JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Melisa J. LAVALLEE, Blair K. SPEARMAN et Qiduan YANG

PSL(2, 7) septimic fields with a power basis

Tome 24, n° 2 (2012), p. 369-375.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_2_369_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 369-375

PSL(2, 7) septimic fields with a power basis

par Melisa J. LAVALLEE, Blair K. SPEARMAN et Qiduan YANG

Résumé. Nous donnons un ensemble infini de corps de degré 7 monogènes distincts dont la clôture normale a pour groupe de Galois $PSL(2,7)$.

Abstract. We give an infinite set of distinct monogenic septimic fields whose normal closure has Galois group $PSL(2,7)$.

1. Introduction

Let K denote an algebraic number field of degree n over $\mathbb{Q}$ and O_K denote its ring of integers. An integral basis for K is a set $\{\eta_1, \eta_2, \ldots \eta_n\}$ of elements of O_K such that every element $\alpha \in O_K$ can be expressed uniquely in the form

$$\alpha = x_1\eta_1 + x_2\eta_2 + \cdots + x_n\eta_n \ (x_1, \ldots, x_n \in \mathbb{Z}).$$

One type of integral basis which is particularly interesting is the power integral basis. In this case there exists an algebraic integer $\theta \in O_K$ such that $\{1, \theta, \theta^2, \ldots \theta^{n-1}\}$ is an integral basis for K, and the number field K is said to be monogenic. It is a nontrivial problem to decide whether a number field has a power basis. The lengthy history of this important problem can be examined in Gaál [2] and Narkiewicz [9]. For algebraic number fields of given degree and Galois group of their normal closure, power bases may be quite rare. As an example, there is only one cyclic quintic field with a power basis which was shown by Gras [3]. The same phenomenon occurs for octic fields with Galois group 2 elementary abelian where there is exactly one field with a power basis as shown by Motoda, Nakahara and Park [6]. On the other hand there are infinitely many dihedral quintic fields with a power basis which were given by Lavallee, Spearman, Williams and Yang [5], and infinitely many PSL(2,5) sextic fields with a power basis as was demonstrated by Spearman, Watanabe and Williams in [8].

In this paper we study septimic field extensions of $\mathbb{Q}$ whose normal closure has Galois group PSL$(2, 7)$, the projective special linear group of 2×2 matrices over $\mathbb{F}_7$. We refer to these fields as PSL$(2, 7)$ septimic fields. The

Manuscrit reçu le 11 janvier 2011.
Research supported by the Natural Sciences and Engineering Research Council of Canada.
Mots clefs. Galois Group, Septimic Field, Power Basis.
Classification math. 11R04, 11R32.

purpose of our paper is to show that infinitely many of these septimic fields are monogenic, as described in the following theorem.

Theorem 1.1. *There are infinitely many integers b such that the polynomials*

$$f_b(x) = x^7 + x^6 + x^5 + bx^4 + (b-2)x^3 - 5x^2 - 2x + 1$$

define distinct monogenic $PSL(2,7)$ septimic fields.

2. A parametric family of PSL(2,7) polynomials

For indeterminates a, A we consider the following family of polynomials due to LaMacchia which can be found in Jensen, Ledet and Yui [4, p. 55].

$$\begin{aligned} f(a,A,x) = {} & x^7 + 2(1-3a)x^6 + (-3+4a+8a^2)x^5 + (-2+6a-14a^2)x^4 \\ & + (2-4a+6a^2-8a^3)x^3 + 8(2+a)a^2x^2 + 4(-3+2a)a^2x \\ & - 8a^3 + Ax^3(1-x). \end{aligned}$$

The Galois group of $f(a,A,x)$ over $\mathbb{Q}(a,A)$ is isomorphic to $PSL(2,7)$. To obtain the family of polynomials $f_b(x)$ in our theorem we let b be an integer and choose

$$a = 1/2,\ A = b - 5/2,$$

scale by replacing x by $-x$ and then simplify. Although it is expected that such a specialization will result in $f_b(x)$ being irreducible over $\mathbb{Q}$ and having Galois group $PSL(2,7)$ this is not guaranteed, so we must confirm the basic algebraic properties of the polynomials $f_b(x)$.

Lemma 2.1. *If b is a positive integer then $f_b(x)$ is irreducible over $\mathbb{Q}$.*

Proof. The polynomials

$$f_0(x) = x^7 + x^6 + x^5 - 2x^3 - 5x^2 - 2x + 1$$

and

$$f_1(x) = x^7 + x^6 + x^5 + x^4 - x^3 - 5x^2 - 2x + 1$$

are irreducible modulo 2. Therefore considering the cases b even and b odd we see that the polynomial $f_b(x)$ is irreducible for all integers b. □

Lemma 2.2. *If b is an integer then the discriminant of the polynomial $f_b(x)$ is*

$$(b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2. \tag{2.1}$$

Proof. This calculation was carried out using Maple. □

Lemma 2.3. *If b is an integer then not all of the roots of the polynomial $f_b(x)$ are real.*

Proof. The discriminant of $f_b(x)$ is clearly nonzero by (2.1) so that the roots of $f_b(x)$ are distinct. If all of the roots of $f_b(x)$ were real then by Rolle's Theorem, the n^{th} derivative of $f_b(x)$ would have $7-n$ real roots for $0 \le n \le 6$. However $f_b^{(5)}(x) = 2520x^2 + 720x + 120$ which has no real roots. This contradiction establishes the result. □

Lemma 2.4. *If b is an integer then the Galois group of $f_b(x)$ is isomorphic to PSL$(2,7)$.*

Proof. By Lemma 2.2 the discriminant of the polynomial $f_b(x)$ is equal to a perfect square in $\mathbb{Q}$. A list of possible Galois groups for septimic polynomials is given by Cohen [1]. Those which correspond to a square discriminant are

C_7, the cyclic group of order 7,
M_{21} or F_{21} the Frobenius group of order 21,
PSL$(2,7)$,
A_7, the alternating group.

By Lemma 2.3, $f_b(x)$ has at least some complex roots. Thus complex conjugation is a nontrivial element of the automorphism group of the splitting field of $f_b(x)$ so the order of the Galois group of $f_b(x)$ is divisible by 2. This eliminates C_7 and M_{21}. To eliminate A_7 we adapt the argument given in [4, p. 55]. A calculation yields the polynomial identity

$$y^3(1+y)f_b(x) + x^3(1+x)f_{-b+5}(y) = p(x,y)q(x,y) \tag{2.2}$$

for polynomials $p(x,y)$ and $q(x,y)$ of degree 3 and 4 in x respectively which are given by

$$p(x,y) = yx^3 + (-y^2+1)x^2 + (y^3+1)x + y^2 + y$$

and

$$\begin{aligned} q(x,y) = {} & (y^3+y^2)x^4 + (y^4+2y^3-y)x^3 + (y^4-3y^2-y+1)x^2 \\ & + (-y^3-y^2-y)x + y^2. \end{aligned}$$

Let β be a root of $f_{-b+5}(x)$. As f_{-b+5} is irreducible over $\mathbb{Q}$ by Lemma 2.1, $\beta \neq 0, -1$. Then setting $y = \beta$ in (2.2) gives

$$\beta^3(1+\beta)f_b(x) = p(x,\beta)q(x,\beta). \tag{2.3}$$

Equation (2.3) is a factorization of $f_b(x)$ into factors of degree 3 and 4 respectively over $\mathbb{Q}(\beta)$ which is a degree 7 extension of $\mathbb{Q}$. We deduce from this that the degree of the splitting field of $f_b(x)$ over $\mathbb{Q}$ is a divisor of $7 \cdot 3! \cdot 4!$. In particular this degree is not divisible by 5 so that the possibility of A_7 as Galois group is now eliminated and the proof is complete. □

3. Calculation of the field discriminant

We have established that the polynomial $f_b(x)$ is irreducible over $\mathbb{Q}$ and has Galois group isomorphic to PSL$(2,7)$. Let θ be a root of $f_b(x)$. Then $K = \mathbb{Q}(\theta)$ is a PSL$(2,7)$ septimic field. We set

$$g(b) = g_1(b)g_2(b) \tag{3.1}$$

where

$$g_1(b) = b^2 - 5b - 25 \tag{3.2}$$

and

$$g_2(b) = 27b^2 - 135b + 769. \tag{3.3}$$

We will determine the field discriminant $d(K)$ of $K = \mathbb{Q}(\theta)$ under the assumption that $g(b)$ is squarefree. We begin with the following lemma.

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 over $\mathbb{Q}$. Suppose that α is a root of $f(x)$ and $K = \mathbb{Q}(\alpha)$. If p is a prime number and k a positive integer with $k < n$ such that $p^k \parallel a_0$ and $p^{k+1-i} \mid a_i$, $1 \le i \le k$ 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 $\wp_1, \ldots \wp_r$ in O_K such that

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

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

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

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

The next two lemmas determine the ramified primes in $\mathbb{Q}(\theta)$. To do this we give two elements in K and their monic minimal polynomials in $\mathbb{Z}[x]$ to which we can apply the previous lemma. To experimentally find candidates for these elements we formally solved the polynomial equation $f_b(x) = 0$ for b, calculated $b^2 - 5b - 25$ from this, then tried factors of this expression to find θ_1. A similar experiment produced θ_2. These elements are

$$\theta_1 = -\theta^4 - 2\theta^3 - 2\theta^2 - \theta + 1,$$

and

$$\theta_2 = -3\theta^4 + 2\theta^2 - 3\theta - 3\ .$$

Lemma 3.2. *Let $b \in \mathbb{Z}$ be such that $g_1(b)$ is squarefree. Let p be a prime such that $p \mid g_1(b)$. Then $p \mid d(K)$.*

Proof. The element θ_1 is clearly a primitive element for K. The monic minimal polynomial $h_b(x)$ of θ_1 in $\mathbb{Q}[x]$ is

$$\begin{aligned} h_b(x) = {} & x^7 + (1-6b)x^6 + (10b^2+29b-40)x^5 \\ & + (b^4 - 5b^3 - 54b^2 + 60b + 475)x^4 - (4b^2 - 9b - 78)g_1(b)x^3 \\ & + 3(2b^2 - 8b - 45)g_1(b)x^2 - 4g_1(b)^2x + g_1(b)^2. \end{aligned}$$

As $g_1(b)$ is squarefree, Lemma 3.1 applies to the polynomial $h_b(x)$ with $k = 2$ and we conclude that $p \mid d(K)$. □

Lemma 3.3. *Let $b \in \mathbb{Z}$ be such that $g_2(b)$ is squarefree. Let p be a prime such that $p \mid g_2(b)$. Then $p \mid d(K)$.*

Proof. The element θ_2 is clearly a primitive element for K. The monic minimal polynomial $k_b(x)$ of θ_2 in $\mathbb{Q}[x]$ is

$$\begin{aligned} k_b(x) = {} & x^7 + 41x^6 + (54b^2 - 27b + 318)x^5 \\ & + (27b^4 - 189b^3 + 1066b^2 - 782b - 4325)x^4 \\ & + (10b^2 - 21b - 50)g_2(b)x^3 \\ & + (36b^2 - 114b + 263)g_2(b)x^2 + 2g_2(b)^2x + g_2(b)^2. \end{aligned}$$

As $g_2(b)$ is squarefree, Lemma 3.1 applies to the polynomial $k_b(x)$ with $k = 2$ and we conclude that $p \mid d(K)$. □

Lemma 3.4. *If $g(b)$ is squarefree then $d(K) = g(b)^2$.*

Proof. Certainly $d(K)$ is a divisor of $g(b)^2$ the discriminant of the polynomial $f_b(x)$. Specifically,

$$g(b)^2 = c^2 d(K)$$

for some nonzero integer c. On the other hand by Lemmas 3.2 and 3.3 each prime number p dividing $g(b)$ divides $d(K)$. Since $g(b)$ is squarefree we deduce that $p \nmid c$. It follows that $c^2 = 1$ proving the Lemma. □

We will require that the polynomial $g(b)$ assume squarefree values for infinitely many positive integers b. Since the polynomial $g(b)$ is reducible over $\mathbb{Z}$ we can use a proposition due to Nair [7, Theorem C, p. 181-182.]. In order to state this proposition we first define

$$N_k(f, x, h) = N_k(x, h) = |\{n : x < n \leq x + h,\ f(n) \text{ is } k\text{-free}\}|$$

Proposition 3.1. *If*

$$f(x) = \prod_{i=1}^{m} (f_i(x))^{\alpha_i}$$

where each f_i is irreducible, $\alpha = \max_i \alpha_i$ and deg $f_i(x) = g_i$, then

$$N_k(x,h) = \Lambda_k h + O\left(\frac{h}{(\log h)^{k-1}}\right) \tag{3.4}$$

for $h = x^\theta$ where $0 < \theta < 1$ and $k \geq \max\{\lambda g_i, \alpha_i\}$, $(\lambda = \sqrt{2} - 1/2)$ provided that at least one $g_i \geq 2$ (the constant Λ_k is positive).

Lemma 3.5. *There exist infinitely many positive integers b such that $g(b)$ is squarefree.*

Proof. The quartic polynomial $g(b)$ is equal to the product of two irreducible quadratic polynomials over $\mathbb{Q}$. The polynomial $g(b)$ has no fixed square divisors as can be deduced from (3.1), (3.2) and (3.3). To apply the previous proposition, we note that $k \geq \max\{\lambda g_i, \alpha_i\}$ simplifies to $k \geq 2$ so that we can set $k = 2$. The conclusion of the Lemma now follows from (3.4). □

4. Proof of Theorem

We are ready to prove our theorem.

Proof. The polynomial $f_b(x)$ has discriminant equal to

$$g(b)^2 = (b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2,$$

by Lemma 2.2. Moreover if θ is a root of $f_b(x)$ then the field $\mathbb{Q}(\theta)$ is a PSL$(2,7)$ septimic extension field of $\mathbb{Q}$ by Lemmas 2.1 and 2.4. By Lemma 3.5 there exist infinitely many positive integers b such that $g(b)$ is squarefree. For these values of b we have by Lemma 3.4 that the field discriminant of $\mathbb{Q}(\theta)$ is equal to $g(b)^2$. It follows that

$$\left\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\right\}$$

is an integral basis for $\mathbb{Q}(\theta)$ proving that $\mathbb{Q}(\theta)$ is monogenic. It remains to show that infinitely many of these monogenic septimic fields are distinct. This follows from the observation that the discriminant equation

$$g(b) = \pm g(t)$$

has a finite number of solutions b for a fixed value of t. This completes our proof. □

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 2000.
[2] I. Gaál, *Diophantine equations and power integral bases. New Computational Methods*. Birkhauser, Boston, 2002.
[3] M.-N. Gras, *Non-monogénéité de l'anneau des entiers des extensions cycliques de Q de degré premier $l \geq 5$*. J. Number Theory **23** (1986), 347–353.
[4] C. U. Jensen, A. Ledet, N. Yui, *Generic Polynomials, constructive aspects of Galois theory, MSRI Publications*. Cambridge University Press, 2002.

[5] M. J. Lavallee, B. K. Spearman, K. S. Williams, and Q. Yang, *Dihedral quintic fields with a power basis*. Mathematical Journal of Okayama University, vol. **47** (2005), 75–79.
[6] Y. Motoda, T. Nakahara and K. H Park, *On power integral bases of the 2-elementary abelian extension fields*. Trends in Mathematics, Information Center for Mathematical Sciences, Volume **8** (June 2006), Number 1, 55–63.
[7] M. Nair, *Power free values of polynomials*. Mathematika **23** (1976), 159–183.
[8] B. K. Spearman, A. Watanabe and K. S. Williams, *PSL(2,5) sextic fields with a power basis*. Kodai Math. J., Vol. **29** (2006), No. 1, 5–12.
[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*. Third Edition, Springer, 2000.

Melisa J. Lavallee
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada, V1V 1V7
E-mail: melisa.lavallee@ubc.ca

Blair K. Spearman
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada, V1V 1V7
E-mail: blair.spearman@ubc.ca

Qiduan Yang
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada, V1V 1V7
E-mail: qiduan.yang@ubc.ca