ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 47, Number 3, 2017

NON-MONOGENITY IN A FAMILY OF OCTIC FIELDS

ISTVÁN GAÁL AND LÁSZLÓ REMETE

ABSTRACT. Let m be a square-free integer, $m \equiv 2, 3 \pmod 4$. We show that the number field $K = \mathbb{Q}(i, \sqrt[4]{m})$ is non-monogene, that is, it does not admit any power integral bases of type $\{1, \alpha, \dots, \alpha^7\}$. In this infinite parametric family of Galois octic fields we construct an integral basis and show non-monogenity using congruence considerations only.

Our method yields a new approach to consider monogenity or to prove non-monogenity in algebraic number fields which is applicable for parametric families of number fields. We calculate the index of elements as polynomials dependent upon the parameter, factor these polynomials, and consider systems of congruences according to the factors.

1. Introduction. Let K be a number field of degree n with a ring of integers $\mathbb{Z}_K$. It is called *monogene* if there is an $\alpha \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, that is, $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an integral basis of K. Such an integral basis is called a *power integral basis*. Monogenity of number fields and calculation of generators of power integral bases is a classical topic of algebraic number theory, cf., [**8, 18**]. There are efficient algorithms for calculating the monogenity of lower degree number fields and the generators of power integral bases [**1, 9, 11, 14**]. However, we only have partial results for higher degree fields [**6, 7, 10, 19**]. The problem is particularly challenging if we try to answer this question in an infinite parametric family of number fields, cf., e.g., [**12, 15**].

Chang [**2**] studied the fields $L = \mathbb{Q}(\omega, \sqrt[3]{m})$, where $\omega = e^{2\pi i/3}$ and m is a square-free integer. He calculated the relative index of an element of L, cf., [**8**]. He did not determine the elements of relative index 1 but used this relation for further calculations of the index. He showed that

2010 AMS *Mathematics subject classification.* Primary 11R04, 11Y50.

Keywords and phrases. Power integral basis, octic fields, relative quartic extension.

Research supported in part by the Hungarian National Foundation for Scientific Research, grant No. K115479.

Received by the editors on June 11, 2015, and in revised form on August 3, 2015.

DOI:10.1216/RMJ-2017-47-3-817

there are no power integral bases in L. This field L is Galois, which simplified some calculations.

This result prompted the immediate consideration of the octic family of fields of type $K = \mathbb{Q}(i, \sqrt[4]{m})$. The analogous method failed when calculating the relative index in our quartic case because it is much more complex than the cubic case. We followed a direct method of calculating the index of elements of K, explicitly calculating the index form and its factors. Using only congruence considerations, we showed:

Theorem 1.1. *Letting m be a square-free integer $m \equiv 2, 3 \pmod 4$, the field $K = \mathbb{Q}(i, \sqrt[4]{m})$ is not monogene.*

Our proof involves calculations performed with `Maple` and a total of eight parameters using complicated formulas dependent on m and the coefficients of the elements in the integral basis. In order to perform these calculations we only considered the cases $m \equiv 2, 3 \pmod 4$. Note that, for $m \equiv 2, 3 \pmod 4$, the elements $\{1, \vartheta, \vartheta^2, \vartheta^3\}$ form an integral basis in $L = \mathbb{Q}(\vartheta)$ (with $\vartheta = \sqrt[4]{m}$), see [**16**]. The integral basis of L is also known for other values of m, [**5, 17**], but, in those cases, the integral basis of L also depends upon other parameters; m is written in the form $m = ab^2c^3$ where a, b and c are square-free and pairwise prime. This would make the integral basis of K, and also all of our formulas, much more complicated, for which our method is nearly impossible to perform.

Previously, we determined the generators of relative power integral bases of K over L and considered one or two additional equations to calculate the generators of power integral bases of K, cf., sextic and octic fields with quadratic subfields [**8**].

The novelty of our present method is that we do not explicitly calculate the generators of relative integral bases of K over L. Further, instead of two or three factors of the index form, here we use as many factors as possible, a total of six. We calculate the index of elements as polynomials depending upon the parameter, factor these polynomials and consider a system of congruences according to the factors.

The straightforward method of our calculations may also be useful in other parametric families of number fields.

2. An integral basis of K. In parametric families, especially in higher degree number fields, say, for degrees > 4, it is difficult to determine an integral basis in a parametric form. Sometimes we succeed in constructing an integral basis, cf., e.g., **[12]**; if not, the problem remains interesting for an order of the field, cf., e.g., **[10, 15]**. In the present case, we have:

Theorem 2.1. *Let m be a square-free integer, $\vartheta = \sqrt[4]{m}$, and let $K = \mathbb{Q}(i, \vartheta)$. If $m \equiv 2 \pmod 4$, then an integral basis of K is*

$$\left\{1, \vartheta, \vartheta^2, \vartheta^3, i, \frac{(1+i)\vartheta + \vartheta^3}{2}, \frac{(1+i)\vartheta^2}{2}, \frac{(1+i)\vartheta^3}{2}\right\}, \tag{2.1}$$

and the discriminant of K is

$$D_K = 2^{18} m^6.$$

If $m \equiv 3 \pmod 4$, then an integral basis of K is

$$\left\{1, \vartheta, \vartheta^2, \vartheta^3, \frac{i+\vartheta^2}{2}, \frac{i\vartheta+\vartheta^3}{2}, \frac{1+i\vartheta^2}{2}, \frac{\vartheta+i\vartheta^3}{2}\right\}, \tag{2.2}$$

and the discriminant of K is

$$D_K = 2^{16} m^6.$$

Proof of Theorem 2.1. Set $M = \mathbb{Q}(i)$ and $L = \mathbb{Q}(\vartheta)$. For $m \equiv 2, 3 \pmod 4$, $\{1, \vartheta, \vartheta^2, \vartheta^3\}$ is an integral basis in L, see **[16]**, with discriminant $D_L = -256m^3$. The relative discriminant of K over L is denoted by $D_{K/L}$. We have

$$D_K = N_{L/\mathbb{Q}}(D_{K/L}) D_L^2, \tag{2.3}$$

which implies that D_K is divisible by $2^{16}m^6$.

There are several classical methods for calculating the integral basis of number fields which work for specific fields but not necessarily for parametric families of fields. In order to construct the integral basis we used the algorithm described by Cook **[4]**. We began with the initial basis

$$\{b_1 = 1, b_2 = \vartheta, b_3 = \vartheta^2, b_4 = \vartheta^3, b_5 = i, b_6 = i\vartheta, b_7 = i\vartheta^2, b_8 = i\vartheta^3\},$$

and calculated the discriminant of this basis as $D = 2^{24}m^6$. Comparing it with (2.3), we can see that

$$D_K = 2^h m^6,$$

with $16 \le h \le 24$.

According to the algorithm of [**4**], we began exchanging the original basis elements with new candidates of basis elements. Our purpose was to diminish $D = 2^{24}m^6$ by a power of 2; thus, only 2 may appear in the denominator. The numerator is a linear combination of the basis elements with coefficients 0 or 1, that is, we constructed elements of the type

$$b = \frac{\lambda_1 b_1 + \cdots + \lambda_8 b_8}{2}, \tag{2.4}$$

with $\lambda_i \in \{0, 1\}$.

The parameter m is either $4n + 2$ or $4n + 3$. We selected those coefficient tuples $(\lambda_1, \ldots, \lambda_8)$ which were appropriate for a new basis element in the following way. We let n run through all residues modulo 64 to check whether the norm of $\lambda_1 b_1 + \cdots + \lambda_8 b_8$ is divisible by $2^8 = 256$. Elements b are sufficient such that this was satisfied for all residues of n modulo 64. Then, we calculated the defining polynomial of b in a parametric form to verify that it is indeed an algebraic integer. Finally, we replaced a basis element by b and calculated the discriminant of the new basis, which must be smaller than the discriminant of the previous basis.

In the case $m = 4n + 2$, the procedure terminated with the observation that no coefficient tuples $(\lambda_1, \ldots, \lambda_8)$ were suitable (the norm of $\lambda_1 b_1 + \cdots + \lambda_8 b_8$ divisible by $2^8 = 256$) for any residues n modulo 64.

In the case $m = 4n + 3$, the discriminant of our basis reached the lower bound $2^{16}m^6$. □

3. Calculating the index of elements.

Proof of Theorem 1.1. Letting $\omega = i$, we have $\vartheta = \sqrt[4]{m}$. Set $\omega^{(1,k)} = i$, $\omega^{(2,k)} = -i$, $1 \le k \le 4$, and let $\vartheta^{(j,k)} = i^{k-1}\sqrt[4]{m}$ for $j = 1, 2$, $1 \le k \le 4$. Let $\{b_1 = 1, b_2, \ldots, b_8\}$ be the integral basis

of Theorem 2.1. We represent α in the form

$$\alpha = x_1 + x_2 b_2 + \cdots x_8 b_8,$$

with $x_1, \ldots, x_8 \in \mathbb{Z}$. Let $\alpha^{(j,k)}$ be the conjugate of any $\alpha \in K$ corresponding to $\vartheta^{(j,k)}$. This may be calculated by using the conjugates of ω and ϑ and the explicit form of $b_2, \ldots, b_8$.

For any primitive element $\alpha \in \mathbb{Z}_K$, the *index* of α, cf., [**8**], is

$$I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+) = \sqrt{\frac{|D(\alpha)|}{|D_K|}}, \tag{3.1}$$

where $D(\alpha)$ is the discriminant of α. We split $D(\alpha)$ into several factors. Let

$$\begin{aligned}
S_1 &= N_{M/\mathbb{Q}}((\alpha^{(j,1)} - \alpha^{(j,2)})(\alpha^{(j,2)} - \alpha^{(j,3)})(\alpha^{(j,3)} - \alpha^{(j,4)})(\alpha^{(j,4)} - \alpha^{(j,1)})),\\
S_2 &= N_{M/\mathbb{Q}}((\alpha^{(j,1)} - \alpha^{(j,3)})(\alpha^{(j,2)} - \alpha^{(j,4)})),\\
S_3 &= (\alpha^{(1,1)} - \alpha^{(2,1)})(\alpha^{(1,2)} - \alpha^{(2,2)})(\alpha^{(1,3)} - \alpha^{(2,3)})(\alpha^{(1,4)} - \alpha^{(2,4)}),\\
S_4 &= (\alpha^{(1,1)} - \alpha^{(2,4)})(\alpha^{(1,2)} - \alpha^{(2,1)})(\alpha^{(1,3)} - \alpha^{(2,2)})(\alpha^{(1,4)} - \alpha^{(2,3)}),\\
S_5 &= (\alpha^{(1,1)} - \alpha^{(2,3)})(\alpha^{(1,2)} - \alpha^{(2,4)})(\alpha^{(1,3)} - \alpha^{(2,1)})(\alpha^{(1,4)} - \alpha^{(2,2)}),\\
S_6 &= (\alpha^{(1,1)} - \alpha^{(2,2)})(\alpha^{(1,2)} - \alpha^{(2,3)})(\alpha^{(1,3)} - \alpha^{(2,4)})(\alpha^{(1,4)} - \alpha^{(2,1)}).
\end{aligned}$$

The polynomials $S_1, \ldots, S_6$ have integer coefficients, which depend on m, $x_2, \ldots, x_8$, but are independent from x_1.

Case 1: $m = 4n + 2$. We substitute $m = 4n + 2$ into $S_1, \ldots, S_6$. We factor the products and find

$$\begin{aligned}
S_1 &= 16(2n+1)^2 Q_1,\\
S_2 &= 16(2n+1) Q_2,\\
S_3 &= 2Q_3,\\
S_4 &= 2Q_4,\\
S_5 &= 2Q_5,\\
S_6 &= 2Q_6,
\end{aligned}$$

where $Q_1, \ldots, Q_6$ are also polynomials with integer coefficients. Therefore, we have

$$S_1 \cdots S_6 = 2^9 (4n+2)^3 Q_1 \cdots Q_6 = \sqrt{|D_K|} Q_1 \cdots Q_6.$$

Hence, by (3.1) and Theorem 2.1, we have $I(\alpha) = Q_1 \cdots Q_6$; therefore, $I(\alpha) = 1$ is equivalent to

$$Q_i = Q_i(x_2, \ldots, x_8, n) = \pm 1, \quad i = 1, \ldots, 6. \tag{3.2}$$

We calculate

$$Q_4 - Q_6 + Q_3 - Q_5 \mod 16,$$

and find that this is $= 8$ (independently from the variables). This is impossible, since $Q_i \mod 16$ must be 1 or 15 for all i. This proves the theorem in Case 1.

Case 2: $m = 4n+3$. Again, we substitute $m = 4n+3$ into $S_1, \ldots, S_6$. By factoring the products, we find

$$\begin{aligned} S_1 &= (4n+3)^2 Q_1, \\ S_2 &= 16(4n+3)Q_2, \\ S_3 &= Q_3, \\ S_4 &= 4Q_4, \\ S_5 &= Q_5, \\ S_6 &= 4Q_6, \end{aligned}$$

where $Q_1, \ldots, Q_6$ are also polynomials with integer coefficients. Therefore, we have

$$S_1 \cdots S_6 = 2^8(4n+3)^3 Q_1 \cdots Q_6 = \sqrt{|D_K|} Q_1 \cdots Q_6.$$

Hence, by (3.1) and Theorem 2.1, we have $I(\alpha) = Q_1 \ldots Q_6$; therefore, $I(\alpha) = 1$ is equivalent to

$$Q_i = Q_i(x_2, \ldots, x_8, n) = \pm 1, \quad i = 1, \ldots, 6. \tag{3.3}$$

We consider all possible cases according to whether $x_2, \ldots, x_8$ and n are even or odd, that is, we substitute

$$x_i = 2t_i, 2t_i + 1, \quad i = 2, \ldots, 8, \ n = 2t_9, 2t_9 + 1,$$

into $Q_1, \ldots, Q_6$, and in all 2^8 cases, we calculate their residues modulo 4. By (3.3), this must be 1 or 3. Further, Q_1, Q_3, $Q_5 \mod 8$ must be 1 or 15 and $Q_6 - Q_4 \mod 8$ must be 0, 2 or 6. Note that all of these residues are independent from the parameters $t_2, \ldots, t_9$, as this occurs in all subsequent residues without further comment.

For the cases that have passed this test, we further considered Q_1 modulo 16. In all of the cases satisfying these conditions, we found that x_5 is even and x_7 is odd, which made it possible to reduce the number of possible cases.

For the remaining cases, we considered Q_2, Q_4, Q_6 mod 4 (must be 1 or 3), Q_1, Q_3, Q_5 mod 8 (must be 1 or 7), and $Q_6 - Q_4$ mod 8 (must be 0, 2 or 6). In the suitable cases, we used $Q_3 - Q_5$ mod 16, which must be 0, 2 or 14. The values obtained were 0 and 8, which implies $Q_3 \equiv Q_5$ mod 16. In all four suitable cases, we used Q_5 mod 16 and always obtained

$$8t_5^2 + 8t_7^2 + 8t_7 + 9 = 8t_7(t_7 + 1) + 8t_5^2 + 9 \equiv 8t_5^2 + 9 \bmod 16.$$

This implies that t_5 is even but not divisible by 4, that is, $t_5 = 4t_5' + 2$.

In the cases satisfying all conditions, we found that we always obtained x_6 and x_8 even. Using these additional conditions in the remaining suitable cases, we printed $Q_5 - Q_3$ mod 32 (must be 0, 2 or 30) and $Q_4 - Q_6$ mod 16 (must be 0, 2 or 14). These residues were again independent from the parameters and did not take acceptable values in a parallel manner. This proves the theorem in Case 2. □

4. Computational aspects. All calculations were performed in `Maple` [**3**]. The factors $S_1, \dots, S_6$ of the indices of elements were extremely complicated and were only manageable with `Maple`. It took 1-3 minutes to simplify them using symmetric polynomials to obtain integer coefficients. The modular tests took only a few seconds.

REFERENCES

1. Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields*: *A hard computation*, Acta Arith. **115** (2004), 85–96.

2. Mu-Ling Chang, *Non-monogenity in a family of sextic fields*, J. Numer. Th. **97** (2002), 252–268.

3. B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan and S.M. Watt, *Maple* V *language reference manual*, Springer, New York, 1991.

4. John Paul Cook, *Computing integral bases*, `http://math.ou.edu/~jcook/LaTeX/integralbases.pdf`.

5. T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. **26** (1984), 27–41.

6. I. Gaál, *Power integral bases in composits of number fields*, Canad. Math. Bull. **41** (1998), 158–161.

7. I. Gaál, *Solving index form equations in fields of degree nine with cubic subfields*, J. Symb. Comp. **30** (2000), 181–193.

8. ———, *Diophantine equations and power integral bases*, Birkhäuser, Boston, 2002.

9. I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith. **89** (1999), 379–396.

10. I. Gaál, P. Olajos and M. Pohst, *Power integral bases in orders of composits of number fields*, Exp. Math. **11** (2002), 87–90.

11. I. Gaál, A. Pethő and M. Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms with an application to index form equations in quartic number fields*, J. Numer. Th. **57** (1996), 90–104.

12. I. Gaál and M. Pohst, *Power integral bases in a parametric family of totally real cyclic quintics*, Math. Comp. **66** (1997), 1689–1696.

13. I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by solving relative Thue equations*, Tatra Math. Publ. **59** (2014), 79-92.

14. I. Gaál and N. Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp. **53** (1989), 689–696.

15. I. Gaál and T. Szabó, *Power integral bases in parametric families of biquadratic fields*, J. Alg. Numer. Th. App. **21** (2012), 105–114.

16. A. Hameed, T. Nakahara, S.M. Husnine and S. Ahmad, *On the existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Res. Math. **7** (2011), 19–24.

17. J.G. Huard, B.K. Spearman and K.S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Numer. Th. **51** (1995), 87–102.

18. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Second edition, Springer, New York, 1974.

19. P. Olajos, *Power integral bases in orders of composite fields* II, Ann. Univ. Sci. Budapest **46** (2003), 35–41.

University of Debrecen, Mathematical Institute, H-4010 Debrecen Pf.12., Hungary
Email address: **gaal.istvan@unideb.hu**

University of Debrecen, Mathematical Institute, H-4010 Debrecen Pf.12., Hungary
Email address: **remete.laszlo@science.unideb.hu**