The Totally Real A_5 Extension of Degree 6 with Minimum Discriminant

David Ford and Michael Pohst

CONTENTS

We determine the totally real algebraic number field F of degree 6 with Galois group A_5 and minimum discriminant, showing that it is unique up to isomorphism and that it is generated by a root of the polynomial

$$f(t) = t^6 - 10t^4 + 7t^3 + 15t^2 - 14t + 3$$

over the rationals. We also list the fundamental units and class number of F, as well as data for several other fields that arose in our computations and that might be of interest.

1. INTRODUCTION

The computation of algebraic number fields having given degree n, signature (r_1, r_2) and minimal (absolute) discriminant has been extended up to degrees 7 (all signatures) and 8 ($r_1 = 0, 8$). Recently there have been several results separating the fields additionally with respect to their Galois groups (with the Galois group being regarded as a permutation group acting on the roots of a generating polynomial). The extensive tables of fields of degree 4 by Ford, Buchmann and Pohst [Buchmann and Ford 1989; Buchmann et al. 1993; Ford 1991] contain, for each signature, fields with each possible Galois group, and therefore also the corresponding fields of minimum discriminant. The same holds for the tables of quintics by Schwarz, Pohst and Diaz y Diaz [Schwarz et al.]. For degree 6, the only extensive results (covering most of the Galois groups) are due to Martinet and others [Bergé et al. 1990; Olivier 1989, 1990, 1991a, 1991b], but they are almost exclusively concerned with imprimitive fields. Martinet [1990] gives a survey of existing results.

The computations of primitive fields of degree 6 and more turn out to be quite time-consuming. (In [Martinet 1990], the author states that "... A_5

Research supported by the Natural Sciences and Engineering Research Council (Canada) and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Quebec).

1058-6458/92 $0.50 per page

and A_6 extensions [of degree 6] are probably out of our computational capabilities".) Consequently, we decided to refine existing methods for a special search of totally real extension fields of degree 6 with alternating Galois group. In Sections 2 and 3 we develop the improved methods. Section 4 contains a summary of the results of the search.

We note that only some of the refinements concern the special type of the Galois group. Others were developed to generate an extensive table of primitive totally real sextics, which will be discussed in a forthcoming paper.

2. GENERATION OF POLYNOMIALS

Given a bound $B \in \mathbf{R}^{>0}$, we want to construct a set $\mathcal{M}$ of monic sixth-degree polynomials such that each primitive totally real algebraic number field F of degree 6 and discriminant $d_F \leq B$ contains a generating element $\rho \in F \backslash \mathbf{Q}$ for which the minimal polynomial $m_\rho(t)$ is contained in $\mathcal{M}$. We proceed by analogy with [Pohst 1982]. We choose ρ to be an algebraic integer; hence,

$$m_\rho(t) = t^6 + a_1 t^5 + a_2 t^4 + a_3 t^3 + a_4 t^2 + a_5 t + a_6 \in \mathbf{Z}[t].$$

According to [Pohst 1982, Theorem 3], ρ can be chosen in such a way that

$$\operatorname{Tr} \rho \in \{0, -1, -2, -3\} \tag{2.1}$$

and

$$\operatorname{Tr} \rho^2 \leq \tfrac{3}{2} + \left(\tfrac{4}{3} B\right)^{1/5} =: \tilde{B}. \tag{2.2}$$

As a consequence of the inequality between arithmetic and geometric means, we get

$$1 \leq |N(\rho)| \leq \left(\tfrac{1}{6} \operatorname{Tr} \rho^2\right)^3. \tag{2.3}$$

Hence, we have estimates for the coefficients a_1, a_2 and a_6 of $m_\rho(t)$. Bounds for the remaining coefficients will be determined below.

Remark. A lower bound for $\operatorname{Tr} \rho^2$ is 9 [Siegel 1945]. If it is not clear how to choose B so that there will be a field F with the desired properties represented in $\mathcal{M}$, one starts with $\operatorname{Tr} \rho^2 = 9, 10, \ldots$ and conditions (2.1) and (2.3) until such a field occurs in the course of the computations, and adjusts B thereafter appropriately.

As noted in [Pohst 1982], instead of calculating bounds for a_3, a_4, a_5 directly, it is easier to determine bounds for the power sums

$$\sigma_i := \sum_{j=1}^{6} \left(\rho^{(j)}\right)^i,$$

where $i = 3, 4, 5, -1$ and the $\rho^{(j)}$ are the zeros of $m_\rho(t)$, and then to make use of Newton's relations

$$\sigma_k + \sum_{i=1}^{k-1} a_i \sigma_{k-i} + k a_k = 0 \quad \text{for } 1 \leq k \leq 6. \tag{2.4}$$

Since [Pohst 1982, Theorem 4] does not seem to be sufficient for extensive calculations with sextics, we choose the following refined approach. We consider the functions

$$s_i(x_1, \ldots, x_6) := \sum_{j=1}^{6} x_j^i \quad \text{for } i = 3, 4, 5, -1,$$

and determine extremal values for them with subsidiary conditions

$$\sum_{j=1}^{6} x_j = \sigma_1 = -a_1,$$
$$\sum_{j=1}^{6} x_j^2 = \sigma_2 = a_1^2 - 2a_2,$$
$$\prod_{j=1}^{6} x_j = a_6.$$

For each fixed triple (a_1, a_2, a_6) within the previously determined bounds, the procedure yields upper and lower bounds for σ_3, σ_4, σ_5 and σ_{-1}.

Solving this extremal value problem along the lines of [Pohst 1982], we find that any local extremum necessarily has at most four different coordinates x_i of multiplicities n_i, for $1 \leq i \leq 4$. The possibilities for (n_1, n_2, n_3, n_4) are

$$(1,1,4,0),\ (1,2,3,0),\ (2,2,2,0),\ (1,1,1,3),\ (1,2,1,2).$$

For each of these possibilities we eliminate variables using the subsidiary conditions, thus obtaining one-variable equations of degrees 6, 12, 6, 3 and 6, respectively. (Four different values for $x_1, \ldots, x_6$ occur only in connection with extremizing s_4, and in that case the sum over these different values must be zero.)

Example. Let x, y, z be (potentially) different values for $x_1, \dots, x_6$, with multiplicities $(1,1,4)$. The subsidiary conditions $x+y+4z+a_1=0$, $x^2+y^2+4z^2-a_1^2+2a_2=0$ and $xyz^4-a_6=0$ are equivalent to

$$\begin{aligned} x+y+4z+a_1&=0,\\ y^2+(4z+a_1)y+(10z^2+4a_1z+a_2)&=0,\\ 10z^6+4a_1z^5+a_2z^4-a_6&=0. \end{aligned}$$

Computing real zeros and substituting back, we get bounds for σ_3, σ_4, σ_5 and σ_{-1}. In view of (2.4) and of the equation $a_6\sigma_{-1}+a_5=0$, bounds for a_3, a_4 and a_5 follow.

We also employed several other bounds from [Pohst 1975] that yield necessary conditions for $f(t)$ to have six real zeros.

3. PROCESSING OF GENERATED POLYNOMIALS

Since the number of 6-tuples $(a_1,a_2,a_3,a_4,a_5,a_6)$ generated is quite large, it is essential to be economic with all calculations in the innermost loop. Therefore, we do not calculate the polynomial discriminant $d(f)$ as suggested in [Pohst 1982]. Instead we compute it as a polynomial in a_5 with coefficients in $\mathbf{Z}[a_1,a_2,a_3,a_4,a_6]$, using Maple [Char et al. 1985]. Thus every polynomial discriminant computation amounts to the evaluation by Horner's method of a polynomial of degree 6 in a_5.

We exclude from further consideration any polynomial with nonsquare discriminant, since we are only interested in fields with Galois group contained in A_6. The comparatively very few polynomials that remain are handled as follows.

- Apply Sturm's rule to remove all polynomials with fewer than six real zeros.
- Remove all reducible polynomials.
- Apply the Round 2 algorithm [Ford 1978; Pohst and Zassenhaus 1989, pp. 291–297; Zassenhaus 1967, 1972; Zimmer 1972, pp. 25–27] to compute an integral basis for each generated field.
- Order the remaining polynomials with respect to their Galois group (computed using Maple), and within each Galois-group type according to the field discriminant.
- Omit isomorphic copies of the same field [Pohst 1987].

4. SUMMARY OF RESULTS

The bounds of Section 2 concern coefficients of minimal polynomials of elements ρ that generate primitive fields. Extensions with Galois group A_4, S_4/V_4 or G_{36}^+ are not primitive, however. The occurrence of such a field in the course of our computations has to be interpreted differently, as the following examples illustrate.

- The polynomial

$$f(t)=t^6-16t^4+8t^3+8t^2-6t+1$$

has a root that generates a totally real algebraic number field F of discrimininant $1832^2 = 3\,356\,224$, and has Galois group S_4/V_4. This is known to be the smallest discriminant for this Galois group [Martinet 1990]. Similarly, we find all 12 fields with Galois group S_4/V_4 and discriminant $d_F \le 21\,000\,000$, and about 100 fields with that Galois group and larger discriminant.

- For totally real sextic number fields F with Galois group G_{36}^+, the minimum discriminant is known to be $3^6 5^4 11^2 = 55\,130\,625$ [Martinet 1990]. The corresponding field F has $\mathbf{Q}(\sqrt{5})$ as its sole quadratic subfield. An integer ρ of $F\setminus\mathbf{Q}$ satisfying the bounds (2.1)–(2.3) is $\frac{1}{2}(1+\sqrt{5})$. However, a generating element for F is obtained only if we consider an integer $\tilde\rho$ of F such that $\operatorname{Tr}\tilde\rho^2$ is the third successive minimum of the quadratic form coming from the trace bilinear form. From [Pohst 1982] we get

$$\operatorname{Tr}\tilde\rho^2 \le \tfrac14\left(6+\tfrac{15}{2}\right)+\left(\frac{4\cdot 55\,130\,625}{6\cdot\frac{15}{2}}\right)^{1/4},$$

and see that this is beyond the bounds found in Section 2. We note that

$$m_{\tilde\rho}(t)=t^6-21t^4-11t^3+99t^2+33t-121.$$

- We obtain seven fields with Galois group A_4, with discriminants 6760^2, 7688^2, 11163^2, 11191^2, 15059^2, 20216^2 and 26569^2. The minimum discriminant for this Galois group is $5096^2 = 25\,969\,216$ [Martinet 1990].

Hence, in the cases of the Galois groups A_4, S_4/V_4 and G_{36}^+, the investigation of relative extensions is certainly superior, and we recovered only part of the tables of [Olivier 1989, 1990, 1991a].

The search for an A_5 extension was performed as explained in the Remark in Section 2. In the course of the computations, we quickly obtained fields of Galois group A_5. Each time a field with Galois group A_5 and a smaller discriminant occurred, we adjusted the bound $\tilde{B}$ of (2.2) correspondingly. Thus we proved the following theorem, using $\tilde{B} = 34$.

Theorem. *The smallest possible discriminant for a totally real A_5 extension of degree* 6 *is $d = 5567^2 = 30\,991\,489$. There is, up to isomorphy, exactly one field F with that discriminant. It is generated by a root ρ of the polynomial*

$$f(t) = t^6 - 10t^4 + 7t^3 + 15t^2 - 14t + 3.$$

The class number of F is 1, *and F has a power integral basis in terms of powers of ρ. A system of fundamental units for F is*

$$\begin{aligned}
\varepsilon_1 &= 5 - 8\rho - 7\rho^2 + 2\rho^3 + \rho^4,\\
\varepsilon_2 &= -23 + 50\rho + 10\rho^2 - 30\rho^3 + \rho^4 + 3\rho^5,\\
\varepsilon_3 &= -25 + 64\rho + 9\rho^2 - 39\rho^3 + 2\rho^4 + 4\rho^5,\\
\varepsilon_4 &= -62 + 131\rho + 26\rho^2 - 79\rho^3 + 3\rho^4 + 8\rho^5,\\
\varepsilon_5 &= -94 + 244\rho + 36\rho^2 - 147\rho^3 + 7\rho^4 + 15\rho^5.
\end{aligned}$$

Defining polynomials and field discriminants for other A_5 extensions with small discriminants are listed in the following table. For each discriminant, there is only one field up to isomorphy.

$t^6 - 9t^4 + 2t^3 + 20t^2 - 8t - 1$	7096^2
$t^6 + 3t^5 - 5t^4 - 14t^3 + 5t^2 + 15t + 4$	8311^2
$t^6 + t^5 - 15t^4 - 27t^3 + 23t^2 + 59t + 19$	10463^2
$t^6 + t^5 - 13t^4 - 7t^3 + 52t^2 + 7t - 53$	10687^2
$t^6 - 13t^4 + 2t^3 + 34t^2 - 30t + 7$	10904^2
$t^6 + 2t^5 - 12t^4 - 21t^3 + 38t^2 + 53t - 10$	10931^2
$t^6 + 2t^5 - 7t^4 - 12t^3 + 10t^2 + 17t + 4$	11699^2
$t^6 + 2t^5 - 13t^4 - 16t^3 + 24t^2 + 37t + 12$	13571^2
$t^6 - 13t^4 + 7t^3 + 44t^2 - 40t - 9$	13613^2
$t^6 - 13t^4 + 4t^3 + 36t^2 - 3t - 22$	16621^2
$t^6 + 3t^5 - 11t^4 - 24t^3 + 36t^2 + 18t - 9$	17859^2
$t^6 - 12t^4 + 6t^3 + 27t^2 - 9t - 7$	18279^2
$t^6 - 13t^4 + 8t^3 + 20t^2 + 3t - 2$	21227^2
$t^6 - 13t^4 + 2t^3 + 41t^2 - 10t - 13$	24524^2
$t^6 + 2t^5 - 13t^4 - 24t^3 + 28t^2 + 44t + 13$	24808^2
$t^6 + 2t^5 - 10t^4 - 16t^3 + 19t^2 + 18t + 1$	26591^2
$t^6 + 2t^5 - 13t^4 - 27t^3 + 18t^2 + 28t - 5$	26843^2
$t^6 + t^5 - 13t^4 - 16t^3 + 36t^2 + 34t - 27$	30067^2
$t^6 + t^5 - 15t^4 - 17t^3 + 41t^2 + 27t - 11$	30119^2

The generation of polynomials took about 342 CPU-hours on a network of Digital MicroVax II and MicroVax III computers in the Department of Computer Science at Concordia University. The class number and fundamental unit computations were done with KANT [Schmettow 1991] at Düsseldorf.

Finally, we should mention that several A_6-extensions occurred. The smallest discriminant value was $13041^2 = 170\,067\,681$. (This extension, as well as the A_5 extension with minimum discriminant, was known to Olivier [1992], but with no proof of minimality.) A verification that this value is indeed minimal requires a bound of $\tilde{B} = 48$ in (2.2). From computations now in progress we estimate that this will take about 33 times as much CPU time as $\tilde{B} = 34$ in the case of A_5.

REFERENCES

[Bergé et al. 1990] A.-M. Bergé, J. Martinet and M. Olivier, "The computation of sextic fields with a quadratic subfield", *Math. Comp.* **54** (1990), 869–884.

[Buchmann and Ford 1989] J. Buchmann and D. Ford, "On the computation of totally real quartic fields of small discriminant", *Math. Comp.* **52** (1989), 161–174.

[Buchmann et al. 1993] J. Buchmann, D. Ford and M. Pohst, "Enumeration of quartic fields of small discriminant", *Math. Comp.* **60** (1993), to appear in April 1993.

[Char et al. 1985] Bruce W. Char et al., *Maple User's Guide*, 4th ed., WATCOM Publications, Waterloo, Ont., 1985.

[Ford 1978] D. Ford, "On the computation of the maximal order in a Dedekind domain", Ph.D. Dissertation, Ohio State University, 1978.

[Ford 1991] D. Ford, "Enumeration of totally complex quartic fields of small discriminant", pp. 129–138 in *Computational Number Theory, Proceedings of the Colloquium on Computational Number Theory, Debrecen (Hungary), 1989*, edited by Pethő et al., de Gruyter, Berlin and New York, 1991.

[Martinet 1990] J. Martinet, "Discriminants and Permutation Groups", pp. 359–385 in *Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association, Banff, 1988*, edited by R. A. Mollin, de Gruyter, Berlin and New York, 1990.

[Olivier 1989] M. Olivier, "Tables de corps sextiques contenant un sous-corps quadratique (I)", *Séminaire* *de Théorie des Nombres de Bordeaux* (Sér. 2) **1** (1989), 205–250.

[Olivier 1990] M. Olivier, "Corps sextiques contenant un corps quadratique (II)", *Séminaire de Théorie des Nombres de Bordeaux* (Sér. 2) **2** (1990), 49–102.

[Olivier 1991a] M. Olivier, "Corps sextiques contenant un corps cubique (III)", *Séminaire de Théorie des Nombres de Bordeaux* (Sér. 2) **3** (1991), 201–245.

[Olivier 1991b] M. Olivier, "Corps sextiques primitifs (IV)", *Séminaire de Théorie des Nombres de Bordeaux* (Sér. 2) **3** (1991), 381–404.

[Olivier 1992] M. Olivier, private communication, 1992.

[Pohst 1975] M. Pohst, "Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper", *J. Reine Angew. Math.* **278/279** (1975), 278–300.

[Pohst 1982] M. Pohst, "On the computation of number fields of small discriminants including the minimum discriminant of sixth degree fields", *J. Number Theory* **14** (1982), 99–117.

[Pohst 1987] M. Pohst, "On computing isomorphisms of equation orders", *Math. Comp.* **48** (1987), 309–314.

[Pohst and Zassenhaus 1989] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyc. of Math. and Its Applications, Cambridge University Press, Cambridge, 1989.

[Schmettow 1991] J. Graf von Schmettow, "KANT: A tool for computations in algebraic number fields", pp. 321–330 in *Computational Number Theory, Proceedings of the Colloquium on Computational Number Theory, Debrecen (Hungary), 1989*, edited by Pethő et al., de Gruyter, Berlin and New York, 1991.

[Schwarz et al.] A. Schwarz, M. Pohst and F. Diaz y Diaz, "A table of quintic number fields", to appear.

[Siegel 1945] C. L. Siegel, "The trace of totally positive and real algebraic integers", *Annals of Math.* **46** (1945), 302–312.

[Zassenhaus 1967] H. Zassenhaus, "Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung", pp. 90–103 in *Funktionalanalysis*, Birkhäuser, Basel, 1967.

[Zassenhaus 1972] H. Zassenhaus, "On the second round of the maximal order program", pp. 398–431 in *Applications of Number Theory to Numerical Analysis*, Academic Press, New York, 1972.

[Zimmer 1972] H. G. Zimmer, *Computational Problems, Methods, and Results in Algebraic Number Theory*, Lect. Notes in Math. **262**, Springer-Verlag, Berlin, 1972.

David Ford, Department of Computer Science, Concordia University, Montréal, Québec, Canada (kbkfe24@vax2.concordia.ca)

Michael Pohst, Mathematisches Institut, Heinrich-Heine-Universität, W-4000 Düsseldorf, Germany (pohst@ze8.rz.uni-duesseldorf.de)

Received July 30, 1992; accepted October 16