Quadratic Extensions of Cyclic Quintic Number Fields

Schehrazad SELMANE *

Abstract— **For each cyclic quintic field $\mathcal{F}$ of discriminant $d_{\mathcal{F}}$ smaller than $2 \cdot 10^7$, we established lists of quadratic relative extensions of absolute discriminant less than $3 \cdot 2^{15} \cdot d_F^2$ in absolute value. For each one of the found fields, the field discriminant, the quintic field discriminant, a polynomial defining the relative quadratic extension, the corresponding relative discriminant, the corresponding polynomial over $\mathcal{Q}$, and the Galois group of the Galois closure are given. Among the found fields, there exists for each fixed cyclic field $\mathcal{F}$, 6 totally imaginary cyclic number fields and between 2 and 4 totally real cyclic number fields.**

Keywords: Cyclic Extension, Discriminant, Number Field, Quintic Field, Relative Quadratic Extension.

1 Introduction

The discriminant $d_{\mathcal{K}}$ of a number field $\mathcal{K}$ of degree n and of signature (r, s) depends upon several elements of $\mathcal{K}$ such that :

- r the number of real places and s the number of complex places.
- Its sign is $(-1)^s$.
- To equal degree, the discriminants have tendencies to grow with the number of real places.
- For every prime number p, the valuation of p in d_K can only take a finite number of values.
- It verifies the Stickelberger's congruence :

$$d_K \equiv 0 \ or \ 1 \ mod \ 4.$$

- One can give lower bounds for $|d_K|$ depending only on r and s [?].
- Finally, it is well known that the set of isomorphism classes of number fields of a given discriminant is finite [?]. It is therefore natural to try to sort the number fields by their discriminants.

Not to mention that the construction of tables of number fields is useful in two ways :

- Test the algorithms available for such constructions.
- Give researchers a vast amount data that they can examine and on which they can make conjectures.

The enumeration of all number fields of degree 10 and of absolute discriminant less than $3 \cdot 2^{15} \cdot d_F^2$ containing cyclic quintic fields of discriminant smaller than $2 \cdot 10^7$ is the purpose of this paper. For each one of the found fields, the field discriminant, the quintic field discriminant, a polynomial defining the relative quadratic extension, the corresponding relative discriminant, the corresponding polynomial over $\mathcal{Q}$, and the Galois group of the Galois closure are given.

To establish these lists, we used techniques of the geometry of numbers, we followed without major modification, the method of [?]; section 2 contains the description of the main steps. The description of the results is done in the third section, where we provide tables illustrating some of the obtained results. The existence of totally imaginary cyclic number fields and totally real cyclic number fields of degree ten have been examined in more details.

2 The method

If $\mathcal{L}$ is a number field of degree $[\mathcal{L} : \mathcal{Q}] = n$, we denote by $\vartheta_{\mathcal{L}}$ its ring of integers, by $\{\omega_1, ..., \omega_n\}$ an integral basis of $\vartheta_{\mathcal{L}}$, and by

$$d_{\mathcal{L}} = \det(Tr_{\mathcal{L}/\mathcal{Q}}(\omega_i \omega_j))$$

its discriminant. Let $J(\mathcal{L})$ be the set of distinct $\mathcal{Q}$ isomorphisms of $\mathcal{L}$ into $\mathcal{C}$, for $\beta \in \mathcal{L}$ we denote the corresponding conjugates by $\beta^{(1)}, ..., \beta^{(n)}$ and we set

$$T_2(\beta) = \sum_{i=1}^{n} |\beta^{(i)}|^2.$$

To establish the lists of all number fields of degree 10 over $\mathcal{Q}$ and of field discriminant smaller than a fixed bound in absolute value containing a cyclic quintic subfield, we have followed without major modification, the method of explicit construction of quadratic relative extensions as described in [?]. In the following, we are going to briefly describe the main stages that led us to establish these lists.

Each relative quadratic extension of a quintic field will be given by second degree polynomial with coefficients in the subfield. To construct such polynomials we make call to the geometry of number methods which allow us to find bounds for the coefficients of the searched polynomials. The basic tool allowing us to construct explicitly all

*University of Sciences and Technology Houari Boumediene. Faculty of Mathematics. Bab-Ezzouar, 16111 Algiers, Algeria. schehrazad.selmane@gmail.com

relative polynomials is the generalization of the Hunter-Pohst theorem given by J. Martinet [?].

Theorem 1 *Let $\mathcal{K}$ be a number field of degree 10, of signature (r,s) and of discriminant $d_{\mathcal{K}}$ such that $|d_{\mathcal{K}}| \leq M$, containing a cyclic quintic field $\mathcal{F}$. There exists an integer $\theta \in \mathcal{K}, \theta \notin \mathcal{F}$ such that*

$\mathcal{K} = \mathcal{F}(\theta)$

$Min(\theta, \mathcal{F}) = x^2 + ax + b \in \vartheta_{\mathcal{F}}[x]$

$$\sum_{i=1}^{10} |\theta^{(i)}|^2 \leq \frac{1}{2} \sum_{\sigma \in J(\mathcal{F})} | \sum_{\tau \in J_\sigma(\mathcal{K})} \tau(\theta)|^2 + \left(\frac{|d_{\mathcal{K}}|}{4|d_{\mathcal{F}}|}\right)^{\frac{1}{5}} \quad (1)$$

where $J_\sigma(\mathcal{K}) = \{\tau \in J(\mathcal{K}) : \tau_{/\mathcal{F}} = \sigma\}$.
This inequality is also valid for all elements of $\mathcal{K}$ of the form $\theta + \gamma$, where γ is any integer of $\mathcal{F}$.

Let then

$$P(x) = x^2 + ax + b \in \vartheta_{\mathcal{F}}[x]$$

be the minimal polynomial of the integer θ over $\mathcal{F}$, whose existence is affirmed in the previous theorem. We denote by $P_\sigma(x)$, $\sigma \in J(\mathcal{F})$, the polynomial

$$P_\sigma(x) = x^2 + \sigma(a)x + \sigma(b).$$

To compute all polynomials $P(x)$ having a root θ subject to inequality (??), we will work in the field $\mathcal{F}$. We assume that the discriminant d_F and an integral basis $W = \{w_1 = 1, w_2, ..., w_5\}$ of $\mathcal{F}$ are known. All used quintic fields $\mathcal{F}$ were taken from [?]. In the list below, the polynomials defining the cyclic quintic fields of discriminant smaller than $2 \cdot 10^7$ are given. We notice that the discriminant of the cyclic quintic fields is of the form p^{4i} $(1 \leq i \leq 2)$.

Discriminant	Polynomial
$14641 = 11^4$	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$
$390625 = 5^8$	$x^5 - 10x^3 - 5x^2 + 10x - 1$
$923521 = 31^4$	$x^5 - x^4 - 12x^3 + 21x^2 + x - 5$
$2825721 = 41^4$	$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$
$13845841 = 61^4$	$x^5 - x^4 - 24x^3 + 17x^2 + 41x + 13$

In order to find all number fields of degree 10 and of discriminant $d_{\mathcal{K}}$ such that $|d_{\mathcal{K}}| \leq M$, containing a cyclic quintic field, we choose $M = 3 \cdot 2^{15} \cdot d_{\mathcal{F}}^2$ and we set $B = \left(\frac{M}{4d_{\mathcal{F}}}\right)^{\frac{1}{5}}$.
Let us show how to determine the coefficients a and b of the relative polynomial P.

According to the second part of theorem 1, the coefficient a of P can be chosen in $\vartheta_{\mathcal{F}} \, mod \, 2\, \vartheta_{\mathcal{F}}$, therefore only 2^5 values can be considered for a :

$$a = \sum_{i=1}^{5} a_i w_i \quad with\, a_i \in \{0,1\}\, for\, i = 1, ..., 5.$$

We determine the possible values of b from the second relative symmetric function, $s_2 = a^2 - 2b$, via the inequality

$$\sum_{i=1}^{5} |s_2^{(i)}|^2 \leq T_2(\theta)^2.$$

Notice that for a fixed value of a, the running time for the computation of the possible b's strongly depends on the size of the real constant bound κ on $T_2(\theta)$ where $\kappa = \frac{1}{2}\sum_{i=1}^{5} |a^{(i)}|^2 + B$. The constant κ depends only on the value of a. Let us show that a can be chosen such that κ is minimum.

Indeed, as inequality (??) remains valid if we change θ by $\theta + \gamma$ for an arbitrary $\gamma \in \vartheta_F$, and as $\theta + \gamma$ is also a generator of the extension K/F, then if we represent c $\big(c = -Tr_{K/L}(\theta + \gamma) = a - 2\gamma\big)$ by means of the basis $\mathcal{W}$ of $\mathcal{F}$ as

$$c = \sum_{i=1}^{5} c_i w_i,$$

$T_2(c)$ becomes a positive definite quadratic form

$$q(c) = cAc^t$$

in the coefficients $c_1, ..., c_5$ $(c = (c_1, ..., c_5))$, and there exists at least one choice of γ which makes $T_2(c)$ minimal. The desired choice is obtained as follows :
we start by computing the coefficient matrix $A = (m_{ij})$ of the quadratic form q. Clearly,

$$m_{ij} = Tr(w_i w_j) \in \mathcal{Z}.$$

Then we decompose the matrix A into sum of squares by cholesky's method

$$q(c) = \sum_{i=1}^{5} m_{ii}\left(c_i + \sum_{j=i+1}^{5} m_{ij}c_j\right)^2$$

and we make $c_1, ..., c_5$ run through the integer values for which $q(c) \leq T_2(a)$ and which satisfy the relationship $c \equiv a \pmod{2\vartheta_{\mathcal{F}}}$.

We shall affect to a the value of c for which $q(c)$ is minimal and we shall set

$$C = \frac{1}{2}\sum_{i=1}^{5} |a^{(i)}|^2 + B$$

Remark. The choice of a is independant of the signature of $\mathcal{K}$ and is also independant of the chosen bound, it depends only on the field $\mathcal{F}$. Therefore, we have established the list of the 32 possible values of a for a fixed quintic field. This improves considerably the execution time of our programs.

Once a convenient value of a is determined , then we compute the set of suitable values of $b = \sum_{i=1}^{5} b_i w_i$ using this inequality

$$\sum_{i=1}^{5} |s_2^{(i)}|^2 \leq C^2$$

which comes from the inequality (??) and the inequality

$$\sum_{i=1}^{5} |s_2^{(i)}| \leq C.$$

If we represent s_2 by the means of the basis $\mathcal{W}$, $s_2 = \sum_{i=1}^{5} y_i w_i$, we notice that

$$\sum_{i=1}^{5} |s_2^{(i)}|^2$$

is just the quadratic form $q(y)$ in the coefficients $y_1, ..., y_5$ $(y = (y_1, ..., y_5))$. As we have already computed the coefficients matrix A and decomposed it into a sum of squares, we compute all $y \in \mathcal{Z}^5$ subject to $q(y) \leq C^2$ and $y_i \equiv z_i \pmod 2$ for $(1 \leq i \leq 5)$, where $a^2 = \sum_{i=1}^{5} z_i w_i$. Then we obtain all the possible choices for the coefficient b.

2.1 The main simplifications

We find ourselves in the presence of a long list of polynomials P. The main simplifications used to reduce, as much as possible, the number of polynomials to be considered to construct the complete lists of the desired fields are described below.

2.1.1 Step 1

- For each of the constructed polynomials, we started by determining whether it can define a field with the desired signature. This question was solved by simply examining the sign of the polynomial discriminant $\Delta = a^2 - 4b$ of each conjugate of P.

- Then, we proceeded with the elimination of polynomials having too large values of $T_2(\theta)$ by checking whether the inequality

$$\sum_{i=1}^{5} |\Delta^{(i)}| \leq 2B \qquad (2)$$

is fulfilled. Indeed, since

$$T_2(\theta) = \sum_{i=1}^{10} |\theta^{(i)}|^2 = \frac{1}{2}\left(\sum_{i=1}^{5} |a^{(i)}|^2 + \sum_{i=1}^{5} |\Delta^{(i)}|\right),$$

then the inequality

$$\sum_{i=1}^{10} |\theta^{(i)}|^2 \leq \frac{1}{2}\sum_{i=1}^{5} |a^{(i)}|^2 + B$$

is equivalent to inequality (??).

- Finally, we checked the irreducibility of the polynomial P for the signature $(10, 0)$ by computing the roots of the five conjugate polynomials of P. For the signature $(0, 5)$ the polynomial is irreducible.

2.1.2 Step 2

- For the polynomials that survived to the previous tests, we used a theorem on ramification in Kummer extensions to compute the relative discriminant δ. Only polynomials for which $\mathcal{N}(\delta) \leq M\ d_{\mathcal{F}}^{-2}$ were kept. This allowed us to obtain the value of $d_{\mathcal{K}}$ directly

$$d_{\mathcal{K}} = (-1)^s\ d_{\mathcal{F}}^2\ \mathcal{N}(\delta).$$

where $\mathcal{N}$ is the the absolute norme in the extension $\mathcal{F}/\mathcal{Q}$

- As we got several polynomials for a given discriminant, we used the function OrderIsSubfield in [?] to decide whether or not such polynomials define the same field up to isomorphism.

- Then, we computed the polynomial

$$f(x) = \prod_{\sigma \in J(\mathcal{F})} P_\sigma(x) = \sum_{i=0}^{10} t_i x^{10-i} \qquad (t_0 = 1)$$

and the Galois group of the Galois closure for each field in the lists using KANT [?].

3 Description of Results.

In this section, we give a brief discussion of some information provided by these computations and a table illustrating the obtained results.

For each fixed quintic subfield, the number nb_1 of obtained fields, the smallest discriminant, the number of discriminants for which there are exactly k non-isomorphic fields having same discriminants are presented in Table 1.

In Table 2, we present some data on the found cyclic fields. Among the 4 found cyclic extensions of signature $(10, 0)$, the first one is the composite field $\mathcal{F} \cdot \mathcal{Q}(\sqrt{5})$ and the last one is the composite field $\mathcal{F} \cdot \mathcal{Q}(\sqrt{2})$. The two other fields contain the quadratic field $\mathcal{Q}(\sqrt{3p})$ and $\mathcal{Q}(\sqrt{p})$ respectively.

.

Table 2 : Cyclic Extensions

$d_{\mathcal{K}}$	$d_{\mathcal{F}}$	$(t_0, ..., t_{10})$	$(a_1, ..., a_5)$	$(b_1, ..., b_5)$
Totally imaginary cyclic number fields				
-11^9	11^4	$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	$(0, 1, 0, 0, 0)$	$(1, 0, 0, 0, 0)$
$-3^5 11^8$	11^4	$(1, -3, 12, 1, 20, -7, 16, -2, 5, -1, 1)$	$(-1, 0, 3, 0, -1)$	$(1, -1, -2, 1, 1)$
$-2^{10} 11^8$	11^4	$(1, 0, 15, 0, 35, 0, 28, 0, 9, 0, 1)$	$(0, 0, 0, 0, 0)$	$(1, -1, -2, 1, 1)$
$-7^5 11^8$	11^4	$(1, -1, 14, -7, 85, -29, 218, -8, 216, -48, 32)$	$(0, 3, 0, -1, 0)$	$(2, -4, 6, 2, -2)$
$-2^{15} 11^8$	11^4	$(1, 0, 18, 0, 112, 0, 280, 0, 240, 0, 32)$	$(0, 0, 0, 0, 0)$	$(8, 0, -8, 0, 2)$
$-5^5 11^9$	11^4	$(1, -1, 12, -12, 56, -56, 133, -133, 188, -188, 199)$	$(0, 3, 0, -1, 0)$	$(4, 2, -3, -1, 1)$
$-3^5 5^{16}$	5^8	$(1, 0, 10, -10, 90, -49, 125, 70, 95, 10, 1)$	$(-2, 4, 5, -2, -4)$	$(6, 6, 1, -1, -1)$
$-2^{10} 5^{16}$	5^8	$(1, 0, 30, 0, 245, 0, 400, 0, 240, 0, 49)$	$(0, 0, 0, 0, 0)$	$(9, -3, -12, 4, 11)$
$-3^5 5^{17}$	5^8	$(1, 0, 10, 5, 0, 41, -25, -170, 65, 25, 199)$	$(-1, -3, 1, 0, -1)$	$(4, -1, -3, 1, 3)$
$-2^{10} 5^{17}$	5^8	$(1, 0, 20, 0, 100, 0, 125, 0, 50, 0, 5)$	$(0, 0, 0, 0, 0)$	$(1, 4, 3, -1, -2)$
$-5^{16} 7^5$	5^8	$(1, 0, 30, -25, 410, -189, 1400, 600, 1480, 160, 32)$	$(-1, -3, 1, 0, -1)$	$(8, -2, 12, -4, -12)$
$-2^{15} 5^{16}$	5^8	$(1, 0, 40, 0, 480, 0, 1800, 0, 1440, 0, 32)$	$(0, 0, 0, 0, 0)$	$(8, -2, 12, -4, -12)$
-31^9	31^4	$(1, 1, 2, -16, -9, -11, 43, 6, 63, 20, 25)$	$(-3, -6, 6, 1, -3)$	$(1, 2, 3, 0, -2)$
$-3^5 31^8$	31^4	$(1, -4, 22, 2, 72, -7, 149, 28, 119, -40, 25)$	$(-4, -6, 6, 1, -3)$	$(15, 27, -18, -4, 8)$
$-2^{10} 31^8$	31^4	$(1, 0, 28, 0, 140, 0, 257, 0, 174, 0, 25)$	$(0, 0, 0, 0, 0)$	$(-3, -6, 19, 2, -11)$
$-7^5 31^8$	31^4	$(1, 4, 50, 7, 416, -1, 1584, -104, 2344, 640, 800)$	$(-1, 2, 3, 0, -2)$	$(-6, -12, 38, 4, -22)$
$-2^{15} 31^8$	31^4	$(1, 0, 56, 0, 560, 0, 2056, 0, 2784, 0, 800)$	$(0, 0, 0, 0, 0)$	$(2, -4, 2, 0, 0)$
$-5^5 31^9$	31^4	$(1, 1, 33, -47, 239, -817, 1283, -3559, 4496, -3700, 6845)$	$(-3, -6, 6, 1, -3)$	$(-3, -5, 21, 2, -12)$
$-3^5 41^8$	41^4	$(1, -4, 29, -166, 650, -1633, 3184, -4776, 4722, -2655, 657)$	$(-3, 0, 3, 0, -2)$	$(2, 6, 8, -1, -5)$
$-2^{10} 41^8$	41^4	$(1, 0, 33, 0, 288, 0, 679, 0, 531, 0, 81)$	$(0, 0, 0, 0, 0)$	$(14, 5, -8, -2, 6)$
$-3^5 41^9$	41^4	$(1, 1, 23, 28, 173, -158, 964, -909, 5115, -2196, 657)$	$(-2, 0, 3, 0, -2)$	$(24, 6, -10, -1, 6)$
$-7^5 41^8$	41^4	$(1, 4, 69, 417, 2093, 6684, 17760, 33265, 38572, 25518, 7681)$	$(1, -1, 0, 0, 0)$	$(2, 3, 2, 0, 0)$
$-2^{15} 41^8$	41^4	$(1, 0, 66, 0, 1152, 0, 5432, 0, 8496, 0, 2592)$	$(0, 0, 0, 0, 0)$	$(6, 12, 10, -2, -6)$
$-2^{10} 41^9$	41^4	$(1, 0, 41, 0, 492, 0, 2255, 0, 3403, 0, 369)$	$(0, 0, 0, 0, 0)$	$(6, 9, 4, -2, -2)$
Totally Real cyclic number fields				
$3^5 11^9$	11^4	$(1, -1, -10, 10, 34, -34, -43, 43, 12, -12, 1)$	$(0, 3, 0, -1, 0)$	$(-2, -2, 3, 1, -1)$
$5^5 11^8$	11^4	$(1, 1, -13, -8, 46, 11, -52, -7, 18, 3, -1)$	$(2, 0, -1, 0, 0)$	$(-4, 0, 4, 0, -1)$
$2^{10} 11^9$	11^4	$(1, 0, -11, 0, 44, 0, -77, 0, 55, 0, -11)$	$(0, 0, 0, 0, 0)$	$(0, 0, -4, 0, 1)$
$2^{15} 11^8$	11^4	$(1, 0, -18, 0, 112, 0, -280, 0, 240, 0, -32)$	$(0, 0, 0, 0, 0)$	$(-4, -6, 0, 2, 0)$
5^{17}	5^8	$(1, 0, -10, 0, 35, -1, -50, 5, 25, -5, -1)$	$(0, 0, 3, -1, -3)$	$(0, -1, 0, 0, 0)$
$2^{15} 5^{16}$	5^8	$(1, 0, -40, 0, 480, 0, -1800, 0, 1440, 0, -32)$	$(0, 0, 0, 0, 0)$	$(-18, 10, 22, -8, -18)$
$5^5 31^8$	31^4	$(1, -4, -34, 20, 224, 7, -405, 32, 229, -40, -25)$	$(1, 0, 1, 0, -1)$	$(-5, -5, 12, 1, -8)$
$3^5 31^9$	31^4	$(1, -1, -29, -15, 239, 321, -515, -1029, 94, 910, 397)$	$(-2, 2, 3, 0, -2)$	$(-9, 11, 1, -1, -1)$
$2^{10} 31^9$	31^4	$(1, 0, -31, 0, 248, 0, -713, 0, 651, 0, -31)$	$(0, 0, 0, 0, 0)$	$(-3, -6, 2, 1, -1)$
$2^{15} 31^8$	31^4	$(1, 0, -56, 0, 560, 0, -2056, 0, 2784, 0, -800)$	$(0, 0, 0, 0, 0)$	$(-10, -10, 24, 2, -16)$
41^9	41^4	$(1, 1, -18, -13, 91, 47, -143, -7, 72, -23, 1)$	$(-4, -1, 2, 0, -1)$	$(2, -1, -3, 0, 2)$
$5^5 41^8$	41^4	$(1, 4, -51, -336, -364, 1485, 4182, 3526, 574, -369, -41)$	$(1, -1, 0, 0, 0)$	$(-1, -3, -1, 0, 0)$,

Table 1: Results

$d_{\mathcal{F}}$	14641		390625	
(r, s)	$(10, 0)$	$(0, 5)$	$(10, 0)$	$(0, 5)$
nb_1	122	132	203	213
Smallest found discriminant $d_{\mathcal{K}}$				
d_K	$3^5 11^9$	-11^9	5^{17}	$-3^5 5^{16}$
k	Number of k non-isomorphic field			
2	–	1	6	4
d_F	923521		2825761	
(r, s)	$(10, 0)$	$(0, 5)$	$(10, 0)$	$(0, 5)$
nb_1	105	246	380	396
Smallest found discriminant $d_{\mathcal{K}}$				
d_K	$31^8 433$	-31^9	41^9	$-3^5 41^8$
k	Number of k non-isomorphic field			
2	2	13	18	17
3	–	1	1	1
4	–	–	2	2

On the six found cyclic fields of signature $(0, 5)$, four are composite fields $\mathcal{F} \cdot \mathcal{Q}(\sqrt{d})$ where $d = -1, -2, -3, -7$. The smallest discriminant $d_{\mathcal{K}} = -p^9$ $(p = 11, 31)$ corresponds to the subfield of degree 10 of the $p^i - th$ cyclotomic field. Finally, the last cyclic field contains the quadratic field $\mathcal{Q}(\sqrt{5p})$.

References

[1] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger: KANT V4, in J. Symbolic Comp. 24 (1997), 267-283.

[2] F. Diaz y Diaz, M. Pohst and A. Schwartz, A table of quintic number fields of signature (5,0), Math. Comp.56 (1991), 801-808.

[3] J. Martinet, Methodes geometriques dans la recherche des petits discriminants, Sem. de Theorie des nombres de paris 1983/1984, Birkhauser Verlag, Bassel (1985) 147-179.

[4] S. Selmane, Quadratic extensions of totally real quintic fields, Math. Comp. 70, 234 (2001), 837-843.

[5] S. Selmane, Enumeration of a Class of Cyclic Number Fields of Degree 10, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2011, WCE 2011, 6-8 July, 2011, London, U.K., pp 114-116.

[6] S. Selmane, Odlyzko-Poitou-Serre Lower Bounds for Discriminant for some Number Fields, To appear in the Maghreb Mathematical Review.