The S_5 Extensions of Degree 6 with Minimum Discriminant

David Ford, Michael Pohst, Mario Daberkow, and Nasser Haddad

CONTENTS

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

The algebraic number fields of degree 6 having Galois group S_5 and minimum discriminant are determined for signatures $(0,3)$, $(2,2)$ and $(6,0)$. The fields F_0, F_2, F_6 are generated by roots of $f_0(t) = t^6 + 3t^4 + 2t^3 + 6t^2 + 1$, $f_2(t) = t^6 - 2t^4 + 12t^3 - 16t + 8$, and $f_6(t) = t^6 - 18t^4 + 9t^3 + 90t^2 - 70t - 69$ respectively. Each of these fields is unique up to isomorphism. This completes the enumeration of primitive sextic fields with minimum discriminant for all possible combinations of Galois group and signature.

1. INTRODUCTION

The primitive algebraic number fields of a given degree having discriminant within given bounds may be enumerated by the method of [Pohst 1982]. This approach is applied in [Pohst et al. 1982] to determine the sextic fields of minimum discriminant with Galois group S_6 (signatures $(6,0)$, $(4,1)$ and $(0,3)$) and in [Olivier 1990] for Galois groups S_6 (all signatures) and $A_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ and A_6 (signature (2,2) only). As we will show, the method suffices as well to determine the fields of minimum discriminant for the group $S_5 \simeq \mathrm{PGL}_2(\mathbb{F}_5)$, except in the totally real case.

The method is not adequate for investigating primitive totally real sextic fields; too many examples are generated. A refined method was developed to reduce the examples to a manageable number, and the totally real sextic fields of minimum discriminant with Galois groups A_5 [Ford and Pohst 1992] and A_6 [Ford and Pohst 1993] were determined.

The number of examples produced by this improved method is still enormous. In searching for

1058-6458/1998 $0.50 per page

fields with alternating Galois groups (A_5 and A_6) it is effective to screen out polynomials with nonsquare discriminant. For the group S_5 this technique is not available. In its place we use a more costly screening method based on mod-p polynomial factorization, the efficiency of which is critical for the feasibility of the computation.

2. DISTINGUISHING GALOIS GROUP S_5

The group $\mathrm{PGL}_2(\mathbb{F}_5)$ is generated as a permutation group by (1 2 3 4 5) and (1 6)(2 3)(4 5); the cycle types 1·1·1·1·2, 1·1·1·3, 1·2·3 and 2·4 do not occur in $\mathrm{PGL}_2(\mathbb{F}_5)$. So if f is a polynomial with Galois group $\mathrm{PGL}_2(\mathbb{F}_5)$ and p is a prime not dividing the discriminant of f then the degree sequence of the mod p factors of f cannot be among these four types [van der Waerden 1966, Section 8.10].

We generate polynomials of the form

$$f(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + a_4t^2 + a_5t + a_6 \in \mathbb{Z}[t], \tag{2–1}$$

the coefficients being determined in the order a_1, a_2, a_6, a_3, a_4, a_5.

For each triple (a_1, a_2, a_6) and for each p in a suitably chosen set of primes $\{p_1, \ldots, p_n\}$ we define a flag I_p and Boolean arrays V_p and W_p.

NAME	SPACE	DEFINITION
I_p	n	Has V_p been initialized (to False)?
$V_p[r_3, r_4, r_5]$	$\sum p^3$	Has $W_p[r_3, r_4, r_5]$ been computed?
$W_p[r_3, r_4, r_5]$	$\sum p^3$	Does $t^6+a_1t^5+a_2t^4+r_3t^3+r_4t^2+r_5t+a_6$ give a cycle type from $\mathrm{PGL}_2(\mathbb{F}_5)$?

The values r_3, r_4, r_5 are the residues of a_3, a_4, a_5 mod p. When p divides the discriminant of $t^6 + a_1t^5+a_2t^4+r_3t^3+r_4t^2+r_5t+a_6$, its mod p factorization gives no information, so we regard $W_p[r_3,r_4,r_5]$ as True.

The polynomial $f(t)$ is excluded if $W_p[r_3, r_4, r_5]$ is False for some p in $\{p_1, \ldots, p_n\}$.

When $|a_6|$ is large few triples (a_3, a_4, a_5) are generated. In such cases it is usual that these few polynomials are all excluded using only a few small primes, and it is worthwhile to avoid taking time to initialize V_p for the larger values of p.

When $|a_6|$ is small, many triples (a_3, a_4, a_5) are generated and all the primes are used. For these cases it is advantageous to have the number of primes as large as possible.

3. SIGNATURE (6, 0)

We are to generate at least one defining polynomial $f(t)$ of the form (2.1) for each primitive sextic algebraic number field F with signature (6,0) and discriminant $d_F \le B = 767431973$. Taking $a_1 \in \{0, 1, 2, 3\}$ and ρ a root of f we have

$$\mathrm{Tr}(\rho^2) \le \tfrac{1}{6}a_1^2 + \left(\tfrac{4}{3}B\right)^{1/5}$$

by [Cohen 1993, Theorem 6.4.2], which for successive values of a_1 gives bounds of 63.386, 63.553, 64.053 and 64.886 for $\mathrm{Tr}(\rho^2)$. Because F is totally real we have

$$\mathrm{Tr}(\rho^2) = a_1^2 - 2a_2 \equiv a_1 \mod 2,$$

so that $\mathrm{Tr}(\rho^2)$ is bounded by 62, 63, 64, 63 for $a_1 =$ 0, 1, 2, 3 respectively. Bounds on the coefficients a_2, a_6, a_3, a_4, a_5 are determined as in [Ford and Pohst 1992].

The polynomials are screened for cycle-type compatibility with $\mathrm{PGL}_2(\mathbb{F}_5)$ using the technique of section 2 with the twenty-five primes in the range $2 \le p \le 97$.

The computation required about 13720 CPU-hours on a Digital VAXstation 4000-90 in the Computer Science Department at Concordia University (the same system used in [Ford and Pohst 1993]). The cases with $\mathrm{Tr}(\rho^2) \ge 55$ were independently confirmed on a network of thirty UNIX workstations at the Technische Universität Berlin.

Theorem 3.1. *The minimum possible discriminant for a totally real S_5 extension of degree 6 is $d_6 =$ $767431973 = 7^3 11^3 41^2$. There is, up to isomorphy,* *exactly one field F_6 of that discriminant with Galois group S_5. It is generated by a root ρ_6 of the polynomial*

$$f_6(t) = t^6 - 18t^4 + 9t^3 + 90t^2 - 70t - 69.$$

The class number of F_6 is 1. An integral basis for F_6 is given by

$$1, \quad \rho_6, \quad \rho_6^2, \quad \rho_6^3, \quad \rho_6^4, \quad \rho_6^5.$$

A system of fundamental units for F_6 is

$$\begin{aligned}
\varepsilon_{61} &= 2 - \rho_6,\\
\varepsilon_{62} &= 8 + 8\rho_6 - 10\rho_6^2 + \rho_6^4,\\
\varepsilon_{63} &= 71 + 102\rho_6 - 47\rho_6^2 - 27\rho_6^3 + 5\rho_6^4 + 2\rho_6^5,\\
\varepsilon_{64} &= 104 + 90\rho_6 - 50\rho_6^2 - 26\rho_6^3 + 5\rho_6^4 + 2\rho_6^5,\\
\varepsilon_{65} &= 101 + 129\rho_6 - 63\rho_6^2 - 38\rho_6^3 + 7\rho_6^4 + 3\rho_6^5.
\end{aligned}$$

4. SIGNATURES (2, 2) AND (0, 3)

We generate at least one defining polynomial $f(t)$ for each primitive sextic algebraic number field F with $|d_F| \le B = 2299968$ as in section 3 of [Pohst 1982], with slight variations. Taking $\rho^{(1)}, \dots, \rho^{(6)}$ to be the algebraic conjugates of a root ρ of $f(t)$ and $m > 0$, we define

$$S_m(\rho) = \sum_{j=1}^{6} \left(\rho^{(j)}\right)^m \quad \text{and} \quad T_m(\rho) = \sum_{j=1}^{6} \left|\rho^{(j)}\right|^m.$$

For $a_1 = 0$, 1, 2, 3 the respective bounds on $T_2(\rho)$ given by [Cohen 1993, Theorem 6.4.2] are 19.830, 19.997, 20.497 and 21.330. Bounds on $\lfloor T_3(\rho)\rfloor$, $\lfloor T_4(\rho)\rfloor$, $\lfloor T_5(\rho)\rfloor$ and $\lfloor T_6(\rho)\rfloor$ follow according to [Pohst 1982, Theorem 4], and bounds for a_2, a_6, a_3, a_4, a_5 are then determined in the usual way, using the facts that $S_m(\rho) \in \mathbb{Z}$ and $|S_m(\rho)| \le \lfloor T_m(\rho)\rfloor$.

The polynomials are screened for cycle-type compatibility with $\mathrm{PGL}_2(\mathbb{F}_5)$ and tested for irreducibility. Due to system restrictions the screening technique of section 2 was applied only for the twenty primes in the range $2 \le p \le 71$.

The computation required about 441 CPU-hours on a Digital AlphaServer 2100 4/200 in the Department of Computing Services at Concordia University (for polynomial generation and screening), plus a small amount of time on other systems (for computing signatures, field discriminants, Galois groups, class groups and fundamental units).

Theorem 4.1. *The minimum discriminant for an S_5 extension of degree 6 and signature $(2, 2)$ is $d_2 = 2299968 = 2^6 3^3 11^3$. There is, up to isomorphy, exactly one field F_2 of that discriminant with Galois group S_5. It is generated by a root ρ_2 of the polynomial*

$$f_2(t) = t^6 - 2t^4 + 12t^3 - 16t + 8.$$

The class number of F_2 is 1. An integral basis for F_2 is given by

$$1, \quad \rho_2, \quad \omega_2 = \tfrac{1}{2}\rho_2^2, \quad \rho_2\omega_2, \quad \omega_2^2, \quad \rho_2\omega_2^2.$$

A system of fundamental units for F_2 is

$$\begin{aligned}
\varepsilon_{21} &= \omega_2,\\
\varepsilon_{22} &= 1 - 3\rho_2 + 6\omega_2 - \omega_2^2 + \rho_2\omega_2,\\
\varepsilon_{23} &= -3 + 3\rho_2 + 5\omega_2 - \rho_2\omega_2 + \omega_2^2 + \rho_2\omega_2^2.
\end{aligned}$$

Theorem 4.2. *The discriminant of minimum absolute value for a totally complex S_5 extension of degree 6 is $d_0 = -1778112 = -2^6 3^4 7^3$. There is, up to isomorphy, exactly one field F_0 of that discriminant with Galois group S_5. It is generated by a root ρ_0 of the polynomial*

$$f_0(t) = t^6 + 3t^4 + 2t^3 + 6t^2 + 1.$$

The class number of F_0 is 1. An integral basis for F_0 is given by

$$1, \quad \rho_0, \quad \rho_0^2, \quad \rho_0^3, \quad \rho_0^4, \quad \omega_0 = \tfrac{1}{3}(1 - \rho_0 + \rho_0^2 + \rho_0^3 - \rho_0^4 + \rho_0^5).$$

A system of fundamental units for F_0 is

$$\varepsilon_{01} = \rho_0, \qquad \varepsilon_{02} = -1 + \rho_0 + \rho_0^2 + \rho_0^3.$$

This result is reported in [Haddad 1996].

GROUP	SIGNATURE	DISCRIM.	GENERATING POLYNOMIAL	REFERENCE
A_5	$(6,0)$	30991489	$t^6-10t^4+7t^3+15t^2-14t+3$	[Ford and Pohst 1992]
	$(2,2)$	287296	$t^6+2t^5+t^4+4t^3+2t^2-4t+1$	[Olivier 1990]
A_6	$(6,0)$	170067681	$t^6-24t^4+21t^2+9t+1$	[Ford and Pohst 1993]
	$(2,2)$	287296	$t^6+2t^5-t^4+2t^2-1$	[Olivier 1990]
S_5	$(6,0)$	767431973	$t^6-18t^4+9t^3+90t^2-70t-69$	—
	$(2,2)$	2299968	$t^6-2t^4+12t^3-16t+8$	—
	$(0,3)$	-1778112	$t^6+3t^4+2t^3+6t^2+1$	—
S_6	$(6,0)$	592661	$t^6-5t^5+2t^4+18t^3-11t^2-19t+1$	[Pohst et al. 1982]
	$(4,1)$	-92779	$t^6+t^5-2t^4-3t^3-t^2+2t+1$	[Pohst et al. 1982]
	$(2,2)$	29077	$t^6+2t^5-t^4-t^2-t+1$	[Olivier 1990]
	$(0,3)$	-14731	$t^6+t^5-t^3-t^2+1$	[Pohst et al. 1982]

Primitive sextic fields of minimal discriminant.

REFERENCES

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993.

[Ford and Pohst 1992] D. Ford and M. Pohst, "The totally real A_5 extension of degree 6 with minimum discriminant", *Experiment. Math.* **1**:3 (1992), 231–235.

[Ford and Pohst 1993] D. Ford and M. Pohst, "The totally real A_6 extension of degree 6 with minimum discriminant", *Experiment. Math.* **2**:3 (1993), 231–232.

[Haddad 1996] N. Haddad, *The totally complex sextic S_5 extension of minimum discriminant*, M.Sc. thesis, Concordia University, 1996.

[Olivier 1990] M. Olivier, "Corps sextiques primitifs", *Ann. Inst. Fourier* (*Grenoble*) **40**:4 (1990), 757–767.

[Pohst 1982] M. Pohst, "On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields", *J. Number Theory* **14**:1 (1982), 99–117.

[Pohst et al. 1982] M. Pohst, P. Weiler, and H. Zassenhaus, "On effective computation of fundamental units, II", *Math. Comp.* **38**:157 (1982), 293–329.

[van der Waerden 1966] B. L. van der Waerden, *Algebra*, 7th ed., Grundlehren der Mathematischen Wissenschaften **33**, Springer, Berlin, 1966. Translated as *Algebra*, Frederick Ungar Publishing Co., New York, 1970 (reprinted by Springer, New York, 1991).

David Ford, Department of Computer Science, Concordia University, 1455 de Maisonneuve Blvd. West, Montreal, Quebec H3G 1M8, Canada (ford@cicma.concordia.ca)

Michael Pohst, Fachbereich 3 Mathematik MA 8-1, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany (pohst@math.tu-berlin.de)

Mario Daberkow, Fachbereich 3 Mathematik, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany (daberkow@math.berkeley.edu)

Nasser Haddad, Department of Mathematics, Concordia University, 1455 de Maisonneuve Blvd. West, Montreal, Quebec H3G 1M8, Canada (haddad@cicma.concordia.ca)

Received July 29, 1996; accepted in revised form June 1, 1997

Instructions for Authors

Experimental Mathematics is devoted to experimental aspects of mathematical research. It publishes proved results inspired by experimentation, conjectures suggested by experiments, surveys of certain areas from the experimental point of view, descriptions of algorithms and software for mathematical exploration, and general articles of interest to the community. A more detailed statement of philosophy and of the publishability criteria is available on the World-Wide Web at `http://www.expmath.org`, or by request from the publisher (see address below, or send e-mail to `expmath@expmath.org`).

Submission Information

To submit a contribution, send four copies of the material, together with a cover letter stating that it is intended for publication in *Experimental Mathematics*, to:

Experimental Mathematics
A K Peters, Ltd.
289 Linden Street
Wellesley, MA 02181
phone: 617-235-2210

You are encouraged to send your text in electronic form as well; see the section on Electronic Text at the end of this document.

Submission of a paper implies that the work has not been published before, except perhaps in the form of an abstract or as part of a lecture, review, or thesis; that it is not under consideration for publication elsewhere; that its publication has been approved by all authors and (if appropriate) by the institution where the work was carried out; that, if and when the manuscript is accepted for publication, the authors agree to automatic transfer of the copyright to the publisher; and that the manuscript will not be published elsewhere in any language with the consent of the copyright holders. Submissions will be acknowledged, but not be returned.

Charges

There are no page charges for publications, but authors are expected to contribute toward the cost of color illustrations in their articles. Rates will take into account funding available to authors and editorial necessity.

Offprints

Authors will receive in all 25 free offprints of their work. At production time authors may order up to 75 additional offprints at cost.

Manuscript Requirements

Manuscripts must be in English, French or German. They should be written clearly and concisely. We reserve the right to edit contributions for style and format, with changes subject to the authors' approval.

All submissions must include the following elements:

1. title and (if title exceeds 75 characters) alternative short title for running heads;
2. postal address, affiliation (if appropriate) and electronic address (if available) for each author;
3. an abstract of at most 150 words, in the same language as the article, and an English translation if the article is not in English.

References

References should include full information: author or institution; full title; publisher, city and year (for books, manuals, etc.), or full journal name, volume, year and page range (for papers). References to software should contain complete manufacturer's or distributor's names and addresses. All references in the bibliography should be cited in the text, or accompanied by comments stating their relevance. Reference tags in the text should include author's last name and year of publication, in brackets [Poincaré 1901]. Use a comma to separate a tag from a subsequent page or section number, and semicolons to separate several tags in the same brackets.

Figures

The following types of figures are acceptable:

1. traditional hand-drawn figures, in india ink on glossy paper or vellum;
2. black-and-white and color photographs, of reproduction quality, mounted on $8\frac{1}{2} \times 11$-inch cardboard;
3. electronically generated figures.

1058-6458/1998

For hand-drawn figures and photographs, an original and three clear copies should accompany the four copies of the text.

For electronically generated figures, you can use photographs or printouts for the submission, but you must supply the electronic source files if your article is accepted for publication. Under no circumstances will we reproduce low-resolution hard copy or screen photographs.

Figure source files should be in Encapsulated PostScript (EPS) or in a form that can be converted to EPS, such as GnuPlot or Mathematica input. Many drawing tools such as Adobe Illustrator and Aldus FreeHand can produce EPS output. If your figure contains bitmaps, please generate them at the highest possible resolution: before taking a screen dump, for example, resize the window, if possible, to occupy the whole screen. When in doubt whether your figure source is in an acceptable format, check with the editors by sending electronic mail to `expmath@expmath.org`.

For each figure, please supply a caption and a number by which the figure is referred to in the text. If possible, integrate the figures with the text; otherwise, indicate their optimal placement by means of a comment such as "Place Figure 1 here". In referring to the figure, avoid constructions ("the curve looks like this:") that require the exact placement to be known in advance.

See also the section on Charges, above.

Programs

Experimental Mathematics does not publish programs in printed form. You can include short illustrative excerpts from your programs, either within the text itself (if at most three lines) or as a separate display. Please supply a caption and a number for each displayed listing. Keep in mind that many readers will not be familiar with the programming language in which your program is written; it is almost always better to explain what a program does in words than to let the program speak for itself.

Similar considerations apply to program output and interactive sessions.

Electronic Text

If your article is accepted, it is helpful for us to have the text in electronic form. You can transfer it by e-mail, ftp, or diskette. Send e-mail to `expmath@expmath.org` for details.

Experimental Mathematics is typeset in LaTeX. This means that the production time is shorter if the article is written in LaTeX or other variants of TeX than otherwise. However, having the text in electronic form helps even if it is not in TeX.

Most word-processing and typesetting systems allow you to save the copy in text-only or ASCII mode, where the formatting codes are discarded, and only the text is kept, in a format that approximates that of the typeset document as well as possible. Please use this option when saving your text for production in *Experimental Mathematics*.

The rest of this section concerns authors who are using TeX in one of its variants. Here again there are many things you can do to help the editor's and compositor's work and expedite production.

You should preferably use LaTeX's `article` style or AMS-TeX's `amsppt` style. Whether you use one of these styles, another style, or another variant of TeX such as plain TeX, indicate at the top of the file what system you're using.

Don't use two-column format.

Be as consistent as possible in using your own macros. Put them into a file that is input at the top the document, after all style files. Do not embed any new definitions in your text. Avoid redefining existing TeX, AMS-TeX or LaTeX commands.

Avoid using explicit vertical spacing commands such as `\vskip`, `\medskip`, `\bigbreak`. Default spacing is provided by `\beginsection`, `\proclaim`, `\demo`, etc. in AMS-TeX and plain TeX, and by `\begin{theorem}`, `\section`, etc., in LaTeX. To set off a paragraph or a portion of your text other than proofs, theorems, exercises, etc., you may add extra space, but please provide the compositor with a comment line (a line preceded by `%`) to make sure this space will not be eliminated in reformatting.

Likewise, avoid using explicit horizontal spacing commands. If you must use extra spacing, do it consistently, by means of a macro that can be adjusted globally by the compositor if necessary. Please add a comment if a specific spacing convention is to be retained.

Do not, under any circumstances, insert forced line breaks or page breaks in your document. There is no point in your trying to optimize line breaks and page breaks in the original manuscript, since they will not be preserved in the journal's two-column format. Forced breaks just confuse the compositor.

Set off displayed equations with `$$` on a line by itself.

In general, if you want certain elements to be kept together, or displayed in a particular fashion, add a comment line for the compositor in your electronic files or indicate it in your hard copy.