

# Non-monogeneity in a family of octic fields

István Gaál\*, and László Remete

University of Debrecen, Mathematical Institute  
H-4010 Debrecen Pf.12., Hungary  
e-mail: gaal.istvan@unideb.hu, remetel42@gmail.com

September 28, 2018

## Abstract

Let  $m$  be a square-free positive 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-monogeneity using only congruence considerations.

Our method yields a new approach to consider monogeneity or to prove non-monogeneity in algebraic number fields. It is well applicable in parametric families of number fields. We calculate the index of elements as polynomials depending on the parameter, factor these polynomials and consider systems of congruences according to the factors.

---

\*Research supported in part by K115479 from the Hungarian National Foundation for Scientific Research

2010 *Mathematics Subject Classification*: Primary 11R04; Secondary 11Y50

*Key words and phrases*: power integral basis, octic fields, relative quartic extension

# 1 Introduction

Let  $K$  be a number field of degree  $n$  with 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 *power integral basis*. Monogeneity of number fields and the calculation of generators of power integral bases is a classical topic of algebraic number theory cf. [18], [8]. For lower degree number fields there are efficient algorithms to decide the monogeneity of the field and to calculate the generators of power integral bases [14],[11], [9], [1]. However, for higher degree fields we only have partial results [6], [7], [10], [19].

The problem is especially challenging if we try to answer this question in an infinite parametric family of number fields cf. e.g. [12], [15].

M.-L. Chang [2] studied the fields  $L = \mathbb{Q}(\omega, \sqrt[3]{m})$  where  $\omega = e^{2\pi i/3}$  and  $m$  a square-free positive integer. He calculated the relative index (cf. [8]) of an element of  $L$ , did not determine the elements of relative index 1, but used this relation for further calculations of the index. He showed there are no power integral bases in  $L$ . This field  $L$  is Galois which made some calculations easier.

This result immediately gave the idea to consider the octic family of fields of type  $K = \mathbb{Q}(i, \sqrt[4]{m})$ . The analogous way using the relative index did not work, because in our quartic case it is much more complicated than in the cubic case. We followed a direct way of calculating the index of elements of  $K$ , calculating explicitly the index form and its factors. Using only congruence considerations we showed:

**Theorem 1.** *Let  $m$  be a square-free positive integer,  $m \equiv 2, 3 \pmod{4}$ . Then the field  $K = \mathbb{Q}(i, \sqrt[4]{m})$  is not monogene.*

Our proof involves calculations performed by using Maple with complicated formulas, depending on  $m$  and the coefficients of the elements in the integral basis, all together 8 parameters. In order to be able 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 known also for other values of  $m$  ([5], [17]), but in those cases the integral basis of  $L$  depends also on other parameters, ( $m$  is written in the form  $m = ab^2c^3$  where  $a, b, c$  are square-free and pairwise prime). This would make the inte-

gral basis of  $K$  and also all our formulas much more complicated, for which our method is hardly possible to perform.

Remark that formerly we usually determined the generators of relative power integral bases of  $K$  over  $L$  and considered one or two further equations to calculate the generators of power integral bases of  $K$  (cf. sextic and octic fields with quadratic subfields in [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 we use here as many factors as possible, actually six factors. We calculate the index of elements as polynomials depending on the parameter, factor these polynomials and consider a system of congruences according to the factors.

The straightforward way of our calculations can be useful also 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 a hard question to determine an integral basis in a parametric form. Sometimes we succeed in constructing an integral basis cf. e.g. [12] or if not, the problem is still interesting in an order of the field cf. e.g. [10], [15]. In the present case we have

**Theorem 2.** *Let  $m$  be a square-free positive 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*

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

*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*

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

and the discriminant of  $K$  is

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

**Proof of Theorem 2.** 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  $D_L = -256m^3$ . Denote by  $D_{K/L}$  the relative discriminant of  $K$  over  $L$ . We have

$$D_K = N_{L/\mathbb{Q}}(D_{K/L}) D_L^2. \quad (3)$$

This 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. To construct the integral basis we used the algorithm described by J.P.Cook [3]. We started from 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:  $D = 2^{24}m^6$ . Comparing it with (3) we can see that

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

with  $16 \leq h \leq 24$ .

According to the algorithm of [3] we started to exchange the original basis elements with new candidates of basis elements. Our purpose is to diminish  $D = 2^{24}m^6$  by a power of 2, thus in the denominator only 2 may appear. The numerator is a linear combination of the basis elements with coefficients 0 or 1, that is we constructed elements of type

$$b = \frac{\lambda_1 b_1 + \dots + \lambda_8 b_8}{2} \quad (4)$$

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

The parameter  $m$  is either  $4n + 2$  or  $4n + 3$ . We select those coefficient tuples  $(\lambda_1, \dots, \lambda_8)$  which are appropriate for a new basis element in the following way. We let  $n$  run through all residues modulo 64 to check if the norm of  $\lambda_1 b_1 + \dots + \lambda_8 b_8$  is divisible by  $2^8 = 256$ . Appropriate are those elements  $b$  such that this was satisfied for all residues of  $n$  modulo 64. Then we calculate the defining polynomial of  $b$  (in a parametric form) to check if it is indeed an algebraic integer. Finally we replaced a basis element by  $b$

and calculated the discriminant of the new basis: this must be smaller than the discriminant of the previous basis.

In case  $m = 4n + 2$  the procedure terminated by observing that no coefficient tuples  $(\lambda_1, \dots, \lambda_8)$  were suitable (the norm of  $\lambda_1 b_1 + \dots + \lambda_8 b_8$  divisible by  $2^8 = 256$ ) for none of the residues  $n$  modulo 64.

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

### 3 Calculating the index of elements

**Proof of Theorem 1.** Let  $\omega = i$  and we have  $\vartheta = \sqrt[4]{m}$ . Set  $\omega^{(1,k)} = i, \omega^{(2,k)} = -i$  ( $1 \leq k \leq 4$ ) and let  $\vartheta^{(j,k)} = i^{k-1} \sqrt[4]{m}$  for  $j = 1, 2, 1 \leq k \leq 4$ . Let  $\{b_1 = 1, b_2, \dots, b_8\}$  be the integral basis of Theorem 2. We represent  $\alpha$  in the form

$$\alpha = x_1 + x_2 b_2 + \dots + x_8 b_8$$

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

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

$$I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+) = \sqrt{\frac{|D(\alpha)|}{|D_K|}}, \quad (5)$$

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

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

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

**Case I:**  $m = 4n + 2$ .

We substitute  $m = 4n + 2$  into  $S_1, \dots, S_6$ . 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  $Q_1, \dots, Q_6$  are also polynomials with integer coefficients. Therefore we have

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

Hence by (5) and Theorem 2, we have  $I(\alpha) = Q_1 \dots Q_6$  therefore  $I(\alpha) = 1$  is equivalent to

$$Q_i = Q_i(x_2, \dots, x_8, n) = \pm 1 \quad (i = 1, \dots, 6). \quad (6)$$

We calculate

$$Q_4 - Q_6 + Q_3 - Q_5 \pmod{16}$$

and find that this is equal to 8 (independently from the variables). It is impossible, since  $Q_i \pmod{16}$  must be 1 or 15 for all  $i$ . This proves the theorem in Case I.

**Case II:**  $m = 4n + 3$ .

Again we substitute  $m = 4n + 3$  into  $S_1, \dots, S_6$ . We factor the products and 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  $Q_1, \dots, Q_6$  are also polynomials with integer coefficients. Therefore we have

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

Hence by (5) and Theorem 2, we have  $I(\alpha) = Q_1 \dots Q_6$  therefore  $I(\alpha) = 1$  is equivalent to

$$Q_i = Q_i(x_2, \dots, x_8, n) = \pm 1 \quad (i = 1, \dots, 6). \quad (7)$$

We consider all possible cases according as  $x_2, \dots, x_8$  and  $n$  are even or odd. That is we substitute

$$x_i = 2t_i, 2t_i + 1 \quad (i = 2, \dots, 8), \quad n = 2t_9, 2t_9 + 1$$

into  $Q_1, \dots, Q_6$  and in all these  $2^8$  cases we calculate their residues modulo 4. By (7) this must be 1 or 3. Further  $Q_1, Q_3, Q_5 \pmod 8$  must be 1 or 15 and  $Q_6 - Q_4 \pmod 8$  must be 0, 2 or 6. Note that all these residues are independent from the parameters  $t_2, \dots, t_9$ , as it happens to all further residues we mention without comments.

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

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

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

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 until here we found that we always have  $x_6$  and  $x_8$  even. Using these additional conditions, in the remaining suitable cases we printed  $Q_5 - Q_3 \pmod{32}$  (must be 0, 2 or 30) and  $Q_4 - Q_6 \pmod{16}$  (must be 0, 2 or 14). These residues were again independent from the parameters and did not parallelly take acceptable values. This proves the theorem in Case II.  $\square$

## 4 Computational aspects

All calculations were performed in Maple [4] on an average laptop. The factors  $S_1, \dots, S_6$  of the indices of elements were extremely complicated, only possible to handle with Maple. It took 1-3 minutes to simplify them using symmetric polynomials in order to get integer coefficients. The modular tests took just a few seconds.

## References

- [1] Y.Bilu, I.Gaál and K.Györy, *Index form equations in sextic fields: a hard computation*, Acta Arithm., **115.1** (2004), 85–96.
- [2] Mu-Ling Chang, *Non-monogeneity in a family of sextic fields*, J. Number Theory, **97**(2002), 252–268.
- [3] John Paul Cook, *Computing integral bases*,  
<http://math.ou.edu/~jcook/LaTeX/integralbases.pdf>
- [4] B.W.Char, K.O.Geddes, G.H.Gonnet, B.L.Leong, M.B.Monagan, S.M.Watt, *Maple V - language reference manual*, Springer, 1991.
- [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 composites 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. Symbolic Comput., **30**(2000), 181–193.
- [8] I.Gaál, *Diophantine equations and power integral bases*, Boston, Birkhäuser, 2002.
- [9] I.Gaál and K.Györy, *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 composites of number fields*, Experimental 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. Number Theory, **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 Mt. Math. Publ., **59** (2014), 79–92.
- [14] I.Gaál and N.Schulte, *Computing all power integral bases of cubic number fields*, Math. Comput., **53**(1989), 689–696.
- [15] I.Gaál and T. Szabó, *Power integral bases in parametric families of bi-quadratic fields*, JP Journal of Algebra, Number Theory and Applications, **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 Research in 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.Number Theory **51**(1995), 87–102.
- [18] W.Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Second Edition, Springer, 1974.
- [19] P.Olajos, *Power integral bases in orders of composite fields. II.*, Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math. **46**(2003), 35–41.