TWO FAMILIES OF MONOGENIC S_4 QUARTIC NUMBER FIELDS

HANSON SMITH

ABSTRACT. Consider the integral polynomials $f_{a,b}(x) = x^4 + ax + b$ and $g_{c,d}(x) = x^4 + cx^3 + d$. Suppose $f_{a,b}(x)$ and $g_{c,d}(x)$ are irreducible, $b \mid a$, and the integers b, d, $256d - 27c^4$, and $\dfrac{256b^3 - 27a^4}{\gcd(256b^3, 27a^4)}$ are all square-free. Using the Montes algorithm, we show that a root of $f_{a,b}(x)$ or $g_{c,d}(x)$ defines a monogenic extension of $\mathbb{Q}$ and serves as a generator for a power basis of the ring of integers. In fact, we show monogeneity for slightly more general families. Further, we obtain lower bounds on the density of polynomials generating monogenic S_4 fields within the families $f_{b,b}(x)$ and $g_{1,d}(x)$.

1. Introduction and Overview of Results

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. If there exists a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ with a root θ such that $\mathbb{Z}[\theta] = \mathcal{O}_K$, then we say K is *monogenic*. In other words, K is monogenic if $\mathcal{O}_K$ admits a power integral basis. A quantity related to monogeneity is the field index. The *field index* is defined to be the pair-wise greatest common divisor $\gcd\limits_{\alpha \in \mathcal{O}_K} [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Note that K can have field index 1 and still not be monogenic. Define the *minimal index* to be $\min\limits_{\alpha \in \mathcal{O}_K} [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Monogeneity is equivalent to having minimal index equal to 1.

Many of the number fields we are most familiar with are monogenic. For example, all quadratic extensions and cyclotomic extensions are monogenic. An example of a non-monogenic field, due to Dedekind [5], is the field obtained by adjoining a root of $x^3 - x^2 - 2x - 8$ to $\mathbb{Q}$. The problem of classifying monogenic number fields is often called *Hasse's problem*, as it is believed to have been posed to the London Mathematical Society by Helmut Hasse in the 1960's. See the remark on page 193 of [22].

We can now state concise, less-general versions of our main results. The following are consequences of Theorems 3.1 and 3.3 and Theorems 3.2 and 3.4, respectively.

2010 *Mathematics Subject Classification.* 11R04, 11R09 11R16.

Key words and phrases. monogeneity, monogenicity, power integral bases, rings of integers, quartic fields.

Corollary 1.1. *Consider $f_{b,b}(x) = x^4 + bx + b$ with $b \in \mathbb{Z}$ and let θ be a root. Suppose b and $256 - 27b$ are square-free and $b \neq 3, 5$. Then, $\mathbb{Q}(\theta)$ is a monogenic S_4 quartic field and θ is a generator of a power integral basis. Further, at least 29.18% of $b \in \mathbb{Z}$ satisfy these conditions.*

Corollary 1.2. *Consider $g_{1,d}(x) = x^4 + x^3 + d$ with $d \in \mathbb{Z}$ and let τ be a root. Suppose d and $256d - 27$ are square-free and $d \neq -2$. Then $\mathbb{Q}(\tau)$ is a monogenic S_4 quartic field and τ is a generator of a power integral basis. Further, at least 41.849% of $d \in \mathbb{Z}$ satisfy these conditions.*

Heuristically, the best possible percentages in Corollaries 1.1 and 1.2 seem to be 55.3%. See Remark 7.4.

2. Previous Work

Before a more detailed exposition of our work, we list some results pertaining to Hasse's problem. It has been shown that almost all abelian extension of $\mathbb{Q}$ with degree coprime to 6 are not monogenic; see Gras [19]. Gassert [16] shows that all fields obtained by adjoining a root of $x^n - a$, where a is square-free and $a^p \not\equiv a$ modulo p^2 for all primes $p \mid n$, are monogenic. In [27], Jones and Phillips identify infinitely many monogenic fields coming from polynomials of the shape $x^n + a(m,n)x + b(m,n)$, where $a(m,n)$ and $b(m,n)$ are prescribed forms. They consider two families of forms, one yielding Galois group S_n and the other A_n. Recently, Bhargava, Shankar, and Wang [2] have shown that the density of monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$ such that a root, θ, of $f(x)$ yields a power basis for the ring of integers of $\mathbb{Q}(\theta)$ is $\frac{6}{\pi^2} = \zeta(2)^{-1} \approx 60.79\%$. In the same paper, they also show that the density of monic integer polynomials with square-free discriminants is

$$\prod_p \left(1 - \frac{1}{p} + \frac{(p-1)^2}{p^2(p+1)}\right) \approx 35.82\%.$$

Note that these polynomials are a subset of the monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$ such that a root, θ, yields a power basis for the ring of integers of $\mathbb{Q}(\theta)$.

Many of the approaches to Hasse's problem have focused on fields with a given Galois group. We summarize the state of the art for degree 4 number fields. For a nice treatise on approaches to monogeneity using index form equations, see Gaál's book [9], "Diophantine Equations and Power Integral Bases." In particular, Chapter 6 deals with the quartic case. A general

algorithm for solving the quartic index form equations is presented, with the author expanding upon specific cases.

A biquadratic field is an extension having $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as the Galois group. A biquadratic extension can be written $\mathbb{Q}(\sqrt{m}, \sqrt{n})$. Gaál, Pethő, and Pohst [11] parametrize the field indices that can occur based on congruence conditions on m and n. Gras and Tanoé's article [20] gives necessary and sufficient conditions for a biquadratic field to be monogenic. Jadrijević [24] describes the minimal and field indices of the two families $\mathbb{Q}\left(\sqrt{(c-2)c}, \sqrt{(c+2)c}\right)$ and $\mathbb{Q}\left(\sqrt{(c-2)c}, \sqrt{(c+4)c}\right)$. This investigation is continued for the family $\mathbb{Q}\left(\sqrt{(c-2)c}, \sqrt{(c+4)c}\right)$ in [25]. When c and $c+4$ are square-free, Gaál and Jadrijević [10] show $\mathbb{Q}\left(\sqrt{2c}, \sqrt{2(c+4)}\right)$ is not monogenic, compute an integral basis, and determine the elements of minimal index.

Dihedral quartic fields have received a significant amount of attention. In [23], Huard, Spearman, and Williams compute the discriminant and an integral basis of quartic fields with quadratic subfields. Further, they find infinitely many monogenic D_8 fields. Specifically, they show that for each square-free c there are infinitely many fields of the form $\mathbb{Q}\left(\sqrt{c}, \sqrt{a+b\sqrt{c}}\right)$ that are monogenic. Gaál and Szabó [15] solve index form equations to show that the power integral bases found in [23] are the only possible power integral bases. In [28], Kable resolves the question of monogeneity when the D_8 field in question has an imaginary quadratic subfield and establishes some bounds in all cases. Using their algorithm from [13], Gaál, Pethő, and Pohst [12] compute "small" indices of totally real quartic fields with Galois group either $\mathbb{Z}/4\mathbb{Z}$ or D_8 and discriminant of absolute value less than 10^6. The indices may not be minimal since the algorithm they implemented checks only for solutions to the index form equation with absolute value less than 10^6.

A *pure* quartic field is a field obtained by adjoining a root of a polynomial of the form $x^4 - a$ to $\mathbb{Q}$. In [7], Funakura gives necessary and sufficient conditions for pure monogenic quartic fields. Gaál and Remete [14], characterize the only power integral bases of a number of infinite families of pure quartic fields using binomial Thue equations and extensive calculations on a supercomputer.

The *simplest* quartic fields are given by a root of $x^4 - tx^3 - 6x^2 + tx + 1$, where $t \neq \pm 3, 0$. They are totally real with Galois group $\mathbb{Z}/4\mathbb{Z}$. If $t^2 + 16$ is not divisible by an odd square, Olajos [30] has shown that the only two simplest quartics that are monogenic occur when $t = 2$ and $t = 4$. In [18],

Gras shows there are only two monogenic imaginary cyclic quartic fields. These are $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}\left(\zeta_{16}-\zeta_{16}^{-1}\right)$.

For A_4 fields, Spearman [32] shows $x^4+18x^2-4tx+t^2+81$ defines an infinite family of monogenic fields when $t\left(t^2+108\right)$ is square-free.

With [8], Gaál considers five families of totally complex quartic polynomials. The polynomials are shown to be irreducible and the Galois groups are classified; A_4, D_8, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ all occur. Further, Gaál computes all power integral bases of the orders generated by the roots.

As for S_4 quartics, work by Bérczes, Evertse, and Győry [1] restricts multiply monogenic orders. A recent paper [17] by Gassert, Smith, and Stange shows x^4-6x^2-tx-3 with $t+8$ and $t-8$ square-free defines an infinite family of monogenic S_4 quartic fields. It is worth noting that the methods of [17] are distinct from much of the other literature in that arithmetic properties of elliptic curves are central to proving monogeneity.

3. Results

In this paper we identify two families of monogenic quartic fields:

Theorem 3.1. *Let a and b be integers such that $\dfrac{256b^3-27a^4}{\gcd(256b^3,27a^4)}$ is square-free. Suppose that $f_{a,b}(x)=x^4+ax+b$ is irreducible and let θ be a root. Further, suppose every prime, p, dividing $\gcd(256b^3,27a^4)$ satisfies one of the following conditions:*

1. *p divides a and b, but p^2 does not divide b.*
2. *$p=2$, $p\nmid b$, and (a,b) is congruent to one of the following pairs in $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$: $(0,1)$, $(2,3)$.*
3. *$p=3$, $p\nmid a$, and (a,b) is congruent to one of the following pairs in $\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$: $(1,3)$, $(1,6)$, $(2,0)$, $(2,3)$, $(4,0)$, $(4,6)$, $(5,0)$, $(5,6)$, $(7,0)$, $(7,3)$, $(8,3)$, $(8,6)$.*

Then, $\mathbb{Q}(\theta)$ is monogenic and θ is a generator of the ring of integers.

Theorem 3.2. *Let c and d be integers such that d is square-free and $256d-27c^4$ is not divisible by the square of an odd prime. If $4\mid(256d-27c^4)$, we require that $v_2(d)=1$, or (c,d) is congruent to either $(0,1)$ or $(2,3)$ in $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Suppose that $g_{c,d}(x)=x^4+cx^3+d$ is irreducible and let τ be a root. Then, $\mathbb{Q}(\tau)$ is monogenic and τ is a generator of the ring of integers.*

If we restrict the above families we can classify the Galois groups and analyze densities. Note the infinitude of the restricted families below shows the more general families described above are infinite.

Theorem 3.3. *With the notation as in Theorem 3.1, consider* $f_{b,b}(x) = x^4 + bx + b$. *Suppose the coefficients of* $f_{b,b}(x)$ *satisfy the conditions given in Theorem 3.1. If* $b \neq 3, 5$, *then* $\mathbb{Q}(\theta)$ *has Galois group* S_4. *Moreover, the density of polynomials satisfying Theorem 3.1 among polynomials of the form* $x^4 + bx + b$ *with* $b \in \mathbb{Z}$ *arbitrary is at least* $\dfrac{51 - 4\pi^2}{4\pi^2} \approx 29.18\%$.

Theorem 3.4. *With the notation as in Theorem 3.2, consider* $g_{1,d}(x) = x^4 + x^3 + d$. *Suppose the coefficients of* $g_{1,d}(x)$ *satisfy the conditions given in Theorem 3.2. If* $d \neq -2$, *then* $\mathbb{Q}(\tau)$ *has Galois group* S_4. *Moreover, the density of polynomials satisfying Theorem 3.2 among polynomials of the form* $x^4 + x^3 + d$ *with* $d \in \mathbb{Z}$ *arbitrary is at least* $\dfrac{14 - \pi^2}{\pi^2} \approx 41.85\%$.

The primary reason for choosing the restricted families in the above theorems was so that we could easily analyze their densities. Within the larger class of polynomials which we prove yield monogenic fields, one can find other restrictions on the coefficients that yield families with a specific Galois group. However, in these cases studying density becomes more difficult, as one is concerned with square-free values of higher degree polynomials. Our methods could achieve similar results for polynomials of the form $x^4 + ax^2 + b$ or $x^4 + c$. However, these families have already been well-studied.

The outline of our paper is as follows: To prove Theorems 3.1 and 3.2 our main tool is the Montes algorithm, which we will briefly describe in Section 4. In Section 5, we show that the restricted families are irreducible and have Galois group S_4. Section 6 is concerned with applying the Montes algorithm to prove monogeneity. Lastly, in Section 7, we analyze the densities of our restricted families.

4. The Montes Algorithm

We prove monogeneity with a simple application of the Montes algorithm. We follow [6] for our exposition of the algorithm. Those interested in more general situations are advised to consult [21]. For the purposes of our work, the goal of the Montes algorithm is to compute the p-adic valuation $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]])$.

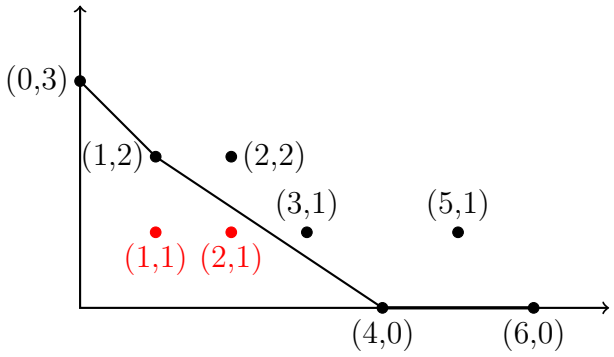
We begin by fixing notation. Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, θ a root of $f(x)$, $K = \mathbb{Q}(\theta)$, $\mathcal{O}_K$ the ring of integers of K, and p a prime in $\mathbb{Z}$. We extend the p-adic valuation on $\mathbb{Z}$ to $\mathbb{Z}[x]$ in the following manner. If $g(x) = b_0 + b_1 x + \cdots + b_k x^k$, define $v_p(g(x)) = \min_{0 \leq j \leq k} (v_p(b_j))$.

Now we describe a version of the Montes algorithm. Consider the reduction of $f(x)$ modulo p. Let $\overline{\phi}(x)$ be an irreducible factor of $f(x)$ modulo p and let $\phi(x)$ be a lift of $\overline{\phi}(x)$ to $\mathbb{Z}[x]$. We may write

$$f(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_r(x)\phi(x)^r$$

where $a_i(x) \in \mathbb{Z}[x]$ has degree strictly less than $\deg(\phi(x))$. We call this the *ϕ-adic development* of f. To any coefficient, $a_i(x)$, of the ϕ-adic development of f we attach the point $(i, v_p(a_i(x)))$ in the plane. The lower convex envelope of these points is called the *ϕ-Newton polygon of f*. The polygon determined by the sides of the ϕ-Newton polygon with negative slope is called the *principal ϕ-polygon of f*. We denote this polygon by N. The integer lattice points on or below N contain the arithmetic information we are interested in. Specifically, the *ϕ-index of f* is $\deg(\phi)$ times the number of points in the plane with integral coordinates that lie on or below N, strictly above the x-axis, and strictly to the right of the y-axis. We denote this number, the number of points in the integer lattice satisfying the above conditions, by $\text{ind}_\phi(f)$.

Example 4.1. To illustrate how the ϕ-Newton polygon is obtained, consider $f(x) = x^6 + 3x^5 + x^4 + 15x^3 + 9x^2 + 18x + 27$. We reduce modulo 3 and obtain $x^4(x^2 + 1)$. Working with the irreducible factor x, we take the lift x and the x-adic development is again our original polynomial $f(x) = x^6 + 3x^5 + x^4 + 15x^3 + 9x^2 + 18x + 27$. Now the x-Newton polygon is:



The x-Newton polygon for $f(x)$

The principal x-polygon merely excludes the side between $(4, 0)$ and $(6, 0)$. Further, accounting for $(1, 1)$, $(2, 1)$, and $(1, 2)$, we see $\text{ind}_x(f) = 3$.

Continuing with our description of the Montes algorithm, to any integral x-coordinate $0 \leq i \leq r$ of the principal ϕ-polygon N, we attach the residual

coefficient $c_i \in \mathbb{F}_p[x]/\phi(x)$, defined to be

$$c_i = \left\{ \begin{array}{ll} 0, & \text{if } (i, v_p(a_i(x))) \text{ lies strictly above } N \\ & \text{or } v_p(a_i(x)) = \infty. \\ \\ \dfrac{a_i(x)}{p^{v_p(a_i(x))}} \in \mathbb{F}_p[x]/\phi(x), & \text{if } (i, v_p(a_i(x))) \text{ lies on } N. \end{array} \right\}$$

Note we have covered all cases since $(i, v_p(a_i(x)))$ cannot lie below N, as N is the lower convex hull of the $(i, v_p(a_i(x)))$.

Let S be one of the sides of N. Suppose S has slope $\lambda = \dfrac{-h}{e}$ where h, e are positive, coprime integers. Define the *length* of S, denoted l, to be the length of the projection onto the x-axis. The *ramification index* of S is e, the denominator of λ. The *degree* of S, denoted d, is $\dfrac{l}{e}$.

Definition 4.2. Let t be the x-coordinate of the initial vertex of S. We define the *residual polynomial* attached to S to be

$$R_\lambda(f)(y) = c_t + c_{t+e}y + \cdots + c_{t+(d-1)e}y^{d-1} + c_{t+de}y^d \in \mathbb{F}_p[x]/\phi(x)[y].$$

Now we state the Theorem of the index, our key tool in proving monogeneity. This is Theorem 1.9 of [6].

Theorem 4.3. *Choose monic polynomials $\phi_1, \ldots, \phi_k$ whose reduction modulo p are the different irreducible factors of $f(x)$. Then,*

$$v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) \geq \operatorname{ind}_{\phi_1}(f) + \cdots + \operatorname{ind}_{\phi_k}(f).$$

Further, equality holds if and only if, for every ϕ_i, each side of the principal ϕ_i-polygon has a separable residual polynomial.

Remark 4.4. The Montes algorithm is concerned with separability. With the notation as above, suppose $f(x) \equiv \gamma(x)\psi(x)$ modulo p where $\gamma(x)$ is separable and $\gcd(\gamma(x), \psi(x)) = 1$. Then, $\gamma(x)$ contributes nothing to $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]])$. To see this, let $\eta(x)$ be an irreducible factor of $\gamma(x)$ and consider the $\eta(x)$-adic development of $f(x)$:

$$f(x) = a_0(x) + a_1(x)\eta(x) + \cdots + a_r(x)\eta(x)^r.$$

Because $f(x)$ has only one factor of $\eta(x)$ modulo p, we note $p \nmid a_1(x)$. Hence the principal η-polygon has only one side and that side terminates at $(1, 0)$. Thus $\operatorname{ind}_\eta(f) = 0$. Furthermore, the residual polynomial will be separable since linear polynomials are always separable.

5. Galois Groups and Irreducibility

Consider the two families $f_{a,b}(x) = x^4 + ax + b$ and $g_{c,d}(x) = x^4 + cx^3 + d$. These polynomials have discriminants $\Delta_f = 256b^3 - 27a^4$ and $\Delta_g = d^2(256d - 27c^4)$. To prove monogeneity, we require the conditions outlined in Theorems 3.1 and 3.2. However, to obtain families with Galois group S_4, we impose further restrictions. Namely, we require $a = b \neq 3, 5$ for $f_{a,b}(x)$ and $c = 1$, $d \neq -2$ for $g_{c,d}(x)$. There are less restrictive S_4 families, but we have chosen these parameters so that we can analyze the densities of these families.

In this section we are concerned with proving the first claims of Theorems 3.3 and 3.4, which we restate.

Theorem 5.1. *The polynomials $f_{b,b}(x) = x^4+bx+b$ and $g_{1,d}(x) = x^4+x^3+d$ where b, d, $256 - 27b$, and $256d - 27$ are square-free, $b \neq 3, 5$, and $d \neq -2$ are irreducible and have Galois group S_4.*

Before proving Theorem 5.1, we state two results we will need. We begin with some definitions. Given a quartic polynomial $h(x) = x^4+a_3x^3+a_2x^2+a_1x+a_0$ with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, we define the *resolvent cubic* to be

$$R_h(y) = y^3 - a_2y^2 + (a_3a_1 - 4a_0)y - a_3^2a_0 - a_1^2 + 4a_2a_0.$$

R_h has roots $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\alpha_1\alpha_4 + \alpha_2\alpha_3$. Given $h(x)$, a *depressed quartic* is obtained by the substitution $x = X - \dfrac{a_3}{4}$ and has the form

$$h_{dep}(X) = X^4 + \left(\frac{-3a_3^2}{8} + a_2\right)X^2 + \left(\frac{a_3^3}{8} - \frac{a_3a_2}{2} + a_1\right)X + \left(-\frac{3a_3^4}{256} + \frac{a_3^2a_2}{16} - \frac{a_3a_1}{4} + a_0\right).$$

If we have a depressed quartic $h_{dep}(x) = x^4 + b_2x^2 + b_1x + b_0$, we define the *resolvent cubic* to be

$$R_{h,dep}(z) = z^3 + 2b_2z^2 + \left(b_2^2 - 4b_0\right)z - b_1^2.$$

Though $R_h(y)$ and $R_{h,dep}(z)$ are both called the resolvent cubic, they are actually different polynomials even if $h(x)$ is depressed to begin with. More specifically, the substitution $y = z - \dfrac{a_3^2}{4} + a_2$ sends $R_h(y)$ to $R_{h,dep}(z)$. Thus R_h has a root in $\mathbb{Q}$ if and only if $R_{h,dep}$ has a root in $\mathbb{Q}$.

Now we recall a classical theorem. One can see [3] for a clear, elementary exposition.

Theorem 5.2. *With the notation as above, $h(x)$ factors into quadratic polynomials in $\mathbb{Q}[x]$ if and only if at least one of the following hold:*

(1) $R_{h,dep}$ has a nonzero root in $\mathbb{Q}^2$. That is, $R_{h,dep}$ has a root that is the square of a nonzero rational number.
(2) $b_1 = 0$ and $b_2^2 - 4b_0 \in \mathbb{Q}^2$.

We will also use the following result of Kappe and Warren [29, Theorem 1] to determine the Galois groups. One can also consult [4] for a nice exposition with ample examples.

Theorem 5.3. *Let $h(x)$ be a quartic polynomial that is irreducible over $\mathbb{Q}$ and let Δ_h be the discriminant. Further, let G_h be the Galois group of h. Then, with the notation as above, the first two columns of the following table imply the third column.*

Δ_h	R_h	G_h
not a square	*irreducible*	S_4
a square	*irreducible*	A_4
not a square	*reducible*	D_8 *or* $\mathbb{Z}/4\mathbb{Z}$
a square	*reducible*	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

We proceed with the proof of Theorem 5.1.

Proof. We begin with the irreducibility $f_{b,b}(x) = x^4 + bx + b$. If b is not ± 1, then $f_{b,b}$ is Eisenstein at any prime dividing b. If $b = \pm 1$, then the rational root test shows that there is not a root in $\mathbb{Q}$. To show $f_{\pm 1,\pm 1}$ does not split into quadratic factors we consider $R_{f_{\pm 1,\pm 1},dep}(z) = z^3 \mp 4z - 1$. The rational root test shows $R_{f_{\pm 1,\pm 1},dep}$ does not have a root in $\mathbb{Q}$, let alone $\mathbb{Q}^2$. Since $b_2 = \pm 1$, Theorem 5.2 shows $f_{\pm 1,\pm 1}$ is irreducible. Note that since $R_{f_{\pm 1,\pm 1},dep}$ is irreducible, $R_{f_{\pm 1,\pm 1}}$ is irreducible.

It remains to consider $R_{f_{b,b}} = y^3 - 4by - b^2$ for $b \neq \pm 1$. Suppose we have a root k. The rational root test shows $k \in \mathbb{Z}$ divides b^2. If p is a prime divisor of b, then reduction modulo p shows p divides k. Since b is square-free, b divides k. Write $k = bk_0$. We have $b^2(bk_0^3 - 4k_0 - 1) = 0$. Thus, $bk_0^3 - 4k_0 - 1 = 0$. If any prime divides k_0, reduction modulo that prime yields a contradiction. Hence, $k_0 = \pm 1$. If $k_0 = 1$, then $b = 5$, and if $k_0 = -1$, then $b = 3$. Therefore, if $b \neq 3, 5$, then $R_{f_{b,b}}$ is irreducible.

For $g_{1,d}(x) = x^4 + x^3 + d$, suppose we have a root l. By Gauss's lemma, $l \in \mathbb{Z}$. We have $l^3(l + 1) = -d$. Since d is square-free, we must have $l = 1$ and $d = -2$. Thus for $d \neq -2$, we conclude $g_{1,d}$ does not have a root in $\mathbb{Q}$. To see that $g_{1,d}$ does not factor into quadratics, we make the change of

variables $x = X - \frac{1}{4}$ to obtain the depressed quartic

$$X^4 - \frac{3}{8}X^2 + \frac{1}{8}X - \frac{3}{256} + d.$$

Here $b_1 = \frac{1}{8}$ so condition (2) of Theorem 5.2 does not hold. Consider $R_{g_{1,d}}(y) = y^3 - 4dy - d$. If $d \neq \pm 1$, then $R_{g_{1,d}}$ is Eisenstein at any prime dividing d and hence irreducible. If $d = \pm 1$, the rational root test shows $R_{g_{1,d}}$ is irreducible. Thus condition (1) of Theorem 5.2 does not hold since $R_{g_{1,d}}$ has a root in $\mathbb{Q}$ if and only if $R_{g_{1,d},dep}$ has a root in $\mathbb{Q}$. We conclude $g_{1,d}$ is irreducible.

We have demonstrated that, with the conditions given in Theorem 5.1, $f_{b,b}, g_{1,d}, R_{f_{b,b}}$, and $R_{g_{1,d}}$ are all irreducible. A quick computation shows that $\Delta_{f_{b,b}}$ and $\Delta_{g_{1,d}}$ are not squares. Thus, Theorem 5.3 shows that $f_{b,b}$ and $g_{1,d}$ have Galois group S_4.

□

Remark 5.4. Let β be a root of $R_{g_{1,d}}$. Note that $g_{1,d}$ and $R_{g_{1,d}}$ both have discriminant $d^2(256d - 27)$. The methods of Section 6 show β generates a power basis for the ring of integers of the cubic field $\mathbb{Q}(\beta)$ exactly when τ, a root of $g_{1,d}$, generates a power basis for the ring of integers of the quartic field $\mathbb{Q}(\tau)$.

6. Monogeneity

For the following we recall a classical formula from algebraic number theory. Let K be a number field obtained by adjoining a root, α, of some monic irreducible polynomial $h(x) \in \mathbb{Z}[x]$. Write $\mathcal{O}_K$ for the ring of integers, $\mathrm{disc}(K)$ for the discriminant of K, and Δ_h for the discriminant of $h(x)$. Let p be a prime. We have

$$v_p(\mathrm{disc}(K)) + 2v_p([\mathcal{O}_K : \mathbb{Z}[\alpha]]) = v_p(\Delta_h).$$

Note this implies any prime dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ also divides Δ_h. Before we proceed with the proof, we recall Theorem 3.1:

Theorem 6.1. *Let a and b be integers such that $\frac{256b^3 - 27a^4}{\gcd(256b^3, 27a^4)}$ is square-free. Suppose that $f_{a,b}(x) = x^4 + ax + b$ is irreducible and let θ be a root. Further, suppose every prime, p, dividing $\gcd(256b^3, 27a^4)$ satisfies one of the following conditions:*

(1) p divides a and b, but p^2 does not divide b.

(2) $p = 2$, $p \nmid b$, *and* (a, b) *is congruent to one of the following pairs in* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*:* $(0, 1)$, $(2, 3)$.

(3) $p = 3$, $p \nmid a$, *and* (a, b) *is congruent to one of the following pairs in* $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$*:* $(1, 3)$, $(1, 6)$, $(2, 0)$, $(2, 3)$, $(4, 0)$, $(4, 6)$, $(5, 0)$, $(5, 6)$, $(7, 0)$, $(7, 3)$, $(8, 3)$, $(8, 6)$.

Then, $\mathbb{Q}(\theta)$ *is monogenic and* θ *is a generator of the ring of integers.*

Proof. Recall $\Delta_f = 256b^3 - 27a^4$. Let p be a prime dividing Δ_f. We will show that $v_p([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$. First, suppose $p \mid \Delta_f$, but $p \nmid \gcd(256b^3, 27a^4)$. Since $\dfrac{256b^3 - 27a^4}{\gcd(256b^3, 27a^4)}$ is square-free, we see

$$1 = v_p(\Delta_f) = v_p(\mathrm{disc}(\mathbb{Q}(\theta))) + 2v_p([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]).$$

Thus $v_p([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$.

So we consider primes p dividing $\gcd(256b^3, 27a^4)$. Suppose p satisfies condition (1). We apply the Montes algorithm. Considering $f_{a,b}(x)$ modulo p we obtain x^4. Thus the only irreducible factor we must consider is x. Taking the lift $\phi(x) = x$, the principal x-polygon of $f_{a,b}(x)$ has one side, originating at $(0, 1)$ and terminating at $(4, 0)$. Thus $\mathrm{ind}_x(f_{a,b}) = 0$. The residual polynomial attached to this side is $y - \frac{b}{p}$, which is clearly separable. By Theorem 4.3, $v_p([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$.

Now suppose $p = 2$ satisfies condition (2). We apply the Montes algorithm. Note that 2 necessarily divides a, so modulo 2 we have

$$f_{a,b}(x) \equiv x^4 + b \equiv (x + 1)^4.$$

The $(x + 1)$-adic development of $f_{a,b}(x)$ is

$$f_{a,b}(x) = (x + 1)^4 - 4(x + 1)^3 + 6(x + 1)^2 + (a - 4)(x + 1) + b - a + 1.$$

To show monogeneity, we need $\mathrm{ind}_{x+1}(f_{a,b}) = 0$. Thus we want $v_2(b-a+1) = 1$. One checks this is equivalent to the criteria given in condition (2). The residual polynomial is linear and hence separable. Thus, Theorem 4.3 tells us $v_2([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$.

Finally, suppose $p = 3$ satisfies condition (3). We begin applying the Montes algorithm. Note that 3 necessarily divides b, so that modulo 3 we have

$$f_{a,b}(x) \equiv x^4 + ax \equiv x(x^3 + a).$$

From Remark 4.4, the separable factor x contributes nothing to the index.

For the factor $(x^3 + a)$, we have two cases:

Case 1: Suppose $a \equiv 1$ modulo 3. Thus $f_{a,b}(x) \equiv x(x+1)^3$ modulo 3, we take the $(x+1)$-adic development

$$f_{a,b}(x) = (x+1)^4 - 4(x+1)^3 + 6(x+1)^2 + (a-4)(x+1) + b - a + 1.$$

In order to have $\mathrm{ind}_{x+1}(f_{a,b}) = 0$, we need $v_3(b-a+1) = 1$. This is satisfied by the following pairs (a,b) in $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$: $(1,3)$, $(1,6)$, $(4,0)$, $(4,6)$, $(7,0)$, $(7,3)$. The residual polynomial is linear and hence separable. Applying Theorem 4.3, we conclude $v_3([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$.

Case 2: Suppose $a \equiv -1$ modulo 3. Thus $f_{a,b} \equiv x(x-1)^3$ modulo 3, we take the $(x-1)$-adic development

$$f_{a,b}(x) = (x-1)^4 + 4(x-1)^3 + 6(x-1)^2 + (a+4)(x-1) + b + a + 1.$$

In order to have $\mathrm{ind}_{x-1}(f_{a,b}) = 0$, we need $v_3(b+a+1) = 1$. This is satisfied by the following pairs (a,b) in $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$: $(2,0)$, $(2,3)$, $(5,0)$, $(5,6)$, $(8,3)$, $(8,6)$. The residual polynomials is linear and hence separable. Applying Theorem 4.3, we conclude $v_3([\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]) = 0$.

Since we have covered all primes dividing the discriminant of $f_{a,b}$, we see $[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]] = 1$. We conclude that $\mathbb{Q}(\theta)$ is monogenic and θ generates the ring of integers. □

Before proving Theorem 3.2, we remind ourselves of the statement:

Theorem 6.2. *Let c and d be integers such that d is square-free and $256d - 27c^4$ is not divisible by the square of an odd prime. If $4 \mid (256d - 27c^4)$, we require that $v_2(d) = 1$, or (c,d) is congruent to either $(0,1)$ or $(2,3)$ in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Suppose that $g_{c,d}(x) = x^4 + cx^3 + d$ is irreducible and let τ be a root. Then, $\mathbb{Q}(\tau)$ is monogenic and τ is a generator of the ring of integers.*

Proof. Recall $\Delta_g = d^2(256d - 27c^4)$. Let p be a prime dividing Δ_g. We will show $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$. First, suppose $p \mid (256d - 27c^4)$, but $p \nmid d$ and $p \neq 2$. By assumption, $v_p(256d - 27c^4) = 1$. Hence

$$1 = v_p(\Delta_g) = v_p(\mathrm{disc}(\mathbb{Q}(\tau))) + 2v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]).$$

Thus $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

Now suppose $p \mid d$. Applying the Montes algorithm, we consider $g_{c,d}(x)$ modulo p. We have two cases:

Case 1: Suppose $p \mid c$. The reduction of $g_{c,d}(x)$ is simply x^4, so we only consider the irreducible factor x. Taking the lift $\phi(x) = x$, the principal x-polygon of $g_{c,d}(x)$ has one side, originating at $(0,1)$ and terminating at $(4,0)$. Thus $\mathrm{ind}_x(g_{c,d}) = 0$. The residual polynomial attached to this side is $y - \frac{d}{p}$, which is clearly separable. Thus, by Theorem 4.3, $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

Case 2: Suppose $p \nmid c$. Modulo p we have

$$g_{c,d}(x) \equiv x^4 + cx^3 \equiv x^3(x + c).$$

We treat the irreducible factor x exactly as above. Again, the principal x-polygon is one-sided and the residual polynomial is separable. We conclude $\mathrm{ind}_x(g_{c,d}) = 0$.

Considering the factor $x + c$, we note it is separable. From Remark 4.4 we see $\mathrm{ind}_{x+c}(g_{c,d}) = 0$ and the residual polynomial is separable. We apply Theorem 4.3 to see $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

For the final scenario, suppose $4 \mid (256d - 27c^4)$ and $2 \nmid d$. Modulo 2 we have

$$g_{c,d}(x) \equiv x^4 + d \equiv (x - 1)^4.$$

Beginning the Montes algorithm, the $(x - 1)$-adic development is

$$(x - 1)^4 + (c + 4)(x - 1)^3 + (3c + 6)(x - 1)^2 + (3c + 4)(x - 1) + c + d + 1.$$

To ensure $\mathrm{ind}_{x-1}(g_{c,d}) = 0$, we need $v_2(c + d + 1) = 1$. One checks this is equivalent to the conditions given in the theorem statement. Finally, if $v_2(c + d + 1) = 1$ the residual polynomial is linear and hence separable. Thus, by Theorem 4.3, $v_2([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

Since we have covered all primes dividing the discriminant of $g_{c,d}$, we conclude $[\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]] = 1$. Thus $\mathbb{Q}(\tau)$ is monogenic and τ generates the ring of integers.

□

7. Density

In this section, we will show the families of monogenic S_4 fields defined by the polynomials $f_{b,b}(x) = x^4 + bx + b$ and $g_{1,d}(x) = x^4 + x^3 + d$ with the conditions imposed in Theorem 5.1 are infinite. In fact, we will give a lower bound on the density of each family. The families $f_{b,b}$ and $g_{1,d}$ are parametrized by b and d respectively. So, by *density*, we mean the natural density of $b \in \mathbb{Z}$ or $d \in \mathbb{Z}$ yielding monogenic fields.

To begin with, it is well-known that the natural density of square-free integers is

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 60.79\%.$$

See [26] for example. Now let $S(x; m, k)$ denote the number of square-free integers that do not exceed x and are congruent to m modulo k. We will also need a result of Prachar from [31]:

Theorem 7.1.

$$S(x;m,k) \sim \frac{6x}{\pi^2 k} \prod_{p|k} \left(1 - \frac{1}{p^2}\right)^{-1} \qquad (x \to \infty)$$

for $\gcd(m,k) = 1$ *and* $k \leq x^{\frac{2}{3}-\epsilon}$.

Before the proof, we recall the second claim of Theorem 3.3:

Theorem 7.2. *The density of monogenic S_4 fields within the number fields defined by $f_{b,b}(x) = x^4 + bx + b$ is at least* $\dfrac{51 - 4\pi^2}{4\pi^2} \approx 29.18\%$.

Proof. From Theorem 6.1, to show that there are infinitely many monogenic fields defined by a root of $f_{b,b}$, it suffices to show there are infinitely many square-free b such that $256 - 27b$ is square-free. The density of square-free b is $\dfrac{6}{\pi^2}$. By Theorem 7.1, the density of square-free numbers congruent to 256 modulo 27 among numbers congruent to 256 modulo 27 is

$$\frac{6}{\pi^2}\left(1 - \frac{1}{9}\right)^{-1} = \frac{27}{4\pi^2}.$$

Thus, at worst, the density of monogenic fields in this family is

$$\frac{6}{\pi^2} - \left(1 - \frac{27}{4\pi^2}\right) = \frac{51 - 4\pi^2}{4\pi^2} \approx 29.18\%.$$

□

As above, before beginning the proof, we recall the second claim of Theorem 3.4:

Theorem 7.3. *The density of monogenic S_4 fields within the number fields defined by $g_{1,d}(x) = x^4 + x^3 + d$ is at least* $\dfrac{14 - \pi^2}{\pi^2} \approx 41.85\%$.

Proof. From Theorem 6.2, to show that there are infinitely many monogenic fields defined by a root of $g_{1,d}$, it suffices to show there are infinitely many square-free d such that $256d - 27$ is square-free. The density of square-free d is $\dfrac{6}{\pi^2}$. By Theorem 7.1, the density of square-free numbers congruent to 27 modulo 256 among numbers congruent to 27 modulo 256 is

$$\frac{6}{\pi^2}\left(1 - \frac{1}{4}\right)^{-1} = \frac{24}{3\pi^2}.$$

Thus, at worst, the density of monogenic fields in this family is

$$\frac{6}{\pi^2} - \left(1 - \frac{24}{3\pi^2}\right) = \frac{14 - \pi^2}{\pi^2} \approx 41.85\%.$$

□

Remark 7.4. As above, let θ be a root of $f_{b,b}(x) = x^4 + bx + b$ and τ a root of $g_{1,d}(x) = x^4 + x^3 + d$. Computationally, it appears that 55.3% of fields of the form $\mathbb{Q}(\theta)$ have θ as a generator of $\mathcal{O}_{\mathbb{Q}(\theta)}$. Likewise, it appears that 55.3% of fields of the form $\mathbb{Q}(\tau)$ have τ as a generator of $\mathcal{O}_{\mathbb{Q}(\tau)}$. If $\mathbb{Q}(\tau)$ is monogenic, it seems that τ is almost always a generator of the ring of integers, since $\mathbb{Q}(\tau)$ appears to be monogenic about 55.3% of the time. However, $\mathbb{Q}(\theta)$ seems to be monogenic about 58.7% of the time. Thus there are some cases where $\mathbb{Q}(\theta)$ is monogenic, but θ does not generate the ring of integers. We obtained these heuristics using SageMath [33] and testing b and d between -2,500,000 and 2,500,000.

Acknowledgements. The author would like to thank Katherine Stange and Alden Gassert for their help and encouragement. The author would also like to thank Sebastian Bozlee for the careful proofreading and Paul Voutier for noticing another case could be covered by Theorem 3.2.

References

[1] A. Bérczes, J.-H. Evertse, and K. Győry, *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5), 12 (2013), pp. 467–497.

[2] M. Bhargava, A. Shankar, and X. Wang, *Squarefree values of polynomial discriminants I*, ArXiv e-prints, (2016).

[3] G. Brookfield, *Factoring quartic polynomials: a lost art*, Mathematics Magazine, 80 (2007), pp. 67–70.

[4] K. Conrad, *Galois groups of cubics and quartics (not in characteristic 2)*.

[5] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Gött. Abhandlungen, (1878), pp. 1–23.

[6] L. El Fadil, J. Montes, and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra Appl., 11 (2012), pp. 1250073, 33.

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

[8] I. Gaál, *Power integral bases in orders of families of quartic fields*, Publ. Math. Debrecen, 42 (1993), pp. 253–263.

[9] ——, *Diophantine equations and power integral bases*, Birkhäuser Boston, Inc., Boston, MA, 2002. New computational methods.

[10] I. Gaál and B. Jadrijević, *Determining elements of minimal index in an infinite family of totally real bicyclic biquadratic number fields*, JP J. Algebra Number Theory Appl., 39 (2017), pp. 307–326.

[11] I. Gaál, A. Pethő, and M. Pohst, *On the indices of biquadratic number fields having Galois group V_4*, Arch. Math. (Basel), 57 (1991), pp. 357–361.

[12] ——, *On the resolution of index form equations*, in Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, S. M. Watt, ed., New York, NY, USA, 1991, ACM, pp. 185–186.

[13] ——, *On the resolution of index form equations in biquadratic number fields. I, II*, J. Number Theory, 38 (1991), pp. 18–34, 35–51.

[14] I. Gaál and L. Remete, *Binomial thue equations and power integral bases in pure quartic fields*, JP J. Algebra Number Theory Appl., 32 (2014), pp. 49–61.

[15] I. Gaál and T. Szabó, *Power integral bases in parametric families of biquadratic fields*, JP J. Algebra Number Theory Appl., 24 (2012), pp. 105–114.

[16] T. A. Gassert, *A note on the monogeneity of power maps*, Albanian J. Math., 11 (2017), pp. 3–12.

[17] T. A. Gassert, H. Smith, and K. E. Stange, *A family of monogenic S_4 quartic fields arising from elliptic curves*, ArXiv e-prints, (2017).

[18] M.-N. Gras, $\mathbf{Z}$*-bases d'entiers* $1, \theta, \theta^2, \theta^3$ *dans les extensions cycliques de degré* 4 *de* $\mathbf{Q}$, in Number theory, 1979–1980 and 1980–1981, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1981, pp. Exp. No. 6, 14.

[19] ——, *Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de* $\mathbf{Q}$, in Séminaire de théorie des nombres, Paris 1984–85, vol. 63 of Progr. Math., Birkhäuser Boston, Boston, MA, 1986, pp. 97–107.

[20] M.-N. Gras and F. Tanoé, *Corps biquadratiques monogènes*, Manuscripta Math., 86 (1995), pp. 63–79.

[21] J. Guàrdia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory, 147 (2015), pp. 549–589.

[22] F. Halter-Koch and R. F. Tichy, eds., *Algebraic number theory and Diophantine analysis*, Walter de Gruyter & Co., Berlin, 2000.

[23] J. G. Huard, B. K. Spearman, and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory, 51 (1995), pp. 87–102.

[24] B. Jadrijević, *Solving index form equations in two parametric families of biquadratic fields*, Math. Commun., 14 (2009), pp. 341–363.

[25] ——, *On elements with index of the form 2^a3^b in a parametric family of biquadratic fields*, Glas. Mat. Ser. III, 50(70) (2015), pp. 43–63.

[26] C. H. Jia, *The distribution of square-free numbers*, Sci. China Ser. A, 36 (1993), pp. 154–169.

[27] L. Jones and T. Phillips, *Infinite families of monogenic trinomials and their Galois groups*, Internat. J. Math., 29 (2018), pp. 1850039, 11.

[28] A. C. Kable, *Power bases in dihedral quartic fields*, J. Number Theory, 76 (1999), pp. 120–129.

[29] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly, 96 (1989), pp. 133–137.

[30] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experiment. Math., 14 (2005), pp. 129–132.

[31] K. Prachar, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math., 62 (1958), pp. 173–176.

[32] B. K. Spearman, *Monogenic A_4 quartic fields*, Int. Math. Forum, 1 (2006), pp. 1969–1974.

[33] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2017. `http://www.sagemath.org`.

Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395, USA

Email address: `hanson.smith@colorado.edu`