q}$, defined by their discriminant $(D_\lambda)_{\lambda\in\Lambda}$

It is proposed to explicitly determine the bases on $\mathbb{Z}$ of the ring of integers of k_n.

For this k_n is associated with the extension field K obtained by adjoining to $\mathbb{Q}$ square roots of the first rational integers and congruent to 1 modulo 4, dividing the discriminants D_λ and the $\sqrt{2}$ numbers or $i = \sqrt{-1}$ if are discriminating congruent 2 or -1 modulo 4.

We know that the product bases on $\mathbb{Z}$ rings of integers of two bodies of numbers with discriminant are relatively prime is a base $\mathbb{Z}$ of the ring of integers of the body consists. This result allows to determine the rings of integers of the body consists. This result allows to determine the K ring of integers and the ring of integers of the subfield k of K.

Include in particular the condition of existence of a normal basis of whole (comprised of conjugated relative to $\mathbb{Q}$ the same integer). We show that this base is unique when it exists (the sign near one of its generators) and given expression. It is whown that in all cases the discriminant of k_n of K is equal to the product of discriminating all in quadratic fields k_n. These results, generalize those obtained by Kenneth S. Williams in the case n=2 ([1]).

Chapter 1: Construction and properties of the field k_n

Paragraph 1: How to define the field k_n

n quadratic fields which generate k_n is assumed given.

We take for generator of each one of the two numbers whose square is rational integer without square factors (squarefree).

Note $\alpha_{2^k}(0 \leq k \leq n-1)$ generators and $A_{2^k}(0 \leq k \leq n-1)$ their squares

(The indicies 2^k will be justified by the introduction of numbers α_i and A_i definied for indices i not power of 2)

No one expresses numbers α_{2^k} is superfluous by the conditions:

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

or the equivalent relationships

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

It follows the conditions (1') that the field $k_n = \mathbb{Q}(\alpha_{2^0}, \dots, \alpha_2^{n-1})$ is a Galoi extension of $\mathbb{Q}$ of degree 2^n whose Galois group G_n id isomorphic to the Cartesian product of n Galois groups of $\mathbb{Q}$ of $\mathbb{Q}(\alpha_{2^k})$(for $0 \leq k \leq n-1$)([2]). G_n is the direct product of n subgroups of order 2. All its components except the neutral element Id. are of order 2 and 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 $\mathbb{Q}$ fixed body of $g_0 \times \dots \times id \times \dots \times g_{n-1}$ or id subgroups replace g_k for $0 \leq k \leq n-1$ ([2]).

Paragraph 2: Choosing a base k on $\mathbb{Q}$

J for non power of 2 and j we define little by little the numbers A_j from the numbers A_{2^k} $(0 \leq k \leq n-1)$ posing for $j = i + 2^k$, $0 < i < 2^k$, $1 \leq k \leq n-1$:

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

or is one of two GCD of A_i and A_{2^k}. It will be specified in Chapter 2 the choice of the sign of $d_{i,2^k}$. It then defines the numbers has relations for j $= i + 2^k$, $0 < i < 2^k$, $1 \leq k \leq n-1$:

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

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

A_j $(0 \leq j \leq 2^n - 1)$ numbers are rational integers without edges(square?) factors and is one of the roots of the polynomial $X^2 - A_j$.

Lemma 1: $N = \{\alpha_j; 0 \leq j \leq 2^n - 1\}$ is a base for k on $\mathbb{Q}$

k_n is indeed the body consists of $\mathbb{Q}(\alpha_{2^k}$ body shall check ballast conditions (1). It therefore has a base product bases $\{1, \alpha 2^k\}$, $(0 \leq k \leq n-1)$. The elements of this base are of the form $\lambda_j \alpha_j$, $(0 \leq j \leq 2^n - 1)$ with $\lambda_j \in \mathbb{Z} - \{0\}$; $\{\alpha_j; 0 \leq j \leq 2^n - 1\}$ together is also a k $\mathbb{Q}$ basic.

Paragraph 3: Galois group G of k_n on Q

$\mathbb{Q}$-automorphism σ of k_n is defined by the given $\sigma(\alpha_{2^k})$ for $0 \leq k \leq n-1$. (The values of σ for other elements of the basis of N of k_n on $\mathbb{Q}$ are deduced by relations (3)).

The numbers $(\alpha_{2^k}^2)$ belonging to $\mathbb{Z}$, are invariant under σ; therefore we have for $\sigma \in G_n$ and $0 \leq k \leq n-1$:

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

Let σ_0 the same application k_n.

σ_{2^p} note the elements of G_n defined by $0 \leq p \leq n-1$ on

$$\sigma_{2^p}(\alpha 2^p) = -\alpha_{2^p}$$

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

Let g_p subgroup $\{\sigma_0, \sigma_{2^p}\}$ of G_n.

G_n is equal to the direct product of $g_0 \times g_1 \times \ldots \times g_{n-1}$ its subgroups $g_p (0 \leq p \leq n-1)$.

This results from the isomorphism between G_n and the Cartesian product $h_0 \times h_1 \times \ldots h_{n-1}$ 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:

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

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

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

G_n is equal to all $sigma_i$ for $0 \leq i \leq 2^n - 1$ and we have:

$$\sigma_i(\alpha_j) = \pm \alpha_j (car (\alpha_j)^2 \in \mathbb{Z})$$