$\mathbf{A_4}$-SEXTIC FIELDS WITH A POWER BASIS

Daniel Eloff, Blair K. Spearman, and Kenneth S. Williams

Abstract. An infinite family of monogenic sextic fields with Galois group A_4 is exhibited.

1. Introduction. Let K be an algebraic number field of degree n. Let O_K denote the ring of integers of K. The field K is said to possess a power basis if there exists an element $\theta \in O_K$ such that $O_K = \mathbb{Z}+\mathbb{Z}\theta+\cdots+\mathbb{Z}\theta^{n-1}$. A field having a power basis is called monogenic. For an extended history of monogenic number fields the reader should consult [3]. For recent work on this topic see [4, 5, 6, 8]. In this paper we exhibit infinitely many monogenic sextic fields with Galois group A_4.

We prove the following result.

Theorem. Let $d \in \mathbb{Z}$. Set

$$f_d(x) := x^6 + (2d+2)x^4 + (2d-1)x^2 - 1 \in \mathbb{Z}[x]. \tag{1.1}$$

Let $\theta_d \in \mathbb{C}$ be a root of $f_d(x)$. Set $K_d = \mathbb{Q}(\theta_d)$. Then

$$[K_d : \mathbb{Q}] = 6, \quad \mathrm{Gal}(f_d) \simeq A_4,$$

and the fields K_d $(d \in \mathbb{Z})$ are distinct. Moreover K_d is monogenic with ring of integers $\mathbb{Z}[\theta_d]$ for infinitely many values of d.

Remark. We prove that K_d is monogenic whenever $4d^2 + 2d + 7$ is squarefree, which occurs for infinitely many values of d by a result of Nagel [7].

We remark that Anai and Kondo [1] have stated without proof that

$$\mathrm{Gal}(x^6 + (2a+2)x^4 + (2a-1)x^2 - 1) \simeq A_4$$

for all $a \in \mathbb{Q}$ for which $x^6 + (2a+2)x^4 + (2a-1)x^2 - 1$ is irreducible in $\mathbb{Q}[x]$. We show in Section 2 that $f_d(x)$ is, in fact, irreducible in $\mathbb{Z}[x]$ for all $d \in \mathbb{Z}$ (Lemma 2.2) and that $\mathrm{Gal}(f_d) \simeq A_4$ for all $d \in \mathbb{Z}$ (Lemma 2.4). In Section 3 we complete the proof of the theorem.

2. Irreducibility and Galois Group of $\mathbf{f_d}$. Throughout this section $d \in \mathbb{Z}$, $f_d(x)$ is given by (1.1), $\theta_d \in \mathbb{C}$ is a root of $f_d(x)$, and $K_d = \mathbb{Q}(\theta_d)$. Clearly $[K_d : \mathbb{Q}] \le 6$. We denote the splitting field of $f_d(x)$ by L_d.

Lemma 2.1.
(a) K_d contains a unique cubic subfield C_d.
(b) C_d is cyclic over $\mathbb{Q}$.

Proof.
(a) Let

$$g_d(x) := x^3 + (2d+2)x^2 + (2d-1)x - 1 \in \mathbb{Z}[x]$$

so that $g_d(x^2) = f_d(x)$. Suppose that $g_d(x)$ is reducible in $\mathbb{Q}[x]$. As $\deg(g_d(x)) = 3$, $g_d(x)$ has a rational root r. As $g_d(x) \in \mathbb{Z}[x]$, we have $r \in \mathbb{Z}$. Then $r \mid g_d(0)(=-1)$ so $r = \pm 1$. As $g_d(-1) = 1$ we have $r \neq -1$ so $r = 1$. Hence, $4d+1 = g_d(1) = 0$, contradicting $d \in \mathbb{Z}$. Thus, $g_d(x)$ is irreducible in $\mathbb{Q}[x]$ so that $\mathbb{Q}(\theta_d^2)$ is a cubic subfield of K_d.

Suppose $C_d = \mathbb{Q}(\theta_d^2)$ and F are two distinct cubic subfields of K_d. Then the compositum field $C_d \vee F$ is a subfield of K_d of degree 9 over $\mathbb{Q}$. Hence, $9 \mid [K_d : \mathbb{Q}]$, contradicting $[K_d : \mathbb{Q}] \leq 6$.

We have shown that $C_d = \mathbb{Q}(\theta_d^2)$ is the unique cubic subfield of K_d.

(b) As $\mathrm{disc}(g_d(x)) = (4d^2 + 2d + 7)^2$, C_d is a cyclic field.

Lemma 2.2. $f_d(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose that $f_d(x)$ is reducible over $\mathbb{Q}$ so that $[K_d : \mathbb{Q}] < 6$. As

$$3 = [C_d : \mathbb{Q}] \mid [K_d : \mathbb{Q}]$$

we have $[K_d : \mathbb{Q}] = 3$. Thus, θ_d is a root of an irreducible cubic in $\mathbb{Z}[x]$, say,

$$h(x) = x^3 + ax^2 + bx + c.$$

Clearly $-\theta_d$ is a root of $h(-x)$ and $h(-x) \neq -h(x)$. As θ_d and $-\theta_d$ are roots of $f_d(x)$ it follows that

$$f_d(x) = -h(x)h(-x) = x^6 + (-a^2 + 2b)x^4 + (b^2 - 2ac)x^2 - c^2.$$

Equating constant terms of $f_d(x)$, we deduce that $c = \pm 1$. Next, equating the coefficients of x^4 and x^2, we obtain

$$2d + 2 = -a^2 + 2b,$$

$$2d - 1 = b^2 - 2ac.$$

Eliminating d, we have

$$(a-c)^2 + (b-1)^2 = -1,$$

a contradiction, proving that $f_d(x)$ is irreducible in $\mathbb{Q}[x]$.

Lemma 2.3. $[L_d : \mathbb{Q}] \leq 12$.

Proof. Let $\pm\phi_1, \pm\phi_2, \pm\phi_3$ be the roots of $f_d(x)$ with $\phi_1 = \theta_d$. Then $-1 = f_d(0) = -\phi_1^2\phi_2^2\phi_3^2$ so $\phi_1\phi_2\phi_3 = \pm 1$. Then $L_d = \mathbb{Q}(\phi_1, \phi_2, \phi_3) = \mathbb{Q}(\phi_1, \phi_2) = C_d(\phi_1, \phi_2)$ as $C_d = \mathbb{Q}(\theta_d^2) = \mathbb{Q}(\phi_1^2)$. Hence, $[L_d : C_d] \leq 2 \times 2 = 4$ and so $[L_d : \mathbb{Q}] = [L_d : C_d][C_d : \mathbb{Q}] \leq 4 \times 3 = 12$ by Lemma 2.1(a).

Lemma 2.4. $\mathrm{Gal}(f_d) \simeq A_4$.

Proof. The field K_d satisfies $[K_d : \mathbb{Q}] = 6$ (Lemma 2.2), K_d contains a cubic subfield (Lemma 2.1(a)), and

$$\mathrm{disc}(f_d) = 2^6(4d^2 + 2d + 7)^4 \in \mathbb{Z}^2.$$

Hence, from Cohen [2], we see that $\mathrm{Gal}(f_d) \simeq A_4$ or S_4. By Lemma 2.3 we deduce that $\mathrm{Gal}(f_d) \simeq A_4$.

Lemma 2.5. C_d is the only subfield ($\neq \mathbb{Q}$, K_d) of K_d.

Proof. This follows immediately from Lemmas 2.1 and 2.4.

3. Proof of Theorem. We begin by recalling the following result [8].

Lemma 3.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ be irreducible. Suppose that $\theta \in \mathbb{C}$ is a root of $f(x)$ and $K = \mathbb{Q}(\theta)$. If p is a prime number such that $p \parallel a_0$ and $p \mid a_1$, then the ideal $< p >$ ramifies in K.

We now prove our theorem. It is assumed throughout this section that $d \in \mathbb{Z}$ is such that $4d^2 + 2d + 7$ is squarefree. If $d \equiv 2 \pmod 3$, say $d = 3m + 2$ ($m \in \mathbb{Z}$), then

$$4d^2 + 2d + 7 = 36m^2 + 54m + 27 \equiv 0 \pmod 9,$$

a contradiction. Hence, $d \not\equiv 2 \pmod 3$. As $d \in \mathbb{Z}$ we have $(4d + 1)^2 \geq 1$. Therefore,

$$4d^2 + 2d + 7 = \frac{(4d + 1)^2}{4} + \frac{27}{4} \geq \frac{1}{4} + \frac{27}{4} = 7.$$

Also,

$$(4d^2 + 2d + 7, 4d + 1) = (d + 7, 4d + 1) = (d + 7, 27) = 1 \tag{3.1}$$

as $d+7 \not\equiv 0 \pmod 3$. Let p be a prime dividing $4d^2+2d+7$. As $4d^2+2d+7$ is assumed to be squarefree we have $p \parallel 4d^2+2d+7$. Then from (3.1), we deduce that $p \nmid 4d+1$. Let

$$k_d(x) = 3^3 g_d\left(\frac{x-2d-2}{3}\right) = x^3 - 3(4d^2+2d+7)x + (4d+1)(4d^2+2d+7).$$

Recall from the proof of Lemma 2.1(a) that $g_d(x)$ is irreducible in $\mathbb{Q}[x]$. Hence, $k_d(x)$ is irreducible in $\mathbb{Q}[x]$. A root of $k_d(x)$ is $\lambda = 3\theta_d^2 + (2d+2)$ and $\mathbb{Q}(\lambda) = \mathbb{Q}(3\theta_d^2 + (2d+2)) = \mathbb{Q}(\theta_d^2) = C_d$. Hence, by Lemma 3.1, the ideal $< p >$ ramifies in C_d so by Dedekind's Theorem $p \mid d(C_d)$. Thus, we have shown that every prime dividing $4d^2+2d+7$ divides $d(C_d)$. As

$$(4d^2+2d+7)^2 = \operatorname{disc}(g_d) = m^2 d(C_d) \tag{3.2}$$

for some $m \in \mathbb{N}$, we see that every prime p dividing $d(C_d)$ divides $4d^2+2d+7$. Thus, $4d^2+2d+7$ and $d(C_d)$ are divisible by exactly the same set of primes. As $4d^2+2d+7$ is squarefree, we deduce from (3.2) that $m=1$ and

$$d(C_d) = (4d^2+2d+7)^2. \tag{3.3}$$

Next, by the conductor-discriminant formula, see for example [2], we deduce using Lemma 2.1(a) and (3.3) that

$$4d^2+2d+7)^4 \mid d(K_d),$$

say

$$d(K_d) = t(4d^2+2d+7)^4 \tag{3.4}$$

for some $t \in \mathbb{N}$. Hence,

$$2^6(4d^2+2d+7)^4 = \operatorname{disc}(f_d) = l^2 d(K_d) = l^2 t(4d^2+2d+7)^4 \tag{3.5}$$

for some $l \in \mathbb{N}$. From (3.5) we see that $t = u^2$ for some $u \in \mathbb{N}$ and $lu = 2^3$. Thus, $u = 1, 2, 2^2$ or 2^3 and

$$d(K_d) = 2^\alpha(4d^2+2d+7)^4, \quad \alpha \in \{0,2,4,6\}.$$

We wish to show that $\alpha = 6$. To do this it suffices to prove that none of the 32 elements

$$\left\{ \frac{a_0 + a_1\theta_d + a_2\theta_d^2 + a_3\theta_d^3 + a_4\theta_d^4 + \theta_d^5}{2} \;\middle|\; a_0, a_1, a_2, a_3, a_4 \in \{0,1\} \right\}$$

is an algebraic integer. We just illustrate this with the element

$$\frac{\theta_d + \theta_d^3 + \theta_d^4 + \theta_d^5}{2}$$

as the remaining 31 elements can be treated in a similar manner.

Let $\gamma = \theta_d + \theta_d^3 + \theta_d^4 + \theta_d^5$. We show first that γ does not belong to a proper subfield of K_d. Suppose on the contrary that $\gamma \in F$, where F is a subfield of K_d with $F \neq K_d$. Then by Lemma 2.5, $\gamma \in C_d$. As $\gamma = \theta_d(1 + \theta_d^2 + \theta_d^4) + \theta_d^4$ and $\theta_d^2,\ \theta_d^4 \in C_d$, we deduce that $\theta_d \in C_d$, a contradiction. Hence, the minimal polynomial of γ over $\mathbb{Q}$ is of degree 6. Using MAPLE we find that the minimal polynomial of γ over $\mathbb{Q}$ is

$$x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_{6,}$$

where

$$a_1 = -(8d^2 + 8d + 12),$$

$$a_2 = 32d^5 + 64d^4 + 152d^3 + 168d^2 + 140d + 74,$$

$$a_3 = -(64d^5 + 64d^4 + 240d^3 + 144d^2 + 212d + 76),$$

$$a_4 = 64d^5 + 208d^3 - 116d^2 + 148d - 208,$$

$$a_5 = 32d^4 + 32d^3 + 144d^2 + 72d + 144,$$

$$a_6 = -(32d^4 + 40d^3 + 128d^2 + 72d + 104).$$

Clearly,

$$\frac{a^6}{2^3} = -(4d^4 + 5d^3 + 16d^2 + 9d + 13) \equiv d^3 + d + 1 \equiv 1 \pmod 2.$$

Hence, $2^6 \nmid a_6$ so that $\gamma/2$ is not an integer of K_d. We treat the remaining 31 elements in a similar manner obtaining the same conclusion each time.

Thus, we have proved that $\alpha = 6$ and $d(K_d) = 2^6(4d^2 + 2d + 7)^4 = \mathrm{disc}(f_d)$. Hence, $\{1,\ \theta_d,\ \theta_d^2,\ \theta_d^3,\ \theta_d^4,\ \theta_d^5\}$ is an integral basis for K_d.

As

$$4d^2 + 2d + 7 = 4d_1^2 + 2d_1 + 7\ (d,\ d_1 \in \mathbb{Z}) \Longrightarrow d = d_1,$$

we deduce that the fields K_d are distinct.

4. Other Power Bases. If $4d^2+2d+7$ is squarefree, we have shown that $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$ is a power basis for the ring O_{K_d} of integers of K_d. As $N(\theta_d) = -1$,

$$\left\{1, \frac{1}{\theta_d}, \frac{1}{\theta_d^2}, \frac{1}{\theta_d^3}, \frac{1}{\theta_d^4}, \frac{1}{\theta_d^5}\right\}$$

is also a power basis for O_{K_d}, that is $\{1, \phi_d, \phi_d^2, \phi_d^3, \phi_d^4, \phi_d^5\}$ is a power basis for O_{K_d} with

$$\phi_d = \frac{1}{\theta_d} = (2d-1)\theta_d + (2d+2)\theta_d^3 + \theta_d^5.$$

With $d = 0$ we carried out a computer search using an index form corresponding to $\left\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\right\}$, and found five more power bases, namely the bases $\left\{1, \psi_i, \psi_i^2, \psi_i^3, \psi_i^4, \psi_i^5\right\}$ $(i = 1, 2, 3, 4, 5)$ with

$$\psi_1 = 2\theta_d^3 + \theta_d^5,$$

$$\psi_2 = -2\theta_d + 2\theta_d^3 + \theta_d^5,$$

$$\psi_3 = -2\theta_d + \theta_d^3 + \theta_d^5,$$

$$\psi_4 = 2\theta_d + 3\theta_d^3 + \theta_d^5,$$

$$\psi_5 = 2\theta_d + 3\theta_d^2 + 3\theta_d^3 + \theta_d^4 + \theta_d^5.$$

None of these power bases is an integer translate or a Galois conjugate of θ_d. This can easily be checked by finding the minimal polynomials of the above elements and observing that they are distinct, even under integer translation. We do not know if there are any other power bases for this sextic field.

Acknowledgement. The second and third authors were supported by grants from the Natural Sciences and Engineering Research Council of Canada.

References

1. H. Anai and T. Kondo, "A Family of Sextic Polynomials With Galois Group A_5-the Computation of Splitting Fields and Galois Groups," *Studies in the Theory of Computer Algebra and Its Applications,* Kyoto, (1995), 57–72.
2. H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer-Verlag, 2000.
3. I. Gaál, *Diophantine Equations and Power Integral Bases: New Computational Methods,* Birkhäuser, Boston, 2002.
4. M. J. Lavallee, B. K. Spearman, K. S. Williams, and Q. Yang, "Dihedral Quintic Fields With a Power Basis," *Math. J. Okayama Univ.,* 47 (2005), 75–79.
5. I. Járási, "Power Integral Bases in Sextic Fields With a Cubic Subfield," *Acta Sci. Math. (Szeged),* 69 (2003), 3–15.
6. L. Miller-Sims and L. Robertson, "Power Integral Bases for Real Cyclotomic Fields," *Bull. Austral. Math. Soc.,* 71 (2005), 167–173.
7. T. Nagel, "Zur Arithmetik der Polynome," *Abh. Math. Sem. Hamburg,* 1 (1922), 179–194.
8. B. K. Spearman, A. Watanabe, and K. S. Williams, "PSL(2,5) Sextic Fields With a Power Basis," *Kodai Math. J.,* 29 (2006), 5–12.

Mathematics Subject Classification (2000): 11R21

Daniel Eloff
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C.
Canada V1V 1V7
email: dan.eloff@gmail.com

Blair K. Spearman
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C.
Canada V1V 1V7
email: blair.spearman@ubc.ca

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
email: williams@math.carleton.ca