

QUADRATIC EXTENSIONS OF TOTALLY REAL QUINTIC FIELDS

SCHEHRAZAD SELMANE

ABSTRACT. In this work, we establish lists for each signature of tenth degree number fields containing a totally real quintic subfield and of discriminant less than 10^{13} in absolute value. For each field in the list we give its discriminant, the discriminant of its subfield, a relative polynomial generating the field over one of its subfields, the corresponding polynomial over \mathbb{Q} , and the Galois group of its Galois closure.

We have examined the existence of several non-isomorphic fields with the same discriminants, and also the existence of unramified extensions and cyclic extensions.

1. INTRODUCTION

Although A. Leutbecher showed 42 examples of totally imaginary tenth degree Euclidean fields in 1985 [5], there exist, to our knowledge, no extensive tables of tenth degree number fields. In this paper, we present tables for each signature of tenth degree number fields containing totally real quintic fields, of discriminant less than 10^{13} in absolute value.

To establish these lists we have explicitly constructed all quadratic extensions of totally real quintic fields with discriminant less than 10^{13} in absolute value, each field being defined by a second degree generating polynomial with coefficients in a convenient subfield. To obtain these lists, we used techniques of the geometry of numbers [6] as described in the second section of this paper. The description of the results is done in the third section, where we also provide several tables illustrating some of the results of these computations.

2. THE METHOD

If L is a number field of degree n and of signature (r, s) , we denote by ϑ_L its ring of integers, by d_L its discriminant, by h_L^+ the narrow class number of L and by $J(L)$ the set of distinct \mathbb{Q} -isomorphisms of L into \mathbb{C} . For $\beta \in L$, we denote the corresponding conjugates by $\beta^{(1)}, \dots, \beta^{(n)}$ and we set $T_2(\beta) = \sum_{i=1}^n |\beta^{(i)}|^2$.

Each relative quadratic extension of a quintic field will be given by a second degree polynomial with coefficients in the subfield. In this section we develop a method allowing us to construct explicitly all the relative polynomials.

Let K be a number field of degree 10, of signature (r, s) and of discriminant d_K , such that $|d_K| \leq 10^{13}$, containing a totally real quintic field F . Theorem 2.8 of

Received by the editor March 26, 1998 and, in revised form, April 27, 1999.

2000 *Mathematics Subject Classification.* Primary 11R99, 11Y40, 11R09, 11R11, 11R29.

Key words and phrases. Quintic fields, relative extensions, discriminant.

©2000 American Mathematical Society

J. Martinet [6] proves the existence of an integer $\theta \in K, \theta \notin F$, such that $K = F(\theta)$ and

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

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

Let

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

be the minimal polynomial of θ over F . We denote by θ' the other root of P , by $P_\sigma(x)$, $\sigma \in J(F)$, the polynomial

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

and we define $f(x)$ the polynomial

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

To construct all the polynomials P of which a root generates one of the searched fields K over F , we will work in the field F . Since

$$|d_K| = d_F^2 N(\delta),$$

where δ is the relative discriminant of K/F and N is the absolute norm in the extension F/\mathbb{Q} , we must consider all totally real quintic fields F with discriminant smaller than $10^{\frac{13}{2}}$ [4]. We assume that the discriminant d_F and an integral basis $W = \{w_1 = 1, w_2, \dots, w_5\}$ of F are already known. We denote by B the matrix whose (i, j) entry is $w_i^{(j)}$ and we define $A = B \cdot B^t$.

Let us show how to determine the coefficients a and b of the relative polynomial P . Since the inequality (1) is valid by translation by an element of ϑ_F , we only have to make a run through a system of representatives of ϑ_F modulo $2\vartheta_F$, and so only 2^5 values must be considered for a :

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

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

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

We notice that for a fixed value of a , the running time for the computation of the possible b 's strongly depends upon the size of the real constant bound κ on $T_2(\theta)$ $\left(\kappa = \frac{1}{2} \sum_{i=1}^5 |a^{(i)}|^2 + M, \text{ where } M = \left(\frac{10^{13}}{4d_F} \right)^{\frac{1}{5}} \right)$. The constant κ only depends on the value of a . Let us show now that a can be chosen such that κ will be minimum. Indeed, as inequality (1) remains valid if we replace θ by $\theta + \gamma$ for an

arbitrary $\gamma \in \vartheta_F$, and as $\theta + \gamma$ is also a generator of extension K/F , then if we set $c = -\text{Tr}_{K/L}(\theta + \gamma) = a - 2\gamma$ and represent it by means of the basis W of F as

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

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

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

in the coefficients c_1, \dots, c_5 ($c = (c_1, \dots, c_5)$), 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,

$$m_{ij} = \text{Tr}(w_i w_j) \quad (1 \leq i, j \leq 5).$$

Then we decompose the matrix A into a sum of squares by Cholesky's method [8]

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

and we make c_1, \dots, c_5 run through the integer values for which $q(c) \leq T_2(a)$ and for which the relationship $c \equiv a \pmod{2\vartheta_F}$ is satisfied. We shall associate to a the value of c for which $q(c)$ is minimal, and we shall set $C = \frac{1}{2} \sum_{i=1}^5 |a^{(i)}|^2 + M$.

Remark 2.1. The choice of a is independent of the signature of K and is also independent of the chosen bound; it depends only on the field F . Therefore, we have established the list of the 32 possible values of a for a fixed quintic field, and have considerably improved the execution time of our programs.

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

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

which comes from (1) and the inequality

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

If we represent s_2 by means of the basis 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 in the coefficients y_1, \dots, y_5 ($y = (y_1, \dots, y_5)$). As we have already computed the coefficient matrix A and decomposed it into a sum of squares, we compute all $y \in \mathbb{Z}^5$ subject to $q(y) \leq C^2$ and $y_i \equiv z_i \pmod{2}$ ($1 \leq i \leq 5$), where $a^2 = \sum_{i=1}^5 z_i w_i$. Therefore we obtain all the possible choices for the coefficient b .

For each of the constructed polynomials, we start by determining whether it can define a field with the desired signature. This question is solved by simply examining

the sign of the polynomial discriminant $\Delta = a^2 - 4b$ of each conjugate of P . To considerably reduce the number of polynomials to be considered, we also eliminate the polynomials having too large values of $T_2(\theta)$. To achieve this, we check whether the inequality

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

which follows from inequality (1) and the fact that if z and z' are two complex numbers then

$$|z + z'|^2 + |z - z'|^2 = 2(|z|^2 + |z'|^2),$$

is fulfilled.

The computation of the roots of the five conjugate polynomials of P was only necessary for totally real tenth degree fields, to test the irreducibility of the polynomial P . We computed $L = |N(\Delta)|$; if L is squarefree, we obtain the value of d_K directly; otherwise we used KANT [2] to compute the field discriminant.

For each value of d_K less than 10^{13} in absolute value we have found several polynomials; the number of these polynomials varies between 545 for the first ones and 4 for the last ones. To decide whether or not such polynomials correspond to isomorphic fields, the function `OrderIsSubfield` [2] was used. To compute the Galois group of each polynomial represented in the tables, we used KANT [2].

3. DESCRIPTION OF TABLES

This section is devoted to a brief description of some information provided by these computations; several tables illustrating some of the results are given.

In Table 1, we present the number of fields that were constructed as well as the number of the discriminants for which there are exactly k non-isomorphic fields with the same discriminants.

In Table 2, we give some data regarding the smallest discriminant for each signature where ρ_1 (resp. ρ_2, ρ_3) is a root of the polynomial $x^5 - 2x^4 - 3x^3 + 4x^2 + 2x - 1$ (resp. $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$, $x^5 - 2x^4 - 3x^3 + 5x^2 + x - 1$) and where η denotes the number of conjugate extensions.

TABLE 1.

signature	(10, 0)	(8, 1)	(6, 2)	(4, 3)	(2, 4)	(0, 5)
number of fields	313	2845	7579	7420	3950	770
k	Number of k non-isomorphic fields					
2	3	316	1180	1331	345	22
3	—	22	312	253	47	—
4	—	6	97	108	5	—
5	—	6	22	19	5	—
6	—	—	8	12	—	—
7	—	—	—	1	—	—
8	—	1	2	4	1	—
9	—	—	—	2	—	—
10	—	—	6	4	—	—
12	—	—	3	3	—	—

TABLE 2.

smallest discriminant	(r, s)	$p(x)$	δ	$f(x)$	η
443952558373	(10, 0)	$x^2 + (-2 - 3\rho_1 + 3\rho_1^2 + 2\rho_1^3 - \rho_1^4)x + (-1 + 3\rho_1 - 2\rho_1^2 - 2\rho_1^3 + \rho_1^4)$	$(757, \rho_1 + 52)$	$x^{10} - 11x^8 - 3x^7 + 37x^6 + 14x^5 - 48x^4 - 22x^3 + 20x^2 + 12x + 1$	1
-70952789611	(8, 1)	$x^2 + (2 - \rho_2^2)x + (3\rho_2 - 3\rho_2^2 - \rho_2^3 + \rho_2^4)$	$(331, \rho_2 + 159)$	$x^{10} + x^9 - 7x^8 - x^7 + 16x^6 - 6x^5 - 14x^4 + 8x^3 + 6x^2 - 2x - 1$	5
17007429581	(6, 2)	$x^2 + (1 - \rho_1)x + (-3\rho_1 + 3\rho_1^3 - \rho_1^4)$	$(29, \rho_1 + 2)$	$x^{10} + 3x^9 - 7x^8 - 10x^7 + 15x^6 + 9x^5 - 15x^4 - 3x^3 + 7x^2 - 1$	1
-4930254263	(4, 3)	$x^2 + (-1 + 3\rho_2 + \rho_2^2 - \rho_2^3)x + 1$	$(23, \rho_2 + 4)$	$x^{10} + 3x^9 + 2x^8 - 3x^7 - 9x^6 - 11x^5 - 9x^4 - 3x^3 + 2x^2 + 3x + 1$	5
1332031009	(2, 4)	$x^2 + x + (2 - 6\rho_3 + 3\rho_3^2 + 2\rho_3^3 - \rho_3^4)$	$()$	$x^{10} + 5x^9 + 22x^8 + 58x^7 + 120x^6 + 178x^5 + 183x^4 + 127x^3 + 54x^2 + 12x + 1$	1
-2357947691	(0, 5)	$x^2 + \rho_2x + 1$	$(11, \rho_2 + 2)$	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	1

TABLE 3.

signature	(10, 0)		(8, 1)		(6, 2)		(4, 3)		(2, 4)		(0, 5)	
Type												
T_1	5	572981288913	-	-	-	-	-	-	-	-	3	-2357947691
T_3	-	-	-	-	-	-	-	-	-	-	1	-6283241669043
T_8	-	-	-	-	6	113395848049	-	-	4	113395848049	-	-
T_{14}	37	617567936161	138	-70952789611	226	42228699557	256	-4930254263	140	19077940409	22	-311034736331
T_{15}	-	-	-	-	2	232712654409	-	-	6	232712654409	-	-
T_{22}	4	1832697153125	-	-	-	-	-	-	-	-	73	-142510530627
T_{23}	-	-	6	-698137963227	8	1473846811257	15	-77570884803	1	2404697428893	-	-
T_{37}	12	1363999753216	-	-	712	44860510809	-	-	436	1332031009	-	-
T_{39}	199	443952558373	1492	-97939335863	3055	17007429581	3681	-12932524947	1443	2932315445	235	-257457296071
T_{44}	1	6714415905961	-	-	590	50522901529	-	-	460	20796235681	-	-
T_{45}	55	2424184585229	1209	-146407115723	2980	23365118029	3468	-14362045027	1460	38628899261	436	-52089208083

TABLE 4.

d_K	$f(x)$	w	h_K^+
	(10, 0)		
572981288913	$x^{10} + x^9 - 10x^8 - 10x^7 + 34x^6 + 34x^5 - 43x^4 - 43x^3 + 12x^2 + 12x + 1$	2	2
669871503125	$x^{10} + x^9 - 13x^8 - 8x^7 + 46x^6 + 11x^5 - 52x^4 - 7x^3 + 18x^2 + 3x - 1$	2	1
762939453125	$x^{10} - 10x^8 + 35x^6 + x^5 - 50x^4 - 5x^3 + 25x^2 + 5x - 1$	2	1
2414538435584	$x^{10} - 11x^8 + 44x^6 - 77x^4 + 55x^2 - 11$	2	2
7024111812608	$x^{10} - 18x^8 + 112x^6 - 280x^4 + 240x^2 - 32$	2	1
	(0, 5)		
-2357947691	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	22	1
-219503494144	$x^{10} + 9x^8 + 28x^6 + 35x^4 + 15x^2 + 1$	4	1
-7024111812608	$x^{10} + 18x^8 + 112x^6 + 280x^4 + 240x^2 + 32$	2	5

For each type of Galois group found, the number of fields and smallest discriminant are given in Table 3; the notation for the group names is similar to that of Butler and McKay [1]. In Table 4, we present some data on the cyclic fields found (w denotes the order of group of roots of unity). We notice that three totally imaginary cyclic number fields have the same value of regulator (26.171106).

We finish by stating three propositions on unramified extensions

Proposition 3.1. *For each totally real quintic field of discriminant less than $10^{\frac{13}{2}}$ with narrow class 4 there exist, up to isomorphism, two non-isomorphic unramified extensions of signature (6, 2). All these extensions have class number 1.*

Proposition 3.2. *For each totally real quintic field of discriminant less than $10^{\frac{13}{2}}$ with narrow class 4 there exist, up to isomorphism, one and only one unramified extension of signature (2, 4).*

Proposition 3.3. *For each totally real quintic field of discriminant less than $10^{\frac{13}{2}}$ with narrow class 2 there exist, up to isomorphism, one unramified extension and only one either for the signature (2, 4) or the signature (6, 2).*

All computations were done on SPARC ULTRA 170E at Fachbereich Informatik Technische Universität Darmstadt.

ACKNOWLEDGMENTS

I would like to thank Professors D. Benayat, J. Buchmann and F. Diaz y Diaz. I would like also to thank Buchmann's group, H. Guerbyenne and T. Yoshi.

ADDED AFTER POSTING

Replace Table 1 with the following table.

signature	(10, 0)	(8, 1)	(6, 2)	(4, 3)	(2, 4)	(0, 5)
number of fields	313	2849	7592	7527	3954	772
k	Number of k non-isomorphic fields					
2	3	317	1182	1352	344	22
3	—	22	314	256	47	—
4	—	6	97	109	5	—
5	—	6	22	20	5	—
6	—	—	8	13	—	—
7	—	—	—	1	—	—
8	—	1	2	4	1	—
9	—	—	—	2	—	—
10	—	—	6	4	—	—
12	—	—	3	3	—	—

Remove Table 3.

REFERENCES

- [1] G. Butler and J. McKay, The transitive groups of degree up to eleven, *Comm. Alg.* 11 (1983), 863–911. MR **84f**:20005
- [2] M. Daberkow, C. Fieker, J. Khiners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, KANT V4, *J. Symbolic Comp.* 24 (1997), 267–283. MR **99g**:11150
- [3] F. Diaz y Diaz, Private communication to the author.
- [4] F. Diaz y Diaz, A table of totally real quintic number fields, *Math. Comp.* 56 (1991), 801–808. MR **91h**:11155
- [5] A. Leutbecher, Euclidean fields having a large Lenstra constant, *Ann. Inst. Fourier, Grenoble* 35, 2 (1985), 83–106. MR **86j**:11107
- [6] J. Martinet, *Methodes geometriques dans la recherche des petits discriminants*, Sem. de Theorie des nombres de paris 1983/1984, Birkhauser Verlag, Basel (1985) 147–179. MR **88h**:11083
- [7] M. Pohst, On the computation of number fields of small discriminant including the minimum discriminant of sixth degree fields, *J. Number Theory* 14 (1982), 99–117. MR **83g**:12009
- [8] M. Pohst, On computing isomorphisms of equation orders, *Math. Comp.* 48 (1987), 309–314. MR **88b**:11066
- [9] Sc. Selmane, Non-primitive number fields of degree eight and of signature (2,3), (4,2) and (6,1) with small discriminant, *Math. Comp.* 68(1999), 333–344. MR **99c**:11160

UNIVERSITY OF SCIENCES AND TECHNOLOGY, H.B. INSTITUTE OF MATHEMATICS,
B.P. 32 EL ALIA, BAB-EZZOUAR, 16111, ALGIERS, ALGERIA
E-mail address: selmane@ist.cerist.dz