MONOGENIC A_4 QUARTIC FIELDS¹

Blair K. Spearman

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

Abstract

It is shown that there exist infinitely many A_4 quartic fields with a power integral basis.

Mathematics Subject Classification: 11R21

Keywords: A_4 quartic field, power integral basis, monogenic

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 $O_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$. Equivalently $O_K = \mathbb{Z}[\theta]$. In this case we say O_K or K is monogenic. We can extend the idea of a power basis to an order of O_K , that is a subring of R of O_K which contains 1 and has finite index in O_K . The ring of integers O_K of K is called the maximal order. An important problem in algebraic number theory is to decide if a number field is monogenic. Every quadratic field is monogenic. Dedekind [1] gave an example of a cubic field which is not monogenic. For background on the history of this problem see [4] and [7].

In [5] the author gives five parametric families of monic quartic polynomials in $\mathbb{Z}[x]$. A root ξ of any of these polynomials defines a totally complex quartic field $\mathbb{Q}(\xi)$. All power bases are determined in the order $\mathbb{Z}[\xi]$. One of these five families of quartic polynomials has Galois group A_4 the alternating group. This family is

$$x^4 + 4kx^3 + 4k^2x^2 + 8x + 4k^2 + 8k + 12, \quad k \in \mathbb{Z}.$$

¹Research was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

In fact the order $\mathbb{Z}[\xi]$ corresponding to a root of this family is never equal to the maximal order for any integer k . It is easy to see this by calculating the minimal monic polynomial of $\frac{\xi^2}{2}$. This polynomial is

$$x^4 - 4k^2x^3 + (4k^4 + 2k^2 - 12k + 6)x^2 + (4k^4 + 8k^3 + 12k^2 - 8)x + k^4 + 4k^3 + 10k^2 + 12k + 9 \in \mathbb{Z}[x].$$

Consequently $\frac{\xi^2}{2}$ is an algebraic integer which clearly does not belong to the order $\mathbb{Z}[\xi]$.

One part of the study of power bases is the process of determining which Galois groups admit infinitely many fields whose rings of integers are monogenic. Therefore it seems worthwhile to give a new parametric family of A_4 quartic fields with this property. We define a parametric family of polynomials as follows.

$$f_t(x) = x^4 + 18x^2 - 4tx + t^2 + 81, \quad t \in \mathbb{N}.$$

Let $\theta = \theta_t$ denote a root of $f_t(x)$ and set $K_t = \mathbb{Q}(\theta_t)$. We prove the following Theorem in section 3 after some useful Lemmas in section 2. As expected, much of the work involves field discriminant calculations.

Theorem. *Suppose that t is a positive integer and that $t(t^2 + 108)$ is square-free. Then K_t is a monogenic A_4 quartic extension of $\mathbb{Q}$. Moreover the fields K_t are distinct.*

Remark. We note that a theorem of Erdős guarantees that $t(t^2 + 108)$ is squarefree for infinitely many positive integers t , (see [2]) so that our theorem will imply that there exist infinitely many monogenic A_4 quartic fields.

2. Some relevant Lemmas for the polynomials $f_t(x)$. Throughout this section t denotes a positive integer, p a prime number, θ_t a root of $f_t(x)$ and $K_t = \mathbb{Q}(\theta_t)$. If a, k are integers with $k > 0$, we use the notation $p \mid a$ for p divides a , $p \nmid a$ for p does not divide a and $p^k \parallel a$ if $p^k \mid a$ but $p^{k+1} \nmid a$.

Lemma 2.1 *If $t(t^2 + 108)$ is squarefree then $f_t(x)$ is irreducible so that K_t is a quartic field extension of $\mathbb{Q}$.*

Proof. Since $t(t^2 + 108)$ is squarefree, clearly t must be odd. It is easy to see that if t is odd then $2 \parallel t(t^2 + 108)$. Therefore $f_t(x)$ is 2-Eisenstein so that $f_t(x)$ is irreducible and hence K_t is a quartic field as required.

Lemma 2.2 *We have $\text{disc}(f_t(x)) = 2^8 t^2 (t^2 + 108)^2$.*

Proof. The calculation of this polynomial discriminant is straightforward.

The next Lemma involves the resolvent cubic of $f_t(x)$. We recall from [6] that the resolvent cubic of a quartic polynomial $x^4 + Px^2 + Qx + R$ is $x^3 - Px^2 - 4Rx + (4PR - Q^2)$.

Lemma 2.3 *If $t(t^2 + 108)$ is squarefree then the resolvent cubic of $f_t(x)$ is irreducible.*

Proof. Corresponding to $f_t(x)$ the resolvent cubic is $x^3 - 18x^2 - 4(t^2 + 81)x + 56t^2 + 5832$. Applying the transformation $x = y + 6$ we obtain the reduced cubic $h(y) = y^3 - 4(t^2 + 108) + 32(t^2 + 108)$. Since t is a positive integer and odd as we saw in the proof of Lemma 2.1, we have $t^2 + 108$ greater than one and odd. Therefore $t^2 + 108$ is divisible by an odd prime p . Since $t(t^2 + 108)$ is squarefree it follows that $h(y)$ is p -Eisenstein and therefore irreducible.

The next four Lemmas are used to determine the field discriminant $d(K_t)$.

Lemma 2.4. *If $t(t^2 + 108)$ is squarefree then $2^8 \parallel d(K_t)$.*

Proof. Recall from the proof of Lemma 2.1 that $f_t(x)$ is 2-Eisenstein. It follows from [3, p. 44] that $2 \nmid \text{ind } \theta_t$, the index of θ_t , so that the power of 2 dividing $d(K_t)$ is equal to the power of 2 dividing $\text{disc}(f_t(x)) = 2^8 t^2 (t^2 + 108)^2$ by Lemma 2.2. Recalling that $t(t^2 + 108)$ is odd we obtain the result.

The next Lemma gives a general result useful for field discriminant calculations.

Lemma 2.5. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$. Suppose that θ is a root of $f(x)$ and $K = \mathbb{Q}(\theta)$. If p is a prime number and k a positive integer with $k < n$ such that $p^k \parallel a_0$ and $p^{k+1-i} \mid a_i$, $1 \leq i \leq k$ then the ideal $\langle p \rangle$ ramifies in K .*

Proof. Suppose that $\langle p \rangle$ does not ramify in K . Then there exist distinct prime ideals $\wp_1, \dots, \wp_r$ such that

$$\langle p \rangle = \wp_1 \cdots \wp_r.$$

As $p^k \parallel a_0$ we have as ideals in O_K , $\langle a_0 \rangle = \wp_1^k \cdots \wp_r^k \langle b \rangle$ for some $b \in \mathbb{Z}$ with $p \nmid b$. Thus $\wp_i \nmid \langle b \rangle$ for $i = 1, \dots, r$. Since $N(\theta_t) = \pm a_0 \equiv 0 \pmod{p}$ the ideal $\langle \theta_t \rangle$ must be divisible by at least one $\wp_i$ say $\wp$. As $\wp^{k+1-i} \mid a_i$, $1 \leq i \leq k$ we have

$$\begin{aligned} a_0 &= a_0 - f(\theta_t) \\ &= (-a_1\theta_t - \cdots - a_k\theta_t^k) - (a_{k+1}\theta_t^{k+1} - \cdots - \theta_t^n) \equiv 0 \pmod{\wp^{k+1}}. \end{aligned}$$

since $\wp^{k+1}$ clearly divides each term inside the pairs of brackets, contradicting $p^k \parallel a_0$. Thus $\langle p \rangle$ ramifies in K .

Lemma 2.6. *If $t(t^2 + 108)$ is squarefree and $p \mid t$ then the ideal $\langle p \rangle$ ramifies in K_t .*

Proof. We begin by giving the minimal polynomial of $\theta_t^2 + 9$. A standard calculation results in

$$x^4 + 2t^2x^2 - 16t^2x + t^4 + 144t^2 \quad (2.1)$$

Before we can apply Lemma 2.5 we must check that this polynomial is irreducible so that $\mathbb{Q}(\theta_t^2 + 9) = \mathbb{Q}(\theta_t)$. We have already noted that if $t(t^2 + 108)$ is squarefree then t is odd. Additionally it is clear that $3 \nmid t$. Therefore we can write $t = 3m \pm 1$ for some positive integer m . Substituting for t in (2.1) and factoring modulo 3 gives

$$(x + 2)(x^3 + x^2 + 2)$$

It follows from this factorization that if the polynomial given in (2.1) is reducible then its factorization must be equal to a linear polynomial times an irreducible cubic and $\theta_t^2 + 9$ is a root of one of these factors. The first possibility is impossible since otherwise $\theta_t^2 + 9$ would satisfy a linear equation over $\mathbb{Q}$ implying that the degree $[K_t : \mathbb{Q}] \leq 2$, contradicting Lemma 2.1. If $\theta_t^2 + 9$ were a root of an irreducible cubic then K_t would have a cubic subfield which is impossible for a quartic field. Therefore the polynomial (2.1) is irreducible. Observe that p^2 is the exact power of p in the constant term of (2.1). Therefore we can apply Lemma 2.5 to (2.1) and the given p , with $k = 2$ and the result follows.

Lemma 2.7 *If $t(t^2 + 108)$ is squarefree and $p \mid t^2 + 108$ then the ideal $\langle p \rangle$ ramifies in K_t .*

Proof. We begin by giving the minimal polynomial of $\theta_t^2 + 3$. A standard calculation results in

$$x^4 + 24x^3 + 2(t^2 + 108)x^2 + 8(t^2 + 108)x + (t^2 + 108)(t^2 + 12) \quad (2.2)$$

Before we can apply Lemma 2.5 we must check that this polynomial is irreducible so that $\mathbb{Q}(\theta_t^2 + 9) = \mathbb{Q}(\theta_t)$. However the proof of Lemma 2.6 shows that $\mathbb{Q}(\theta_t^2 + 9) = \mathbb{Q}(\theta_t)$ and clearly $\mathbb{Q}(\theta_t^2 + 3) = \mathbb{Q}(\theta_t^2 + 9)$ so irreducibility is immediate. Observe that p exactly divides the constant term of (2.2). Therefore we can apply Lemma 2.5 to (2.2) with the given p , and $k = 1$ to complete the proof.

3. Proof of Theorem. Let t be a positive integer such that $t(t^2 + 108)$ is squarefree. We must show

- (1). $\text{Gal}(f_t(x)) \simeq A_4$.
- (2). $d(K_t) = \text{disc}(f_t(x))$.
- (3). The fields K_t are distinct.

By Lemma 2.1 we know that $f_t(x)$ is irreducible. To show that the Galois group of $f_t(x) \simeq A_4$ we must show that $\text{disc}(f_t(x))$ is a perfect square in $\mathbb{Z}$ and that the resolvent cubic of f has no rational roots. See [6] for details. Lemma 2.2 gives $\text{disc}(f_t(x)) = 2^8 t^2 (t^2 + 108)^2$. Lemma 2.3 shows that the resolvent cubic is irreducible so has no rational root. This establishes (1).

By Lemma 2.4 $2^8 \mid d(K)$. Since $t(t^2 + 108)$ is squarefree t is squarefree and odd. Let p be a prime with $p \mid t$. By Lemma 2.6 $\langle p \rangle$ ramifies in K_t so $p \mid d(K)$. However there exists a positive integer c such that

$$d(K)c^2 = \text{disc}(f_t(x)) = 2^8 t^2 (t^2 + 108)^2. \quad (2.3)$$

It follows that $d(K)$ is a square so that $p^2 \mid d(K)$ and hence as t is squarefree we have $t^2 \mid d(K)$. Exactly the same argument applied to the primes dividing $t^2 + 108$ gives $(t^2 + 108)^2 \mid d(K_t)$. Since $t(t^2 + 108)$ is squarefree we deduce that the integers 2^8 , t^2 and $(t^2 + 108)^2$ are pairwise relatively prime. Hence their product $2^8 t^2 (t^2 + 108)^2 \mid d(K_t)$. Combining this statement with (2.3) we deduce that $c = 1$ and $d(K_t) = \text{disc}(f_t(x))$ so that $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis for K_t . Therefore K_t is a monogenic A_4 quartic field and we have verified (2).

To finish our proof and show that the fields K_t are distinct we just have to show that for each positive integer n there is at most one value of t such that $2^8 t^2 (t^2 + 108)^2 = n^2$. Therefore we obtain infinitely many different field discriminants from the infinite set of positive integers t such that $t(t^2 + 108)$ is squarefree, which guarantees that our fields K_t are distinct. Since $t, t(t^2 + 108)$ and n are positive we can reduce to showing that for any positive rational number r , $t(t^2 + 108) - r$ has at most one solution. Viewed as a polynomial in t the discriminant is equal to $-2^8 3^9 - 27r^2 < 0$. Hence this cubic polynomial has one real root and (3) follows.

References

- [1] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh. Kgl. Ges. Wiss. Göttingen **23** (1878), 1-23.

- [2] P. Erdős, *Arithmetic properties of polynomials*, J. London Math. Soc. **28** (1953), 416-425.
- [3] J. Esmonde and M.R. Murty, *Problems in algebraic number theory*, Springer New York, 1999.
- [4] I. Gaál, *Diophantine equations and power integral bases. New Computational Methods*, Birkhauser, Boston 2002
- [5] I. Gaál, *Power integral bases in orders of families of quartic fields*, Publ. Math. (Debrecen) **42** 1993, 253-263.
- [6] L.C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly, **96** (1989) 133-137.
- [7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Third Edition Springer (2000).

Received: May 25, 2006