Proceedings of the World Congress on Engineering 2011 Vol I
WCE 2011, July 6 - 8, 2011, London, U.K.

Enumeration of a Class of Cyclic Number Fields of Degree 10

Schehrazad SELMANE *

Abstract—**For each cyclic quintic field F of discriminant d_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 cyclic field F, we proved the existence of 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_K of a number field K of degree n and of signature (r, s) depends upon several elements of K such that :

- The numbers r of real places and s 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 :

$$d_K \equiv 0 \text{ or } 1 \text{ mod } 4. \quad (1)$$

- 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 (Hermite). It is therefore natural to try to sort the number fields by their discriminants.

In this paper, we enumerate 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 $2 \cdot 10^7$. 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 Q, and the Galois group of the Galois closure are given. For each fixed field F, we proved the existence of 6 totally imaginary cyclic number fields and between 2 and 4 totally real cyclic number fields.

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

2 The method

If L is a number field of degree $[L : Q] = n$, we denote by ϑ_L its ring of integers and by d_L its discriminant. Let $J(L)$ be the set of distinct Q isomorphisms of L into C, for $\beta \in L$ 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 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 [4]. In the following, we are going to briefly describe the main stages that led us to establish these lists.

The basic tool that allowed us to construct explicitly all relative quadratic extensions of a quintic field with discriminant less than a given bound is the following theorem due to J. Martinet [3].

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

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

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

Let then

$$P(x) = x^2 + ax + b \in \vartheta_F[x]$$

be the minimal polynomial of θ over F. We denote by $P_\sigma(x)$, $\sigma \in J(F)$, 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 (2), we will work in the field F. We assume that the discriminant d_F and an integral basis

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$W = \{w_1 = 1, w_2, ..., w_5\}$ of F are known. All used quintic fields F were taken from [2]. 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_K such that $|d_K| \leq M$, containing a cyclic quintic field, we choose $M = 3 \cdot 2^{15} \cdot d_F^2$ and set $B = \left(\frac{M}{4d_F}\right)^{\frac{1}{5}}$. Let us show how to determine the coefficients a and b of the relative polynomial P.

2.1 Choice of a

According to theorem 1, the coefficient a of P can be chosen in $\vartheta_F \, mod \, 2\, \vartheta_F$, therefore only 2^5 values must be considered for a :

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

Moreover, according to [4], each one of the 32 possible values of a can be chosen so that $C = \frac{1}{2}\sum_{i=1}^{5} |a^{(i)}|^2 + B$ is minimum.

2.2 Choice of b

Once a convenient value of a is determined, we compute the set of suitable values of $b = \sum_{i=1}^{5} b_i w_i$ from the second relative symmetric function

$$s_2 = \theta^2 + \theta'^2 = a^2 - 2b$$

where θ' denotes the other root of P. The values of s_2 are computed from the inequality

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

which is deduced from inequality (2) and this inequality $\sum_{i=1}^{5} |s_2^{(i)}| \leq C$.

2.3 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.

2.3.1 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

$$\sum_{i=1}^{5} |\Delta^{(i)}| \leq 2B \qquad (3)$$

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 (3).

- Finally, we checked the irreducibility of the polynomial P for the signature $(10, 0)$.

2.3.2 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 $N(\delta) \leq M\, d_F^{-2}$ were kept. This allowed us to obtain the value of d_K directly

$$d_K = (-1)^s\, d_F^2\, N(\delta).$$

- As we got several polynomials for a given discriminant, we used the function OrderIsSubfield in [1] to decide whether or not such polynomials define the same field up to isomorphism.

- Then, we computed the polynomial

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

and the Galois group of the Galois closure for each field in the lists using KANT [1].

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table 1: Results

d_F	14641		390625	
(r,s)	$(10,0)$	$(0,5)$	$(10,0)$	$(0,5)$
nb_1	122	132	203	213
Smallest found discriminant d_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_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

Table 2: Cyclic Extensions

r	d_F	d_K	$t_1, ..., t_{10}$
10	11^4	$3^5 11^9$	$-1, -10, 10, 34, -34, -43, 43, 12, -12, 1$
		$5^5 11^8$	$1, -13, -8, 46, 11, -52, -7, 18, 3, -1$
		$2^{10} 11^9$	$0, -11, 0, 44, 0, -77, 0, 55, 0, -11$
		$2^{15} 11^8$	$0, -18, 0, 112, 0, -280, 0, 240, 0, -32$
0		-11^9	$1, 1, 1, 1, 1, 1, 1, 1, 1, 1$
		$-3^5 11^8$	$-3, 12, 1, 20, -7, 16, -2, 5, -1, 1$
		$-2^{10} 11^8$	$0, 15, 0, 35, 0, 28, 0, 9, 0, 1$
		$-7^5 11^8$	$-1, 14, -7, 85, -29, 218, -8, 216, -48, 32$
		$-2^{15} 11^8$	$0, 18, 0, 112, 0, 280, 0, 240, 0, 32$
		$-5^5 11^9$	$-1, 12, -12, 56, -56, 133, -133, 188, -188, 199$
10	5^8	5^{17}	$0, -10, 0, 35, -1, -50, 5, 25, -5, -1$
		$2^{15} 5^{16}$	$0, -40, 0, 480, 0, -1800, 0, 1440, 0, -32$
0		$-3^5 5^{16}$	$0, 10, -10, 90, -49, 125, 70, 95, 10, 1$
		$-2^{10} 5^{16}$	$0, 30, 0, 245, 0, 400, 0, 240, 0, 49$
		$-3^5 5^{17}$	$0, 10, 5, 0, 41, -25, -170, 65, 25, 199$
		$-2^{10} 5^{17}$	$0, 20, 0, 100, 0, 125, 0, 50, 0, 5$
		$-\ 7^5 5^{16}$	$0, 30, -25, 410, -189, 1400, 600, 1480, 160, 32$
		$-2^{15} 5^{16}$	$0, 40, 0, 480, 0, 1800, 0, 1440, 0, 32$
10	31^4	$5^5 31^8$	$-4, -34, 20, 224, 7, -405, 32, 229, -40, -25$
		$3^5 31^9$	$-1, -29, -15, 239, 321, -515, -1029, 94, 910, 397$
		$2^{10} 31^9$	$0, -31, 0, 248, 0, -713, 0, 651, 0, -31$
		$2^{15} 31^8$	$0, -56, 0, 560, 0, -2056, 0, 2784, 0, -800$
0		-31^9	$1, 2, -16, -9, -11, 43, 6, 63, 20, 25$
		$-3^5 31^8$	$-4, 22, 2, 72, -7, 149, 28, 119, -40, 25$
		$-2^{10} 31^8$	$0, 28, 0, 140, 0, 257, 0, 174, 0, 25$
		$-7^5 31^8$	$4, 50, 7, 416, -1, 1584, -104, 2344, 640, 800$
		$-2^{15} 31^8$	$0, 56, 0, 560, 0, 2056, 0, 2784, 0, 800$
		$-5^5 31^9$	$1, 33, -47, 239, -817, 1283, -3559, 4496, -3700, 6845$
10	41^4	41^9	$1, -18, -13, 91, 47, -143, -7, 72, -23, 1$
		$5^5 41^8$	$4, -51, -336, -364, 1485, 4182, 3526, 574, -369, -41$
0		$-3^5 41^8$	$-4, 29, -166, 650, -1633, 3184, -4776, 4722, -2655, 657$
		$-2^{10} 41^8$	$0, 33, 0, 288, 0, 679, 0, 531, 0, 81$
		$-3^5 41^9$	$1, 23, 28, 173, -158, 964, -909, 5115, -2196, 657$
		$-7^5 41^8$	$4, 69, 417, 2093, 6684, 17760, 33265, 38572, 25518, 7681$
		$-2^{15} 41^8$	$0, 66, 0, 1152, 0, 5432, 0, 8496, 0, 2592$
		$-2^{10} 41^9$	$0, 41, 0, 492, 0, 2255, 0, 3403, 0, 369$

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 $F \cdot Q(\sqrt{5})$ and the last one is the composite field $F \cdot Q(\sqrt{2})$. The two other fields contain the quadratic field $Q(\sqrt{3p})$ and $Q(\sqrt{p})$ respectively.

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

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

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)