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 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 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 basis. For this reason, some authors say $\mathcal{O}_K$ admits a *power integral basis* instead of saying K is monogenic.

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, 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 was posed in the 1960's by Helmut Hasse.

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

Theorem 1.1. *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.

Date: February 26, 2018.

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

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

Theorem 1.2. *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 (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 the density. Note the infinitude of the restricted families below shows the more general families described above are infinite.

Theorem 1.3. *With the notation as in Theorem 1.1, consider $f_{b,b}(x) = x^4 + bx + b$. Suppose $f_{b,b}(x)$ satisfies the conditions given in Theorem 1.1 so that $\mathbb{Q}(\theta)$ is monogenic. If $b \neq \pm 5$, then $\mathbb{Q}(\theta)$ has Galois group S_4. Moreover, the density of polynomials satisfying the conditions of Theorem 1.1 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 1.4. *With the notation as in Theorem 1.2, consider $g_{1,d}(x) = x^4 + x^3 + d$. Suppose $g_{1,d}(x)$ satisfies the conditions given in Theorem 1.2 so that $\mathbb{Q}(\tau)$ is monogenic. If $d \neq -2$, then $\mathbb{Q}(\tau)$ has Galois group S_4. Moreover, the density of polynomials satisfying the conditions of Theorem 1.2 among polynomials of the form $x^4 + x^3 + d$ with $d \in \mathbb{Z}$ arbitrary is at least $\dfrac{14 - \pi^2}{\pi^2} \approx 41.85\%$.*

We can state consequences of the above concisely:

Corollary 1.5. *Consider $f_{b,b}(x) = x^4 + bx + b$ with $b \in \mathbb{Z}$ and let θ be a root. At least 29.18% of polynomials of the form $f_{b,b}(x)$ yield monogenic, S_4 fields, $\mathbb{Q}(\theta)$, such that θ generates a power basis for the ring of integers.*

Corollary 1.6. *Consider $g_{1,d}(x) = x^4 + x^3 + d$ with $d \in \mathbb{Z}$ and let τ be a root. At least 41.849% of polynomials of the form $g_{1,d}(x)$ yield monogenic, S_4 fields, $\mathbb{Q}(\tau)$, such that τ generates a power basis for the ring of integers.*

Heuristically, the best possible percentages in Corollaries 1.5 and 1.6 seem to be 55.3%. See Remark 5.4.

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; see below.

The outline of our paper is as follows: To prove Theorems 1.1 and 1.2 our main tool is the Montes algorithm, which we will briefly describe in Section 2. In Section 3, we show that the restricted families are irreducible and have Galois group S_4. Section 4 is concerned with applying the Montes algorithm to prove monogeneity. Lastly, in Section 5, we analyze the densities of our restricted families.

Before continuing, 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 [10]. It is known that all fields obtained by adjoining a root of $x^n - a$, where a is square-free and a^p is not congruent to a modulo p^2 for all primes $p \mid n$, are monogenic [8]. Recently, Bhargava, Shankar, and Wang 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 $\frac{6}{\pi^2} = \zeta(2)^{-1} \approx 60.79\%$ [2]. 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 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. Gras and Tanoé give necessary and sufficient conditions for a biquadratic field, an extension having $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as Galois group, to be monogenic [11]. Dihedral quartic fields have received a significant amount of attention. In [13], Huard, Spearman, and Williams find a monogenic family. Specifically, they find infinitely many fields of the form $\mathbb{Q}\left(\sqrt{c}, \sqrt{a + b\sqrt{c}}\right)$ with c square-free to be monogenic. In [15], Kable resolves the problem when the D_8 field in question has an imaginary quadratic subfield and establishes some bounds in all cases. 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 considers the pure case and completely classifies pure monogenic quartic fields. For A_4 fields, Spearman has found an infinite family [19]. For cyclic quartic fields, with a mild square-free hypothesis, Olajos has shown that there are only two totally real fields that are monogenic [17]. In [10], Gras shows there are only two monogenic imaginary cyclic quartic fields. These are $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$. As for S_4 quartics, work by Bérczes, Evertse, and Győry [1] restricts multiply monogenic orders and a recent paper by Gassert, Smith, and Stange finds an infinite family [9]. It is worth noting that the methods of [9] are distinct from much of the other literature in that arithmetic properties of elliptic curves are central to proving monogeneity.

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.

2. 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 [12]. For the purposes of our work, the goal of the Montes algorithm is to compute the p-adic valuation $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]])$.

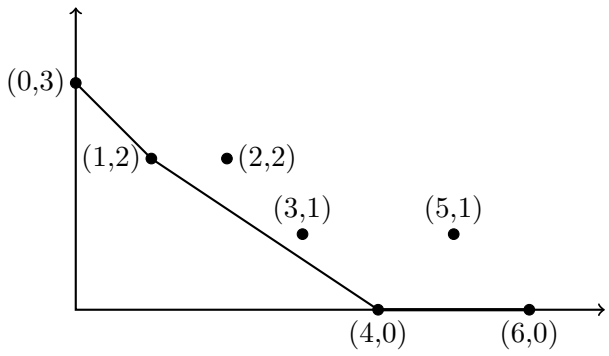
We begin by fixing notation. Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, θ a root of $f(x)$, $K = \mathbb{Q}(\theta)$, $\mathcal{O}_K$ the ring of integers of K, and p a prime in $\mathbb{Z}$. We extend the p-adic valuation on $\mathbb{Z}$ to $\mathbb{Z}[x]$ in the following manner. If $g(x)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

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*, denoted N. This polygon contains 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 2.1. 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 $(1, 1)$, $(1, 2)$, and $(2, 1)$, we see $\text{ind}_x(f) = 3$.

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

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

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

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 2.2. 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 monogenicity. This is Theorem 1.9 of [6].

Theorem 2.3. *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 2.4. 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.

3. 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 $\Delta_f = b^3(256 - 27a^4b)$ and $\Delta_g = d^2(256d - 27c^4)$. To prove monogeneity, we require the conditions outlined in Theorems 1.1 and 1.2. However, to obtain families with Galois group S_4, we impose further restrictions. Namely, we require $a = b$, $b \neq \pm 5$ 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.

Theorem 3.1. *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, $b \neq \pm 5$, and $d \neq -2$ are irreducible and have Galois group S_4.*

Before proving Theorem 3.1, 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

$$R_h(y) = y^3 - a_2y^2 + (a_3a_1 - 4a_0)y - a_3^2a_2 - a_1^2 + 4a_2a_0.$$

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 $x = X - \frac{a_3}{4}$ 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

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

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 $y = z - \frac{a_3^2}{4} + a_2$ 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 3.2. *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 [16, Theorem 1] to determine the Galois groups. One can also consult [4] for a nice exposition with ample examples.

Theorem 3.3. *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 3.1.

Proof. First we will show that $f_{b,b}(x) = x^4 + bx + b$ and $g_{1,d}(x) = x^4 + x^3 + d$ are irreducible. We begin with $f_{b,b}$. 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 $f_{b,b}$ does not split into quadratic factors we consider $R_{f_{b,b},dep}(z) = z^3 \pm 4z - 1$. The rational root test shows $R_{f_{b,b},dep}$ does not have a root in $\mathbb{Q}$, let alone $\mathbb{Q}^2$. Since $b_2 = \pm 1$, Theorem 3.2 shows $f_{b,b}$ is irreducible. Note that since $R_{f_{b,b},dep}$ is irreducible, $R_{f_{b,b}}$ is irreducible.

For $g_{1,d}$, suppose we have a root k. By Gauss's lemma, $k \in \mathbb{Z}$. We have $k^3(k+1) = -d$. Since d is square-free, we must have $k = 1$ 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 variable $x = X - \frac{1}{4}$ 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 3.2 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 3.2 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.

In proving $f_{b,b}$ and $g_{1,d}$ are irreducible, we have shown $R_{f_{b,b}}$ and $R_{g_{1,d}}$ are irreducible. A quick computation shows that, with the conditions given in Theorem 3.1, $\Delta_{f_{b,b}}$ and $\Delta_{g_{1,d}}$ are not squares. Thus Theorem 3.3 shows that $f_{b,b}$ and $g_{1,d}$ have Galois group S_4.

□

4. 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. We proceed with the main results of this section.

Theorem 4.1. *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.*

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

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 2.3 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

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

First, we consider the irreducible factor x. Taking the lift x, the x-adic development is $f_{a,b}(x) = x^4 + ax + b$. By hypothesis $3 \nmid a$, so the principal x-polygon is one-sided and terminates at $(1,0)$. Thus $\mathrm{ind}_x(f_{a,b}) = 0$. The residual polynomial is linear and hence separable.

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 2.3, 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 $\text{ind}_{x-1}(f_{a,b}) = 0$, 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 2.3, 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. □

Theorem 4.2. *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 (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

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

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 $\text{ind}_x(g_{c,d}) = 0$. The residual polynomial attached to this side is $y - \frac{d}{p}$, which is clearly separable. Thus, by Theorem 2.3, $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

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 $\text{ind}_x(g_{c,d}) = 0$.

Considering the factor $x + c$, we note it is separable. From Remark 2.4 we see $\text{ind}_{x+c}(g_{c,d}) = 0$ and the residual polynomial is separable. We apply Theorem 2.3 to see $v_p([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

For the final scenario, suppose $4|(256d - 27c^4)$ 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 $\text{ind}_{x-1}(g_{c,d}) = 0$, 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 2.3, $v_2([\mathcal{O}_{\mathbb{Q}(\tau)} : \mathbb{Z}[\tau]]) = 0$.

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. □

5. 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 3.1 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 [14] 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 [18]:

Theorem 5.1.

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

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

We proceed with the main results of this section.

Theorem 5.2. *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 4.1, 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 5.1, 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

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

□

Theorem 5.3. *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 4.2, 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 5.1, 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 5.4. 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 [5] and testing b and d between -2,500,000 and 2,500,000.

References

[1] A. Bérczes, J.-H. Evertse, and K. Győry. Multiply monogenic orders. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 12(2):467–497, 2013. ISSN 0391-173X.

[2] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants I. *ArXiv e-prints*, Nov. 2016. URL https://arxiv.org/abs/1611.09806.

[3] G. Brookfield. Factoring quartic polynomials: a lost art. *Mathematics Magazine*, 80(1):67–70, 2007. URL http://www.jstor.org/stable/27642994.

[4] K. Conrad. Galois groups of cubics and quartics (not in characteristic 2). URL http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf.

[5] T. S. Developers. *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2017. http://www.sagemath.org.

[6] L. El Fadil, J. Montes, and E. Nart. Newton polygons and p-integral bases of quartic number fields. *J. Algebra Appl.*, 11(4):1250073, 33, 2012. ISSN 0219-4988. doi: 10.1142/S0219498812500739. URL http://dx.doi.org/10.1142/S0219498812500739.

[7] T. Funakura. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, 26:27–41, 1984. ISSN 0030-1566.

[8] T. A. Gassert. A note on the monogeneity of power maps. *Albanian J. Math.*, 11(1):3–12, 2017. ISSN 1930-1235.

[9] T. A. Gassert, H. Smith, and K. E. Stange. A family of monogenic S_4 quartic fields arising from elliptic curves. *ArXiv e-prints*, Aug. 2017. URL https://arxiv.org/abs/1708.03953.

[10] M.-N. Gras. 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*, volume 63 of *Progr. Math.*, pages 97–107. Birkhäuser Boston, Boston, MA, 1986.

[11] M.-N. Gras and F. Tanoé. Corps biquadratiques monogènes. *Manuscripta Math.*, 86(1):63–79, 1995. ISSN 0025-2611. doi: 10.1007/BF02567978. URL http://dx.doi.org/10.1007/BF02567978.

[12] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *J. Number Theory*, 147:549–589, 2015. ISSN 0022-314X. doi: 10.1016/j.jnt.2014.07.027. URL http://0-dx.doi.org.libraries.colorado.edu/10.1016/j.jnt.2014.07.027.

[13] J. G. Huard, B. K. Spearman, and K. S. Williams. Integral bases for quartic fields with quadratic subfields. *J. Number Theory*, 51(1):87–102, 1995. ISSN 0022-314X. doi: 10.1006/jnth.1995.1036. URL http://dx.doi.org/10.1006/jnth.1995.1036.

[14] C. H. Jia. The distribution of square-free numbers. *Sci. China Ser. A*, 36(2): 154–169, 1993. ISSN 1001-6511.

[15] A. C. Kable. Power bases in dihedral quartic fields. *J. Number Theory*, 76 (1):120–129, 1999. ISSN 0022-314X. doi: 10.1006/jnth.1998.2350. URL http://dx.doi.org/10.1006/jnth.1998.2350.

[16] L.-C. Kappe and B. Warren. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly*, 96(2):133–137, 1989. ISSN 0002-9890. URL https://doi.org/10.2307/2323198.

[17] P. Olajos. Power integral bases in the family of simplest quartic fields. *Experiment. Math.*, 14(2):129–132, 2005. ISSN 1058-6458. URL http://projecteuclid.org/euclid.em/1128100125.

[18] K. Prachar. Über die kleinste quadratfreie Zahl einer arithmetischen Reihe. *Monatsh. Math.*, 62:173–176, 1958. URL https://doi.org/10.1007/BF01301288.

[19] B. K. Spearman. Monogenic A_4 quartic fields. *Int. Math. Forum*, 1(37-40): 1969–1974, 2006. ISSN 1312-7594. doi: 10.12988/imf.2006.06174. URL http://dx.doi.org/10.12988/imf.2006.06174.

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

E-mail address: hanson.smith@colorado.edu