An Infinite Family of Non-Abelian Monogenic Number Fields

Ofer Grossman, Dongkwan Kim

November 11, 2015

Abstract

We study non-abelian monogenic algebraic number fields (i.e., non-abelian number fields whose rings of integers have a basis of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for some α). There are numerous results about abelian monogenic number fields, yet for the non-abelian case little is understood. As our main result, we find an infinite family of non-abelian monogenic degree 6 number fields.

1 Introduction

A classic open problem in number theory is to characterize number fields whose rings of integers have the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. We call a number field with such a ring of integers *monogenic.*

The problem of characterizing monogenic fields was proposed by Hasse, and remains an active field of research. While there is no general characterization, progress has been made on low degree cases. For example, in [1, 6] necessary and sufficient conditions for the monogeneity of cubics are presented.

An example of a family of monogenic number fields is the cyclotomic fields. Since the ring of integers of a cyclotomic field is generated by a root of unity, it is monogenic. Cyclotomic fields also have the property that they are *abelian* (they are Galois extensions and their Galois groups are abelian). The Kronecker-Weber theorem states that all abelian number fields are subfields of cyclotomic fields. We would like to study other cases of Galois extensions with a power integral basis, so we will study non-abelian extensions.

We start off with some definitions.

Definition 1.1. We call a number field K *monogenic* if its ring of integers $\mathcal{O}_K$ has a basis of the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. We call the set $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ a *power integral basis.*

Definition 1.2. We call a number field *non-abelian* if it is Galois and its Galois group is non-abelian.

The theory of monogenic fields has been studied in depth by Gaál and Grás. Gaál's book [5] contains results pertaining to lower degree monogenic extensions. Specifically, it focuses on computational methods to calculate the power integral basis. The book uses these algorithms to discuss computational methods of finding solutions to Diophantine equations.

Grás, in [7], proves that cyclic extensions of prime degree $p \geq 5$ are either non-monogenic or are the maximal real subfield of some cyclotomic field.

In [6], Grás proves that for n relatively prime to 6, there are only finitely many abelian monogenic fields of degree n.

Although much progress has been made in analyzing and classifying abelian monogenic fields, not much progress has been made on non-abelian monogenic number fields. We make progress by finding an infinite family of degree six non-abelian monogenic fields, thus proving the following theorem:

Theorem 1.3 (Main Theorem)**.** *There exists infinitely many non-abelian monogenic number fields. Specifically, there exists an infinite family of monogenic non-abelian fields of Galois group S_3.*

We also make progress on a problem with a long line of research. The problem is to characterize all groups G which have infinitely many monogenic sextic (degree 6) fields with Galois group G. Progress has been made on finding specific Galois groups for which there are infinitely many monogenic sextic fields. In [4], Eloff, Daniel and Spearman find a family of infinitely many monogenic sextics with Galois group A_4. In [9] Spearman, Watanabe, and Williams show that there exist infinitely many monogenic degree 6 number fields with Galois group $PSL(5, 2)$. In [8], Lavalee finds families of monogenic sextic fields, including infinitely many monogenic sextic fields with Galois groups $D_6, A_4, (S_4, +), A_4 \times C_2, S_4 \times C_2$. We further improve upon this result by finding an infinite family of monogenic degree 6 fields with Galois group S_3. Finding an infinite family of sextic number fields with other Galois groups remains an open problem. Note that none of the previous groups had order 6, so our result is the first infinite family of monogenic sextic number fields which are Galois.

Our results may have applications to breaking fully homomorphic encryption protocols which rely on the assumption that ring learning with errors (RLWE) is hard. In [3], an attack on specific instances of RLWE is proposed, and it is posed as a problem to find non-abelian monogenic number fields of cryptographic size.

We hope our results will inspire more work on non-abelian monogenic fields.

2 Preliminaries

In this section we present various results which we will later use to prove the main theorem (Theorem 1.3).

Theorem 2.1 (Conductor-Discriminant Formula)**.** *For any two number fields $A \subset B$, we have* $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

Proof. See Proposition 4.4.8 in [2]. □

Theorem 2.2 (Dedekind)**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field, $T \in \mathbb{Z}[x]$ the monic minimal polynomial of α, and let p be a prime number. Let $\overline{f}$ denote the reduction of f modulo p. Let*

$$\overline{T}(x) = \prod_{i=0}^{k} \overline{t_i}(x)^{e_i}$$

be the factorization of T modulo p. Let

$$G(x) = \prod_{i=0}^{k} t_i(x),$$

where the t_i are arbitrary monic lifts of $\overline{t_i}$.

Let $H(X) \in \mathbb{Z}[x]$ be a monic lift of $\overline{T}(X)/\overline{G}(X)$ and set $F(X) = (G(X)H(X) - T(X))/p \in \mathbb{Z}[x]$ Then $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is not divisible by p if and only if

$$(\overline{F}, \overline{G}, \overline{H}) = 1$$

in $\mathbb{F}_p[X]$.

Proof. See Theorem 6.1.4 in [2]. □

The following theorem gives a sufficient condition for monogeneity.

Theorem 2.3 (Discriminant Test)**.** *Let $f(x)$ be a polynomial with integer coefficients and $K = \mathbb{Q}[x]/f(x)$. If* $\mathrm{disc}(f) = \mathrm{disc}(K)$, *then K is monogenic.*

Proof. We know that the discriminant of $f(x)$ is the discriminant of $\mathbb{Z}[\alpha]$, where α is a root of $f(x)$. We also know that $\mathcal{O}_K$ contains α, and therefore contains $\mathbb{Z}[\alpha]$.

We now have that $\mathrm{disc}(\mathbb{Z}[\alpha]) = \mathrm{disc}(K)[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$. Since the discriminants are equal, we have $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$, and therefore the two rings are equal. Subsequently, it follows that α generates the ring $\mathcal{O}_K$. □

Theorem 2.4. *The Galois group of a cubic $f(x)$ is S_3 if and only if* $\mathrm{disc}(f)$ *is not a square.*

3 A Family of Non-Abelian Monogenic Sextic Number Fields

In this section, we show that infinitely many polynomials of the form $x^6 + 3x^5 + ax^4 + (2a - 5)x^3 + ax^2 + 3x + 1$ are non-abelian and monogenic. In the first subsection we find a for which the polynomial is irreducible. In the next subsection we find a for which the splitting field of the polynomial is non-abelian. Specifically, we show that the Galois group is S_3. In the last subsection we show the splitting field is monogenic, completing the proof.

3.1 Proving Irreducibility

We let

$$\begin{aligned} f_a(x) &= x^6 + 3x^5 + ax^4 + (2a - 5)x^3 + ax^2 + 3x + 1 \\ g_a(x) &= x^3 + (a - 6)x - (a - 6). \end{aligned}$$

Using a computer algebra system, we calculate that the discriminants of $f_a(x)$ and $g_a(x)$, are $-(4a + 3)^3(a - 6)^4$, and $-(4a + 3)(a - 6)^2$, respectively.

Lemma 3.1. *If $a - 6$ is square-free, then $g_a(x)$ is irreducible.*

Proof. $g_a(x)$ is a cubic. Thus, if it is reducible, then one of its factors will be linear, and it will have an integer root. Let that root be r.

Let p be a prime dividing $a - 6$. Since $a - 6$ is square-free, p divides $a - 6$ exactly once. If r is a root of $g_a(x)$, then p must divide r. But then the terms r^3 and $(a - 6)r^2$ will be divisible by p^2, while $a - 6$ will not, so $g_a(x)$ has no roots modulo p^2. Therefore, as long as $a - 6$ is square-free and different from ±1, the polynomial $g_a(x)$ is irreducible.

We can check the case $a - 6 = \pm 1$ and see that in those cases g_a is irreducible, completing the proof. □

Lemma 3.2. *If $-(4a + 3)$ is not a square, and $a \neq -2, 6$, then $f_a(x)$ is irreducible*

Proof. Suppose $f_a(x)$ is reducible. It cannot have a linear factor since $f_a(1), f_a(-1)$ are nonzero. We let $F_a(x)$ be the factor with smallest degree.

First, assume the degree of $F_a(x)$ is 2. Let b be a root of $f_a(x)$. Then $\mathbb{Q}[b] = \mathbb{Q}[1/b]$ is a degree 2 extension. However, because $-g_a(-1 - x - 1/x)x^3 = f_a(x)$, and 0 is not a root of $f_a(x)$, we know that $-g_a(-b - 1/b - 1) = 0$. Because $g_a(x)$ is irreducible, $\mathbb{Q}[-b - 1/b - 1]$ is an extension of degree 3. This is impossible because $\mathbb{Q}[-b - 1/b - 1]$ is a subfield of $\mathbb{Q}[b]$, which we have shown is an extension of degree 2.

Now we assume the degree of $F_a(x)$ is 3. Note that if $f(r) = 0$, then also $f(1/r) = 0$. We let the roots of $f_a(x)$ be $r_1, r_2, r_3, r_1^{-1}, r_2^{-1}, r_3^{-1}$. We know that the roots of $F_a(x)$ must multiply to ±1. Therefore, they cannot contain a pair of inverse roots r and r^{-1}. Therefore, without loss of generality, we may assume the roots of $F_a(x)$ are r_1, r_2, r_3. It follows that either there exist b and c such that

$$\begin{aligned} F_a(x) &= x^3 + bx^2 + cx + 1 \\ G_a(x) &= x^3 + cx^2 + bx + 1, \end{aligned}$$

or

$$F_a(x) = x^3 + bx^2 + cx - 1$$
$$G_a(x) = x^3 - cx^2 - bx - 1.$$

We first deal with the case $F_a(x) = x^3 + bx^2 + cx + 1$ and $G_a(x) = x^3 + cx^2 + bx + 1$.

Comparing coefficients in $F_a(x)G_a(x) = f_a(x)$ results in the identities:

$$b + c = 3$$
$$bc + b + c = a$$
$$b^2 + c^2 + 2 = 2a - 5.$$

We now see $bc = a - 3$, and therefore $b^2 + c^2 - 2bc + 2a - 6 = 2a - 7$, and therefore $(b - c)^2 = -1$, a contradiction.

We now deal with the case $F_a(x) = x^3 + bx^2 + cx - 1$ and $G_a(x) = x^3 - cx^2 - bx - 1$.

We get the identities

$$b - c = 3$$
$$-bc + c - b = a$$
$$-b^2 - c^2 - 2 = 2a - 5.$$

The first two equations imply that $-bc = a - 3$. Therefore, $-b^2 - c^2 - 2 - 2bc - 2a - 6 = 2a - 5$, and therefore $-(b + c)^2 = 4a + 3$. This is impossible because $-(4a + 3)$ is not a square. □

3.2 Finding the Galois Group

In this section, we show that the field $\mathbb{Q}[x]/f_a(x)$ is a non-abelian number field. We will do this by showing that the polynomial $g_a(x)$ has Galois group S_3 and that its splitting field is the same as the splitting field of $f_a(x)$.

Lemma 3.3. *$\mathbb{Q}[x]/f_a(x)$ is Galois.*

Proof. We will show that from one of the roots of $f_a(x)$, we can generate all of the roots.

Let one of the roots be r. We see that the rest of the roots of $f_a(x)$ are $-(r + 1), 1/r, -1/(r + 1), -(1/r + 1), -1/(1/r + 1)$. This can be verified with a computer algebra system. Note that all these roots are distinct, and therefore these are all of the roots of $f_a(x)$. Therefore, one of the roots of $f_a(x)$ generates all of the roots, and it follows that $\mathbb{Q}[x]/f_a(x)$ is Galois. □

Theorem 3.4. *If $f_a(x)$ and $g_a(x)$ are irreducible, and $4a + 3$ is not a square, then $\mathbb{Q}[x]/f_a(x)$ is non-abelian.*

Proof. We let the roots of $f_a(x)$ be $r_1, r_2, r_3, r_1^{-1}, r_2^{-1}, r_3^{-1}$. Then the polynomial $g_a(x)$ has roots $-r_1 - r_1^{-1} - 1, -r_2 - r_2^{-1} - 1$, and $-r_3 - r_3^{-1} - 1$. We can see this is true because $g_a(-1 - x - 1/x)x^3 = f_a(x)$, and 0 is not a root of $f_a(x)$. Therefore, $\mathbb{Q}[x]/g_a(x)$ is a subfield of the field $\mathbb{Q}[x]/f_a(x)$.

Now, if we show that the Galois group of the splitting field of $g_a(x)$ is S_3, then we will be done because we know that the splitting field of g_a is contained in the splitting field of $f_a(x)$ which is of degree 6. To show the Galois group of the splitting field of $g_a(x)$ is S_3, we use a computer algebra system to find the discriminant of $g_a(x)$ in terms of a, and see that it is $-(4a + 3)^3(a - 6)^4$. Since we have assumed that $4a + 3$ is not a square, by Theorem 2.4 it follows that the Galois group is S_3. Therefore $\mathbb{Q}[x]/f_a(x)$ is non-abelian. □

3.3 Proof of Monogeneity

In the previous sections, we found a for which $f_a(x)$ is irreducible, and we showed that for such a $\mathbb{Q}[x]/f_a(x)$ has Galois group S_3. In this section, we find a for which $\mathbb{Q}[x]/f_a(x)$ is monogenic.

We let $K = \mathbb{Q}[x]/f_a(x)$, and $L = \mathbb{Q}[x]/g_a(x)$.

Lemma 3.5. *Suppose $a-6$ is square-free. If $g_a(\alpha) = 0$, then $\gcd([\mathcal{O}_L : \mathbb{Z}[\alpha]], a-6) = 1$.*

Proof. The theorem follows from Theorem 2.2 by setting $T(x) = g_a(x)$ and letting p be some prime divisor of $a-6$. Then $\overline{T}(x) = x^3$, so $\overline{G}(x) = x$.

We now have $F(x) = (x^3 - T(x))/p = \frac{-(a-6)x+(a-6)}{p}$.

We now find that $(\overline{F}, \overline{G}, \overline{H}) = (a-6)/p$ which is a unit in $\mathbb{F}_p$ since p divides $a-6$ exactly once when $a-6$ is square-free. Therefore, $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ is not divisible by p for all p that divide $a-6$, so $\gcd([\mathcal{O}_L : \mathbb{Z}[\alpha]], a-6) = 1$. □

We know that $\frac{\operatorname{disc}(g_a)}{\operatorname{disc}(L)}$ is a square, since $\frac{\operatorname{disc}(g_a)}{\operatorname{disc}(L)} = [\mathcal{O}_L : \mathbb{Z}[\alpha]]^2$, where α is a root of $g_a(x)$. Therefore, because $\operatorname{disc}(g_a) = -(4a+3)(a-6)^2$, if $4a+3$ is square-free, using Lemma 3.7, $\operatorname{disc}(L) = \operatorname{disc}(g_a) = -(4a+3)(a-6)^2$. Therefore, by the conductor-discriminant formula (Theorem 2.1), it follows that $(4a+3)^2(a-6)^4|\operatorname{disc}(K)$. We know that $\operatorname{disc}(f_a) = -(4a+3)^3(a-6)^4$. Therefore, $\frac{\operatorname{disc}(f_a)}{\operatorname{disc}(K)}$ divides $4a+3$, so $\frac{\operatorname{disc}(f_a)}{\operatorname{disc}(K)}$ is square-free. However, we know that $\frac{\operatorname{disc}(f_a)}{\operatorname{disc}(K)} = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2$, where β is a root of f_a. Therefore, because the right side is square-free, both sides must equal 1.

We now have the following lemma.

Lemma 3.6. *If $a-6$ and $4a+3$ are both square-free, then $\operatorname{disc}(K) = \operatorname{disc}(f_a) = -(4a+3)^3(a-6)^4$, and therefore by the discriminant test (Theorem 2.3), K is monogenic.*

We will now show that the density of a such that both $a-6$ and $4a+3$ are square-free is positive.

Lemma 3.7. *As a approaches infinity, the fraction of a for which both $a-6$ and $4a+3$ are square-free is always greater than some positive constant.*

Proof. The density of n such that n is square-free approaches $d = \zeta(2)^{-1} \approx 0.608$ [**?**]. It follows that d fraction of our choices for a would make $a-6$ square-free.

The density numbers of the form $4a$ that are square-free is 0, since $4a$ is divisible by 2^2. The maximal possible density of square-free numbers of the form $4a+1$ and $4a+2$ is 1. We let x be the lim inf of the number of square-free numbers of the form $4a+3$, for $0 < a < A$, divided by A. (The intuition is to let x be the density of square-free numbers of the form $4a+3$; however, we don't know whether such a density exists in the limit, so we consider the lower bound). Taking the average density and using the fact that $.6 < d$ gives

$$.6 < d \leq \frac{0+1+1+x}{4} = .5 + x/4.$$

Therefore, x must be greater than .4. However, if .4 of the integers of the form $4a+3$ are square-free, and d of the integers of the form $a-6$ are square-free integers since $d + .4 > 1$, the lim inf of the density of a such that both $4a+3$ and $a-6$ are square-free must be positive. □

In summation, we have the following theorem:

Theorem 3.8. *There exist infinitely many polynomials of the form $x^6 + 3x^5 + ax^4 + (2a - 5)x^3 + ax^2 + 3x + 1$ that are irreducible, non-abelian, and monogenic.*

This in turn implies the following theorem:

Theorem 3.9 (Main Theorem)**.** *There exists infinitely many non-abelian monogenic number fields.*

4 Conclusion, Open Problems and Further Research

We have found an infinite family of monogenic non-abelian number fields, proving that infinitely many such fields exist. This evidence leads us to suspect that such families could be found for higher degrees as well. We conjecture that such families exist for all symmetric Galois groups.

It is an open problem to determine whether there exist monogenic non-abelian fields of arbitrarily high degree. Finding such a family of polynomials may be helpful in showing that ring learning with errors is not hard on all rings, which could help break various fully homomorphic encryption protocols [3].

It is also still open to classify all Galois groups G that have infinitely many monogenic sextic fields with Galois group G. So far, monogenic sextics with Galois groups $A_4, D_6, A_4, (S_4, +), A_4 \times C_2, S_4 \times C_2, PSL(5, 2)$ and S_3 have been found. Classifying the other possible Galois groups remains open.

Acknowledgments

We would like to thank David Jerison, Ankur Moitra, and Andrew Sutherland for helpful discussions.

References

[1] Gabriel Archinard. Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogène. *Enseignement Math*, 20(2):179–191, 1974.

[2] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag New York, Inc., New York, NY, USA, 1993.

[3] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Ring-lwe cryptography for the number theorist. Cryptology ePrint Archive, Report 2015/758, 2015. http://eprint.iacr.org/.

[4] Daniel Eloff, Blair K Spearman, and Kenneth S Williams. a_4-sextic fields with a power basis. *Missouri J. Math. Sci*, 19:188–194, 2007.

[5] István Gaál. *Diophantine equations and power integral bases.* Springer Science+Business Media, LLC, 2002.

[6] Marie-Nicole Grás. Sur les corps cubiques cycliques dont lanneau des entiers est monogène. *CR Acad. Sci. Paris Sér. A*, 278:59–62, 1974.

[7] Marie-Nicole Grás. Non monognit de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degr premier $l \geq 5$. *J. Number Theory*, 23(3), 1986.

[8] Melisa J Lavallee, Blair K Spearman, and Kenneth S Williams. Lifting monogenic cubic fields to monogenic sextic fields. *Kodai Mathematical Journal*, 34(3):410–425, 2011.

[9] Blair K Spearman, Aya Watanabe, and Kenneth S Williams. Psl (2, 5) sextic fields with a power basis. *Kodai Mathematical Journal*, 29(1):5–12, 2006.