TOWARDS VAN DER WAERDEN'S CONJECTURE

SAM CHOW AND RAINER DIETMANN

ABSTRACT. How often is a quintic polynomial solvable by radicals? We establish that the number of such polynomials, monic and irreducible with integer coefficients in $[-H, H]$, is $O(H^{3.91})$. More generally, we show that if $n \geqslant 3$ and $n \notin \{7, 8, 10\}$ then there are $O(H^{n-1.017})$ monic, irreducible polynomials of degree n with integer coefficients in $[-H, H]$ and Galois group not containing A_n. Save for the alternating group and degrees $7, 8, 10$, this establishes a 1936 conjecture of van der Waerden.

1. INTRODUCTION

1.1. Counting solvable quintics.

By the Abel–Ruffini theorem, there are integer quintic polynomials that cannot be solved by radicals. But how often is a quintic polynomial solvable by radicals?

Let H be a large, positive real number. In this article, one objective is to count monic, irreducible quintic polynomials

$$f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \qquad (1.1)$$

that are solvable by radicals, where $a, b, c, d, e \in \mathbb{Z} \cap [-H, H]$, denoting their number by $N(H)$. It follows from a more general result [23, Theorem 1] that $N(H) \ll_\varepsilon H^{\varepsilon + 25/6}$, and we are able to improve upon this.

Theorem 1.1. *We have*
$$N(H) \ll_\varepsilon H^{\varepsilon + 7/2 + 1/\sqrt{6}} \leqslant H^{3.91}.$$

We will see that H^4 is a significant threshold.

The Galois group of a separable polynomial is the automorphism group of its splitting field [21, §6.3]. An irreducible polynomial is solvable by radicals if and only if its Galois group is a solvable group. In this way, the question posed can be viewed through the lens of *enumerative Galois theory*, a topic in arithmetic statistics concerned with the frequency of Galois groups of polynomials or number fields.

Enumerative Galois theory for polynomials has a long history. It follows from Hilbert's irreducibility theorem [31] that the number $\mathcal{E}_n(H)$ of monic, irreducible, non-S_n integer polynomials with coefficients in $[-H, H]$ is $o(H^n)$ as $H \to \infty$. In 1936, van der Waerden showed that

$$\mathcal{E}_n(H) \ll_n H^{n-1/(6(n-2)\log\log H)},$$

and conjectured that $\mathcal{E}_n(H) = o(R_n(H))$ as $H \to \infty$, where $R_n(H)$ counts reducible polynomials [45]. We know that if $n \geqslant 3$ then

$$R_n(H) = c_n H^{n-1} + O(H^{n-2}(\log H)^2),$$

where c_n is a positive constant, see [13] and [15, Appendix B]. Thus, van der Waerden's conjecture can be equivalently stated as follows.

Conjecture 1.2 (van der Waerden 1936). *For $n \geqslant 3$, we have*

$$\mathcal{E}_n(H) = o(H^{n-1}) \qquad as\ H \to \infty.$$

Remark 1.3. Since the initial release of this manuscript, Bhargava has resolved a weak form of van der Waerden's conjecture [5], namely that $\mathcal{E}_n(H) \ll_n H^{n-1}$. The present article concerns a stronger form of the conjecture, that $\mathcal{E}_n(H) = o(H^{n-1})$. Van der Waerden [45] wrote that "Es scheint nämlich, daß die irreduziblen Polynome mit Affekt noch erheblich seltener sind als die reduziblen Polynome", speculating that irreducible non-S_n polynomials are substantially rarer than reducible polynomials.

In [24], the second named author showed that if $n \geqslant 3$ then

$$\mathcal{E}_n(H) \ll_{n,\varepsilon} H^{\varepsilon+n-2+\sqrt{2}},$$

breaking a record previously held by van der Waerden [45], Knobloch [33], Gallagher [27] and Zywina [49]. Recently, we settled the cubic and quartic cases of van der Waerden's conjecture.

Theorem 1.4 (From [15]). *Van der Waerden's conjecture holds for $n = 3$ and $n = 4$. Moreover, we have*

$$H \ll \mathcal{E}_3(H) \ll_\varepsilon H^{\varepsilon+3/2}, \qquad H^2(\log H)^2 \ll \mathcal{E}_4(H) \ll H^{\varepsilon+5/2+1/\sqrt{6}} \ll H^{2.91}$$

S. Xiao [48] was able to prove a stronger bound in the cubic case, namely $\mathcal{E}_3(H) \ll H(\log H)^2$.

More generally, how often does each group occur as the Galois group of a polynomial of a fixed degree $n \geqslant 3$? For $G \leqslant S_n$, let us write $N_{G,n} = N_{G,n}(H)$ for the number of monic, irreducible, integer polynomials, with coefficients bounded by H in absolute value, whose Galois group is conjugate to G. The second named author showed in [23] that

$$N_{G,n} \ll_{n,\varepsilon} H^{\varepsilon+n-1+1/[S_n:G]}. \tag{1.2}$$

The Galois group G_f of an irreducible polynomial f acts transitively on its roots [21, Proposition 6.3.7], that is, it is a transitive subgroup of S_n. This greatly limits the number of possibilities for the conjugacy class of G_f. For example, in the case $n = 5$ of quintic polynomials, the transitive subgroups of S_5 are:

- S_5, the full symmetric group on five elements, which has order 120 and is insolvable;
- A_5, the alternating group, which has order 60 and is insolvable;
- $\mathrm{AGL}(1, \mathbb{F}_5)$, the general affine group, which has order 20 and is solvable;
- D_5, the dihedral group of order 10, which is solvable; and
- C_5, the cyclic group of order 5, which is solvable.

As S_5 and A_5 are the only transitive subgroups of S_5 that are insolvable, Theorem 1.1 makes progress towards the quintic case of van der Waerden's conjecture. It implies that

$$N_{\mathrm{AGL}(1,\mathbb{F}_5),5} + N_{D_5,5} + N_{C_5,5} = N(H) \ll H^{3.91} = o(H^4) \tag{1.3}$$

so, for the quintic case of van der Waerden's conjecture, only A_5 remains. This is to say that we have the following consequence of Theorem 1.1.

Corollary 1.5. *If $N_{A_5,5} = o(H^4)$ then van der Waerden's conjecture holds for $n = 5$.*

For $s, t \in \mathbb{Z}$, the de Moivre quintic

$$X^5 + 5sX^3 + 5s^2X + t$$

has Galois group $\mathrm{AGL}(1, \mathbb{F}_5)$ whenever it is irreducible, see [21, Example 13.2.10]. It now follows from Eisenstein's criterion that

$$N_{\mathrm{AGL}(1,\mathbb{F}_5),5} \gg H^{3/2}.$$

As $\mathrm{AGL}(1, \mathbb{F}_5)$ is solvable, we thus obtain the following lower bound to complement the upper bound in Theorem 1.1.

Corollary 1.6. *We have*

$$N(H) \gg H^{3/2}.$$

1.2. **Sextic and higher-degree polynomials.** Save for the alternating group, we are able to prove van der Waerden's conjecture in any degree except for $7, 8, 10$. Here is our main theorem.

Theorem 1.7 (Main Theorem). *If $n \geqslant 3$ and $n \notin \{7, 8, 10\}$ then there are $O(H^{n-1.017})$ monic, irreducible polynomials of degree n with integer coefficients in $[-H, H]$ and Galois group not containing A_n.*

Corollary 1.8. *Let $n \geqslant 3$ with $n \notin \{7, 8, 10\}$, and suppose $N_{A_n,n} = o(H^{n-1})$ as $H \to \infty$. Then van der Waerden's conjecture holds in degree n.*

When $n = 9$ or $n \geqslant 11$, we reach Theorem 1.7 via the index of G.

Theorem 1.9. *Let $n = 9$ or $n \geqslant 11$, let G be a transitive subgroup of S_n that does not contain A_n, and put $d = [S_n : G]$. Then $d \geqslant 240$, and*

$$N_{G,n} \ll_{n,\varepsilon} H^{n+\varepsilon-3/2+3d^{-1/3}} \leqslant H^{n-1.017}.$$

In the sextic case, we have the following estimates.

Theorem 1.10. *Let G be a transitive subgroup of S_6 that does not contain A_6. Then*

$$N_{G,6} \ll_\varepsilon H^{\varepsilon+9/2+1/\sqrt{6}} \leqslant H^{4.91}.$$

Moreover, if G is solvable then

$$N_{G,6} \ll_\varepsilon H^{\varepsilon+9/2+1/\sqrt{10}} \leqslant H^{4.82}.$$

Corollary 1.11. *There are $O(H^{4.82})$ monic, irreducible, solvable sextic polynomials with integer coefficients in $[-H, H]$.*

Note that Theorem 1.7 follows from Theorems 1.1, 1.4, 1.9 and 1.10. We can also handle proper subgroups of the alternating group, exploiting the additional information that the discriminant is a square.

Theorem 1.12. *Let $n \geqslant 3$ with*

$$n \notin \{u^2, u^2 + 1\} \qquad (u \in \mathbb{N} \text{ odd}). \tag{1.4}$$

Let G be a proper, transitive subgroup of A_n, and put $d = [S_n : G]$. Then $d \geqslant 6$ and

$$N_{G,n} \ll_{n,\varepsilon} H^{\varepsilon+n-3/2+1/\sqrt{d}} \leqslant H^{n-1.09}.$$

In particular, the theorem applies when $n \in \{7, 8\}$. For each $n \in \{7, 8, 10\}$, these being the exceptional degrees in Theorem 1.7, this leaves just one conjugacy class of G not containing A_n for which we do not know that $N_G = o(H^{n-1})$. These are called 7T4, 8T47 and 10T43, see the tables of Butler and McKay [12]. It is probable that the condition (1.4) can be removed through further reasoning, see [25, §6].

1.3. **Methods.** We approach the problem from the perspective of diophantine equations. Recall that cubic and quartic polynomials were treated in [15].

1.3.1. *Quintic polynomials.* We begin by introducing a standard invariant $\Delta = \Delta_f$ of a monic quintic polynomial f, the *discriminant*, and a standard auxiliary polynomial $\theta = \theta_f$, the *sextic resolvent*. If f is solvable, then θ has a rational root [21, Corollary 13.2.11], which must in fact be an integer as a consequence of f being monic. By introducing this root y as an additional variable, we obtain a diophantine equation. If f has coefficients in $[-H, H]$, then we will see that $y \ll H^2$. With the coefficients as in (1.1) we show that, for generic a, b, c, the vanishing of $\theta(a, b, c, d, e, y)$ defines an absolutely irreducible surface in $\mathbb{A}^3_{d,e,y}$ containing no rational lines. We need to count integer points on this surface, bounded by a rectangle of dimensions $2H, 2H, O(H^2)$, uniformly in a, b, c. We achieve this using the *determinant method*. Pioneered by Bombieri and Pila who studied planar curves [8], this has seen a number of developments over the years, and enables us to cover the overwhelming majority of these integer points by a relatively small number of curves, which eventually turns out to be decisive. Specifically, we use Browning's version [10, Lemma 1], which relies on deep work of Salberger, see Theorem 2.5.

1.3.2. *Sextic polynomials.* We approach sextic polynomials in much the same way as we approach quintic polynomials. The resolvents are much more complicated, to the extent that they are inconvenient to print in expanded form. We computed and manipulated them using the software *Mathematica* [46]. The case of insolvable sextics is more demanding both technically and computationally; one of the steps is to show that our surfaces generically lack certain low-degree curves.

1.3.3. *Higher-degree polynomials.* In this case we have general resolvents Φ_G from [23] and [14]. If the Galois group is G, then Φ_G has an integer root, which we introduce as an extra variable to obtain a diophantine equation in y and the coefficients of f. Fixing all but three of the coefficients of f generically furnishes an absolutely irreducible threefold. We can cover its integer points up to height H by a relatively small number of surfaces, using a determinant method result of Heath-Brown's [30, Theorem 15]. A result of Pila's [38] enables us to efficiently count integer points on an irreducible component of such a surface, unless it happens to be linear. The latter scenario concerns a two-parameter family of polynomials, whose Galois theory can be understood over the two-parameter function field using the framework developed by Uchida [44], J. H. Smith [42] and S. D. Cohen [17, 18]. Refining the separable resolvent theory of [14], we are led to the problem of counting integer points on an irreducible, high-degree surface in a lopsided box. We complete the proof by establishing a lopsided version of Pila's theorem [38] in a special case. To achieve the latter we first establish an almost-uniform, quantitative version of Hilbert's irreducibility theorem, refining a case of [19, Theorem 2.1].

For the lopsided version version of Pila's theorem and for the almost-uniform, quantitative version of Hilbert's irreducibility theorem, see §6. For Galois theory over two-parameter function fields, we find that the Galois group of

$$f(X) = G_0(X) + aG_1(X) + bG_2(X)$$

over $\mathbb{C}(a, b)$ is S_n in the following two new cases, assuming that f is irreducible over $\mathbb{Q}(a, b)$, for any $n \geqslant 6$, any $\alpha, \beta, \gamma \in \mathbb{Q}$ and any $a_1, \ldots, a_{n-3} \in \mathbb{Z}$ for which we have (7.3):

(i)

$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 - \alpha, \quad G_1(X) = X^2 - \beta, \quad G_2(X) = X - \gamma$$

(ii)

$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 - \alpha, \quad G_1(X) = X^2 - \beta, \quad G_2(X) = 1.$$

1.4. **Variants.** Enumerative Galois theory for number fields is another thriving area of research, and one that is closely related to enumerative Galois theory for polynomials [34, 36, 47]. There are some subtle differences between the two types of problem, for instance Bhargava [4] famously showed that a positive proportion of quartic fields fail to have full Galois group S_4. One can also try to relax the condition of the polynomial being monic, equivalently counting binary forms. Different heights can be considered, for example heights that respect linear transformations, or that are more compatible with other arithmetic statistics such as number fields, class groups, and ranks of elliptic curves [6, 7, 47, 48]. More general probability distributions for the coefficients have been considered in [37]. Recently there have been substantial developments in the problem with small coefficients and large degree [1, 2, 9]. There have also been some nice results on the distribution of Galois groups of characteristic polynomials of matrices [26, 32, 39].

1.5. **Organisation.** We discuss finer aspects of the methods in §2. We prove Theorem 1.1 in §3. In §4, we discuss the role of separable resolvents, and extend the existing work [14, 23] on this topic. Theorem 1.10 is proved in §5. In §6, we establish an almost-uniform version of Hilbert's irreducibility theorem and a lopsided version of Pila's theorem, as well as making preparations for Galois theory over two-parameter function fields. Then, in §7, we establish Theorem 1.9. Finally, in §8, we prove Theorem 1.12.

1.6. **Notation.** We adopt the convention that ε denotes an arbitrarily small positive constant, whose value is allowed to change between occurrences. We use the Vinogradov and Bachmann–Landau notations throughout, the implicit constants being allowed to depend on ε. Throughout H denotes a positive real number, sufficiently large in terms of ε. If F is a polynomial with complex coefficients then $|F|$ is the greatest absolute value of its coefficients.

1.7. **Funding and acknowledgements.** SC was supported by EPSRC Fellowship Grant EP/S00226X/2, and by the Swedish Research Council under grant no. 2016-06596. We thank an anonymous referee for detailed feedback, and Bijay Bhatta for drawing our attention to a significant typo.

2. Further discussion of the methods

2.1. **Resolvents.** Let
$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X].$$
A *resolvent* is an auxiliary polynomial $\Phi(Y)$ whose factorisation type provides information about the Galois group of f. The resolvents that we use in this manuscript have a specific property; to a transitive subgroup G of S_n, we associate $\Phi = \Phi_G$ such that if $G_f \leqslant G$ then Φ has a root $y \in \mathbb{Z}$. To show that the condition $G_f \leqslant G$ is unlikely, we count integer solutions to
$$\Phi(y; a_1, \ldots, a_n) = 0, \tag{2.1}$$
subject to size constraints. For us, these constraints always have the shape
$$|a_1|, \ldots, |a_n| \leqslant H, \qquad y \ll H^{O(1)}.$$

2.2. **The determinant method.** The next step is to fix all but two or three of the variables $a_1, \ldots, a_n$ in some generic way, so that the resulting surface or threefold is absolutely irreducible. This simplifies our problem substantially, but on the other hand its coefficients are now of size $H^{O(1)}$ instead of being constant. The *determinant method* is a versatile approach to counting integer points on varieties, with good uniformity in the coefficients. This makes it an ideal weapon for our approach.

The archetypal application of the determinant method is the following theorem [8].

Theorem 2.1 (Bombieri–Pila 1989). *Let C be an absolutely irreducible algebraic curve of degree $d \geqslant 2$ in $\mathbb{R}^2$. Then the number of integer points in $C \cap [-H, H]^2$ is $O_{d,\varepsilon}(H^{\varepsilon+1/d})$.*

We use this and its lopsided generalisation, as stated in [23, Lemma 8]. This was essentially given by Browning and Heath-Brown [11], however a short argument has been incorporated in order to relax the absolute irreducibility requirement to irreducibility over $\mathbb{Q}$.

Theorem 2.2 (Lopsided Bombieri–Pila). *Let $F \in \mathbb{Z}[x_1, x_2]$ be irreducible over $\mathbb{Q}$ and have degree $d \in \mathbb{N}$. Further, let $B_1, B_2 \geqslant 1$, and define*

$$N(F; B_1, B_2) = \#\{\mathbf{x} \in \mathbb{Z}^2 : F(\mathbf{x}) = 0, |x_i| \leqslant B_i \ (1 \leqslant i \leqslant 2)\}.$$

Put

$$T = \max\left\{B_1^{e_1} B_2^{e_2}\right\},$$

where the maximum is taken over all $(e_1, e_2) \in \mathbb{Z}_{\geqslant 0}^2$ for which $x_1^{e_1} x_2^{e_2}$ occurs in $F(\mathbf{x})$ with non-zero coefficient. Then

$$N(F; B_1, B_2) \ll_{d,\varepsilon} T^\varepsilon \exp\left(\frac{\log B_1 \cdot \log B_2}{\log T}\right).$$

Pila [38] subsequently generalised Theorem 2.1.

Theorem 2.3 (Pila 1995, special case). *Let $N \geqslant 2$ be an integer, and let V be an irreducible affine hypersurface in $\mathbb{R}^N$ of degree $d \geqslant 2$. Then the number of integer points in $V \cap [-H, H]^N$ is $O_{N,d,\varepsilon}(H^{N-2+\varepsilon+1/d})$.*

We establish a lopsided variant of this, see Theorem 6.3, which we use in our proof of Theorem 1.9.

A key idea in the determinant method is to cover the integer points on a variety by lower-dimensional varieties. A famous result of this type is Heath-Brown's [30, Theorem 15], which is also lopsided.

Theorem 2.4 (Heath-Brown 2006). *Let $N \geqslant 2$ be an integer. Suppose $F(x_1, \ldots, x_N) \in \mathbb{Z}[\mathbf{x}]$ defines an absolutely irreducible hypersurface of degree $d \in \mathbb{N}$. Let $B_1, \ldots, B_N \geqslant 1$. Put*

$$T = \max\left\{\prod_{i \leqslant N} B_i^{e_i}\right\},$$

where the maximum is taken over all $(e_1, ..., e_N) \in \mathbb{Z}_{\geqslant 0}^N$ for which $x_1^{e_1} \cdots x_N^{e_N}$ occurs in $F(\mathbf{x})$ with non-zero coefficient. Then there exist $g_1, \ldots, g_J \in \mathbb{Z}[\mathbf{x}]$, each coprime to F and of degree $O_{N,d,\varepsilon}(1)$, where

$$J \ll_{N,d,\varepsilon} T^\varepsilon \exp\left\{(N-1)\left(\frac{\prod \log B_i}{\log T}\right)^{1/(N-1)}\right\} (\log |F|)^{2N-3},$$

such that if $\mathbf{x} \in ([-B_1, B_1] \cap \mathbb{Z}) \times \cdots \times [-B_N, B_N] \cap \mathbb{Z})$ and $F(\mathbf{x}) = 0$ then $g_j(\mathbf{x}) = 0$ for some j.

Note that T will be larger, and the bound on J stronger, if d is large. This is the case for our resolvents when n is large, and so we apply Theorem 2.4 with $N = 4$ in our proof of Theorem 1.9. We will find that $|F| \ll H^{O(1)}$ in our applications, and it is essential that we have a bound of this flavour.

In the case $N = 3$ of surfaces, the factor of $N - 1$ can be removed at the expense of introducing a small exceptional set, using Salberger's rather sophisticated adelic machinery. The mild dependence on $|F|$ can also be removed in this case. Such a result was formulated by Browning in [10, Lemma 1].

Theorem 2.5 (Browning 2011). *Suppose $F(x_1, x_2, x_3) \in \mathbb{Z}[\mathbf{x}]$ defines an absolutely irreducible surface of degree $d \in \mathbb{N}$, and let $B_1, B_2, B_3 \geqslant 1$. Put*

$$T = \max \left\{ B_1^{e_1} B_2^{e_2} B_3^{e_3} \right\},$$

where the maximum is taken over all $(e_1, e_2, e_3) \in \mathbb{Z}_{\geqslant 0}^3$ for which $x_1^{e_1} x_2^{e_2} x_3^{e_3}$ occurs in $F(\mathbf{x})$ with non-zero coefficient, and also put

$$V_3 = \exp \left\{ \left(\frac{\log B_1 \cdot \log B_2 \cdot \log B_3}{\log T} \right)^{1/2} \right\}.$$

Then there exist $g_1, \ldots, g_J \in \mathbb{Z}[\mathbf{x}]$ and $Z \subset \mathbb{Z}^3$, with

$$J \ll_{d,\varepsilon} T^\varepsilon V_3, \qquad |Z| \ll_{d,\varepsilon} T^\varepsilon V_3^2,$$

such that the following hold:

(i) Each g_j is coprime to F and has degree $O_{d,\varepsilon}(1)$;
(ii) If $\mathbf{x} \in ([-B_1, B_1] \cap \mathbb{Z}) \times ([-B_2, B_2] \cap \mathbb{Z}) \times ([-B_3, B_3] \cap \mathbb{Z}) \setminus Z$ and $F(\mathbf{x}) = 0$ then $g_j(\mathbf{x}) = 0$ for some j.

It remains an open problem to achieve such a refinement for larger N. In particular, our methods would be more effective if we had it in the case $N = 4$ of threefolds.

As mentioned, uniformity in the coefficients is a key strength of the determinant method. We close this subsection with a brief discussion of the level of uniformity required for our arguments to succeed. Observe that a factor of $(\log |F|)^{2N-3}$ appears in Theorem 2.4. Consequently, we require that

$$\log |F| \ll H^\varepsilon.$$

As discussed, we will see that we have $|F| \ll H^{O(1)}$ in practice, which is even stronger.

2.3. Covering integer points on surfaces by curves.

We use an assortment of resolvents in the cases $n = 5$ and $n = 6$. Importantly, these are computationally tractable, in that we can manipulate the coefficients using mathematical software. To fix ideas, we focus our discussion on the case $n = 5$ of solvable quintics. We write our polynomial as

$$f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e,$$

and we recall the sextic resolvent θ from §1.3.1. We need to count integer solutions to

$$\theta(y; a, b, c, d, e) = 0$$

with $a, b, c, d, e \ll H$ and $y \ll H^2$. The idea is to fix a, b, c such that the vanishing of

$$g(d, e, y) = \theta(y; a, b, c, d, e)$$

defines an absolutely irreducible affine surface $Y_{a,b,c}$. We can show that this condition is generic, in a strong quantitative sense.

Theorem 2.5 enables us to cover the integer points of controlled height on $Y_{a,b,c}$ by a small number of curves, up to a small set of exceptional points. Such a curve has the form

$$g(d, e, y) = h(d, e, y) = 0,$$

for some polynomial h that is coprime to g. By elimination theory, we can work with an irreducible planar curve $\mathcal{C}_1$ given by $F(d, e) = 0$.

2.3.1. *Rational lines.* At this stage there is a marked dichotomy. If $\mathcal{C}_1$ is a line, then it can contain roughly H integer points up to height H, and the basic strategy of counting points on $\mathcal{C}_1$ is inadequate. If, however, the curve $\mathcal{C}_1$ is non-linear, then Theorem 2.2 would assure us that it contains $O(H^{\varepsilon+1/2})$ integer points up to height H.

If $\mathcal{C}_1$ is a line, then we can use its equation to obtain a planar curve $\mathcal{C}_2$ in y and one of the other variables, and we may assume that $\mathcal{C}_2$ is irreducible. If $\mathcal{C}_2$ is non-linear, then Theorem 2.2 delivers a satisfactory count. If $\mathcal{C}_2$ is linear, then the linear equations defining $\mathcal{C}_1$ and $\mathcal{C}_2$ entail that $Y_{a,b,c}$ contains a rational line. For generic a, b, c, we can show that the surface $Y_{a,b,c}$ does not contain a rational line, by comparing coefficients. However, this step is computer-assisted, so we are unable to carry it out if n is large. Thus, Theorem 1.9 requires an alternate strategy.

2.4. Covering integer points on threefolds by surfaces.
For larger values of n, we use a more general resolvent Φ, and we need to count integer solutions to

$$\Phi(y; a_1, \ldots, a_n) = 0$$

with $a_1, \ldots, a_n \ll H$ and $y \ll H^C$, where $C = O_n(1)$. The idea is to fix $a_1, \ldots, a_{n-3}$ such that the equation

$$\Phi(y; a_1, \ldots, a_{n-3}, a, b, c) = 0$$

defines an absolutely irreducible affine threefold $\mathcal{Y} = \mathcal{Y}_{a_1, \ldots, a_{n-3}}$. We can show that the latter condition is generic. Theorem 2.4 enables us to cover the integer points of controlled height on $\mathcal{Y}$ by a small number of surfaces.

We initially follow the approach of §2.3, giving $\mathcal{F}(a, b, c) = 0$ for some irreducible polynomial $\mathcal{F}$ of bounded degree. Theorem 2.3 yields

$$\#\{(a, b, c) \in (\mathbb{Z} \cap [-H, H])^3\} \ll H^{\varepsilon+3/2},$$

unless $\mathcal{F}$ is linear. If $\mathcal{F}$ is linear then this count can be as large as H^2, so a further idea is needed.

2.4.1. *Two-parameter function fields.* Using the linear equation $\mathcal{F} = 0$, we can write our original polynomial in the form

$$f(X) = G_0(X) + aG_1(X) + bG_2(X),$$

for some $a, b \in \mathbb{Z}$ and some polynomials G_0, G_1, G_2. Using the aforementioned framework of Uchida, Smith, and Cohen, we can show that

$$\mathrm{Gal}(f, \mathbb{C}(a, b)) = S_n.$$

This requires a two-parameter linear family of polynomials, which is why we initially fixed all but three of the variables $a_1, \ldots, a_n$, instead of all but two. We then have

$$\mathrm{Gal}(f, \mathbb{Q}(a, b)) = S_n.$$

Using resolvents, we can finally deduce that a generic polynomial in this two-parameter linear family has Galois group S_n.

2.5. Comparing the two approaches.
As discussed, the method of §2.3 fails for higher degrees because of its machine dependence. To see why the strategy of §2.4 fails for lower degrees, we return to the points made in §2.2. Heath-Brown's Theorem 2.4 incurs an additional factor of $N - 1 = 3$ in the exponent, and will only prevail for us if the index $d = [S_n : G]$ is large. If G does not contain A_n and $n \geqslant 12$, for instance, then we know from [23, Lemma 3] that $d \geqslant 462$. This is why the method of §2.4 is more effective when the degree is large.

3. Counting solvable quintics

3.1. **The sextic resolvent.** In this subsection, we introduce the basic objects and definitions needed for Theorem 1.1. The *discriminant* of f given by (1.1) is an octic polynomial in a, b, c, d, e, explicitly given by

$$
\begin{aligned}
\Delta = {}& 256a^5e^3 - 192a^4bde^2 - 128a^4c^2e^2 + 144a^4cd^2e - 27a^4d^4 + 144a^3b^2ce^2 - 6a^3b^2d^2e - 80a^3bc^2de + 18a^3bcd^3 \\
& - 1600a^3be^3 + 16a^3c^4e - 4a^3c^3d^2 + 160a^3cde^2 - 36a^3d^3e - 27a^2b^4e^2 + 18a^2b^3cde - 4a^2b^3d^3 - 4a^2b^2c^3e \\
& + a^2b^2c^2d^2 + 1020a^2b^2de^2 + 560a^2bc^2e^2 - 746a^2bcd^2e + 144a^2bd^4 + 24a^2c^3de - 6a^2c^2d^3 + 2000a^2ce^3 - 50a^2d^2e^2 \\
& - 630ab^3ce^2 + 24ab^3d^2e + 356ab^2c^2de - 80ab^2cd^3 + 2250ab^2e^3 - 72abc^4e + 18abc^3d^2 - 2050abcde^2 + 160abd^3e \\
& - 900ac^3e^2 + 1020ac^2d^2e - 192acd^4 - 2500ade^3 + 108b^5e^2 - 72b^4cde + 16b^4d^3 + 16b^3c^3e - 4b^3c^2d^2 - 900b^3de^2 \\
& + 825b^2c^2e^2 + 560b^2cd^2e - 128b^2d^4 - 630bc^3de + 144bc^2d^3 - 3750bce^3 + 2000bd^2e^2 + 108c^5e - 27c^4d^2 \\
& + 2250c^2de^2 - 1600cd^3e + 256d^5 + 3125e^4.
\end{aligned}
$$

Denote by θ the *sextic resolvent* [21, Chapter 13], explicitly given by

$$
\theta(y) = \theta(a, b, c, d, e, y) = (y^3 + B_2y^2 + B_4y + B_6)^2 - 2^{10}\Delta y,
$$

where

$$
\begin{aligned}
B_2 &= 8ac - 3b^2 - 20d, \\
B_4 &= 3b^4 - 16ab^2c + 16a^2c^2 + 16bc^2 + 16a^2bd - 8b^2d \\
&\quad - 112acd + 240d^2 - 64a^3e + 240abe - 400ce,
\end{aligned}
$$

and

$$
\begin{aligned}
B_6 = {}& 8ab^4c - b^6 - 16a^2b^2c^2 - 16b^3c^2 + 64abc^3 - 64c^4 - 16a^2b^3d + 28b^4d + 64a^3bcd \\
& - 112ab^2cd - 128a^2c^2d + 224bc^2d - 64a^4d^2 + 224a^2bd^2 - 176b^2d^2 - 64acd^2 + 320d^3 \\
& + 48ab^3e - 192a^2bce - 80b^2ce + 640ac^2e + 384a^3de - 640abde - 1600cde \\
& - 1600a^2e^2 + 4000be^2.
\end{aligned}
$$

This is an integer polynomial that is sextic in y. If

$$
a, b, c, d, e \in \mathbb{Z}, \qquad |a|, |b|, |c|, |d|, |e| \leqslant H,
$$

and G_f is solvable, then θ has an integer root y. Then $y \ll H^2$, for if $|y| > CH^2$ for a large constant C then

$$
y^6 \ll \Delta|y| \ll H^8|y|,
$$

contradicting that $|y| > CH^2$.

To estimate the number of integers solutions to $\theta(a, b, c, d, e, y) = 0$ with $a, b, c, d, e \ll H$ and $y \ll H^2$, we begin by choosing $a, b, c \ll H$. The vanishing of $\theta(a, b, c, d, e, y)$ then cuts out an affine surface $Y_{a,b,c}$. A heuristic application of the determinant method, cf. [15, §5], suggests that we should eventually conclude that there are $O(H^{\varepsilon+7/2+1/\sqrt{6}})$ solutions. In order to formalise this, there are two types of triples (a, b, c) to consider. The first is the *degenerate* type, where $Y_{a,b,c}$ either contains a rational line or is not absolutely irreducible. The second is the *non-degenerate* type, where $Y_{a,b,c}$ is absolutely irreducible and contains no rational lines.

3.2. **Non-degenerate triples.** In this subsection, we show that there are $O(H^{\varepsilon+7/2+1/\sqrt{6}})$ integer quintuples $(a, b, c, d, e) \in [-H, H]^5$ such that (a, b, c) is non-degenerate and f as given

by (1.1) is irreducible and solvable. First choose a non-degenerate triple (a, b, c) in one of $O(H^3)$ possible ways. Let

$$g(d, e, y) = y^6 + \sum_{i=0}^{5} c_i(d, e)y^i$$

be $\theta(a, b, c, d, e, y)$ specialised to values of a, b, c, so that $Y_{a,b,c}$ is defined by the vanishing of g. With C a large, positive constant, invoking the determinant method enables us to essentially cover

$$Y_{a,b,c} \cap ([-H, H] \cap \mathbb{Z})^2 \times ([-CH^2, CH^2] \cap \mathbb{Z})$$

by a controlled number of curves, with estimates that are uniform in a, b, c. By Theorem 2.5, there exist $g_1, \ldots, g_J \in \mathbb{Z}[d, e, y]$, and $Z = Z_{a,b,c} \subset \mathbb{Z}^3$, with $J \ll H^{\varepsilon + 1/\sqrt{6}}$ and $|Z| \ll H^{\varepsilon + 2/\sqrt{6}}$, such that the following hold:

(i) Each g_j is coprime to g and has degree $O(1)$;
(ii) If $(d, e, y) \in Y_{a,b,c} \cap ([-H, H] \cap \mathbb{Z})^2 \times ([-CH^2, CH^2] \cap \mathbb{Z}) \setminus Z$ then

$$g(d, e, y) = g_j(d, e, y) = 0 \tag{3.1}$$

for some j.

The total contribution from (a, b, c) non-degenerate and $(d, e, y) \in Z_{a,b,c}$ is

$$O(H^{3+\varepsilon+2/\sqrt{6}}) \ll H^{\varepsilon+7/2+1/\sqrt{6}},$$

so it remains to count solutions to (3.1), given j.

If $\deg_y(g_j) = 0$ then let $F(d, e) = g_j(d, e, y)$. Otherwise, let $F(d, e)$ be the resultant of g and g_j in the variable y. By [22, Chapter 3, §6, Proposition 3], applied with k as the fraction field of $\mathbb{Z}[d, e]$, this is a non-zero element of $\mathbb{Z}[d, e]$. By [22, Chapter 3, §6, Proposition 5], we have $F(d, e) = 0$ for any solution (d, e, y) to (3.1).

Observe that $F(d, e) = 0$ if and only if we have $\mathcal{F}(d, e) = 0$ for some irreducible divisor $\mathcal{F}(d, e) \in \mathbb{Q}[d, e]$ of $F(d, e)$. If $\mathcal{F}(d, e)$ is non-linear, then Theorem 2.2 gives

$$\#\{(d, e) \in (\mathbb{Z} \cap [-H, H])^2 : \mathcal{F}(d, e) = 0\} \ll H^{\varepsilon + 1/2}.$$

Then y is determined by $g(d, e, y) = 0$ in at most six ways, so the number of solutions (d, e, y) is $O(H^{\varepsilon+1/2})$, and the contribution from this case is $O(H^{\varepsilon+7/2+1/\sqrt{6}})$.

Suppose instead that $\mathcal{F}(d, e)$ is linear. Then

$$\alpha d + \beta e + \gamma = 0,$$

for some $(\alpha, \beta, \gamma) \in (\mathbb{Q}^2 \setminus \{(0,0)\}) \times \mathbb{Q}$. If $\beta \neq 0$ then substitute $e = -\beta^{-1}(\alpha d + \gamma)$ into $g(d, e, y) = 0$, giving

$$y^6 + \sum_{i=0}^{5} P_i(d)y^i = 0, \tag{3.2}$$

where

$$P_i(d) = c_i(d, -\beta^{-1}(\alpha d + \gamma)) \in \mathbb{Q}[d] \qquad (0 \leqslant i \leqslant 5).$$

Factorise the left hand side of (3.2) over $\mathbb{Q}$, and let $\mathcal{P}(d, y) \in \mathbb{Q}[d, y]$ be an irreducible factor. Note that $\mathcal{P}(d, y)$ is non-linear, for if it were linear then

$$\mathcal{P}(d, y) = \mathcal{F}(d, e) = 0$$

would define a rational linear subvariety of $Y_{a,b,c}$, of dimension greater than or equal to 1, contradicting the non-degeneracy of (a, b, c). Now Theorem 2.2 yields

$$\#\{(d, y) \in \mathbb{Z}^2 \cap [-H, H] \times [-CH^2, CH^2] : \mathcal{P}(d, y) = 0\} \ll H^{\varepsilon + 2/D},$$

where C is a large, positive constant and $D = \max\{\deg_d(\mathcal{P}), 2\deg_y(\mathcal{P})\} \geqslant 2$.

If $D \geqslant 4$ then the bound is adequate, so we may suppose that $D \in \{2, 3\}$, and in particular $\deg_y(\mathcal{P}) \leqslant 1$. As $\mathcal{P}(d, y)$ divides

$$y^6 + \sum_{i=0}^{5} P_i(d)y^i,$$

we infer that $\mathcal{P}(d, y)$ is a rational multiple of $y - F(d)$, where $F(d) \in \mathbb{Q}[d]$ has degree 2 or 3. Thus, we may assume that

$$\mathcal{P}(d, y) = y - F(d).$$

Next, write

$$(y - F(d))\left(y^5 + \sum_{i=0}^{4} f_i(d)y^i\right) = y^6 + \sum_{i=0}^{5} P_i(d)y^i.$$

For $i = 2, 4, 6$, let

$$b_i(d) = B_i(a, b, c, d, -\beta^{-1}(\alpha d + \gamma)),$$

and also write

$$\mathcal{D}(d) = 2^{10}\Delta(a, b, c, d, -\beta^{-1}(\alpha d + \gamma)).$$

Now

$$(y - F(d))\left(y^5 + \sum_{i=0}^{4} f_i(d)y^i\right) = (y^3 + b_2(d)y^2 + b_4(d)y + b_6(d))^2 - \mathcal{D}(d)y.$$

Equating coefficients in y yields

$$f_4(d) - F(d) = 2b_2(d)$$
$$f_3(d) - f_4(d)F(d) = b_2(d)^2 + 2b_4(d)$$
$$f_2(d) - f_3(d)F(d) = 2b_2(d)b_4(d) + 2b_6(d)$$
$$f_1(d) - f_2(d)F(d) = b_4(d)^2 + 2b_2(d)b_6(d)$$
$$f_0(d) - f_1(d)F(d) = 2b_4(d)b_6(d) - \mathcal{D}(d)$$
$$-f_0(d)F(d) = b_6(d)^2.$$

As $\deg(F) = D \geqslant 2$ and $\deg(b_2) = 1$, we must have $\deg(f_4) = D$. As $\deg(b_4) = 2$, we must then have $\deg(f_3) = 2D$. As $\deg(b_6) = 3$, we must then have $\deg(f_2) = 3D$, whereupon $\deg(f_1) = 4D$. Finally, as $\deg(\mathcal{D}) = 5$, we obtain $\deg(f_0) = 5D$, contradicting the final equation.

If instead $\beta = 0$, then we substitute $d = -\gamma/\alpha$ into $g(d, e, y) = 0$ and apply similar reasoning. This time

$$b_i(e) = B_i(a, b, c, -\gamma/\alpha, e) \qquad (i = 2, 4, 6),$$
$$\mathcal{D}(e) = 2^{10}\Delta(a, b, c, -\gamma/\alpha, e),$$

and

$$\deg(b_2) \leqslant 0, \qquad \deg(b_4) \leqslant 1, \qquad \deg(b_6) \leqslant 2, \qquad \deg(\mathcal{D}) = 4.$$

Then the argument of the $\beta \neq 0$ case carries through.

The upshot is that the contribution from (a, b, c) non-degenerate and $(d, e, y) \in Y_{a,b,c} \setminus Z_{a,b,c}$ is $O(H^3 J H^{\varepsilon + 1/2}) \ll H^{2\varepsilon + 7/2 + 1/\sqrt{6}}$. Having also considered the case $(d, e, y) \in Z_{a,b,c}$, we conclude that the total contribution from non-degenerate triples (a, b, c) is $O(H^{\varepsilon + 7/2 + 1/\sqrt{6}})$.

3.3. **Degenerate triples.** We now complete the proof of Theorem 1.1 by considering degenerate triples.

3.3.1. *Lines on the surface.* The idea is to show that, for generic a, b, c, the surface $Y_{a,b,c}$ contains no rational lines. A rational line on $Y_{a,b,c}$ has one of the following parametrisations:

   I. $\mathcal{L} = \{(0, \mathcal{E}, \mathcal{Y}) + t(1, E, Y) : t \in \mathbb{Q}\}$, for some $\mathcal{E}, \mathcal{Y}, E, Y \in \mathbb{Q}$;
  II. $\mathcal{L} = \{(\mathcal{D}, 0, \mathcal{Y}) + t(0, 1, Y) : t \in \mathbb{Q}\}$, for some $\mathcal{D}, \mathcal{Y}, Y \in \mathbb{Q}$;
 III. $\mathcal{L} = \{(\mathcal{D}, \mathcal{E}, 0) + t(0, 0, 1) : t \in \mathbb{Q}\}$, for some $\mathcal{D}, \mathcal{E} \in \mathbb{Q}$.

Let $g(d, e, y)$ be $\theta(a, b, c, d, e, y)$ specialised to the chosen values of a, b, c, so that $Y_{a,b,c}$ is defined by the vanishing of g. In each case, we substitute the parametrisation of the line into $g(d, e, y) = 0$ and expand it as a polynomial in t, and this has to be the zero polynomial.

In Case I, the polynomial has degree at most 6 in t, with sextic coefficient

$$(Y - 4)^4(Y^2 - 24Y + 400),$$

so $Y = 4$. After substituting this, the polynomial has degree at most 5 in t, with quintic coefficient

$$-20480(a - 5E)^4,$$

so $E = a/5$. After substituting this, the polynomial has degree at most 4 in t, with quartic coefficient

$$\frac{262144a^8}{125} - \frac{524288a^6b}{25} + \frac{393216a^4b^2}{5} - 131072a^2b^3 + 81920b^4.$$

Hence, there are $O(H^2)$ integer triples $(a, b, c) \in [-H, H]^3$ such that $Y_{a,b,c}$ contains a rational line of Type I.

In Case II, the polynomial has degree at most 6 in t, with sextic coefficient Y^6, so we must have $Y = 0$. Substituting this, and using the 'Eliminate' command in *Mathematica*, we see that the vanishing of the quartic, cubic, and quadratic coefficients determines an equation $P(a, b, c) = 0$, where $P \in \mathbb{Z}[a, b, c]$ is non-trivial of degree $O(1)$. Consequently, there are $O(H^2)$ integer triples $(a, b, c) \in [-H, H]^3$ such that $Y_{a,b,c}$ contains a rational line of Type II.

In Case III, the polynomial is monic and sextic, so Case III cannot occur. Having considered all cases, we conclude that there are $O(H^2)$ integer triples $(a, b, c) \in [-H, H]^3$ such that $Y_{a,b,c}$ contains a rational line.

3.3.2. *Absolute irreducibility.* The idea is to show that $Y_{a,b,c}$ is absolutely irreducible for generic a, b, c. It is easy to verify that $g(d, e, y) = \theta(a, b, c, d, e, y)$ is sextic in d, e, y, irrespective of a, b, c. It then follows from classical theory [40, Chapter V, Theorem 2A] that there exist integer polynomials $p_1(a, b, c), \ldots, p_s(a, b, c) \in \mathbb{Q}[a, b, c]$ of degree $O(1)$ such that if $a, b, c \in \mathbb{Q}$ then

$$Y_{a,b,c} \text{ is reducible over } \overline{\mathbb{Q}} \Leftrightarrow p_i(a, b, c) = 0 \ (1 \leqslant i \leqslant s).$$

The next lemma shows that p_i is non-zero for some i.

Lemma 3.1. $Y_{0,0,0}$ *is absolutely irreducible.*

Proof. The surface $Y_{0,0,0} \subset \mathbb{A}^3_{d,e,y}$ is cut out by the vanishing of

$$g(d, e, y) = (y^3 - 20dy^2 + 240d^2y + 320d^3)^2 - 1024(256d^5 + 3125e^4)y,$$

which is monic in y, so it suffices to show that $g(1, e, y)$ is absolutely irreducible. *Mathematica* assures us that

$$g(1, e, y) = 102400 - 108544y - 3200000e^4y + 44800y^2 - 8960y^3 + 880y^4 - 40y^5 + y^6$$

is irreducible over $\mathbb{Q}$. Moreover, its Newton polygon is the convex hull of $(0,0)$, $(0,1)$, $(4,1)$, $(0,2)$, $(0,3), (0,4), (0,5), (0,6)$, which has vertices $(0,0)$, $(0,6)$, $(4,1)$. The greatest common divisor of $0, 0, 0, 6, 4, 1$ is 1, so by [3, Proposition 3] we conclude that $g(1, e, y)$ is absolutely irreducible, as required. $\square$

Consequently, the triples (a, b, c) such that $Y_{a,b,c}$ is not absolutely irreducible are all zeros of a fixed non-zero polynomial of bounded degree. In particular, there are $O(H^2)$ such integer triples $(a, b, c) \in [-H, H]$.

3.3.3. *The sextic resolvent (reprise).* In the previous two subsubsections, we showed that there are $O(H^2)$ degenerate triples $(a, b, c) \in [-H, H]$. Let us now fix such a triple. Let $F(d, e; X)$ be $f(a, b, c, d, e; X)$ specialised to our fixed values of the coefficients a, b, c. By [23, Lemma 2], there are $O(1)$ values of $d \in \mathbb{Z}$ for which $F(d, e; X) \in \mathbb{Q}(e)[X]$ has non-S_5 Galois group over $\mathbb{Q}(e)$, uniformly in a, b, c. The contribution to $N(H)$ from these $O(1)$ special choices of d is $O(H^3)$, since there are $O(H)$ possibilities for e.

For the other $O(H)$ specialisations of d, the Galois group of $F(d, e; X) \in \mathbb{Q}(e)[X]$ is S_5. Having specialised d as well as a, b, c, we return to examine the sextic resolvent.

Lemma 3.2. *Let $a, b, c, d \in \mathbb{Z}$, and suppose that*

$$\mathrm{Gal}(X^5 + aX^4 + bX^3 + cX^2 + dX + e, \mathbb{Q}(e)) = S_5.$$

Then

$$h(e, y) := g(d, e, y) \in \mathbb{Z}[e, y]$$

is irreducible over $\mathbb{Q}$.

Proof. It follows from a generalisation of Hilbert's irreducibility theorem [19, Theorem 2.1] that for some $e_0 \in \mathbb{Z}$ we have

$$\mathrm{Gal}(X^5 + aX^4 + bX^3 + cX^2 + dX + e_0, \mathbb{Q}) = S_5.$$

Now, by [21, Proposition 13.2.7], the sextic resolvent $h(e_0, y) \in \mathbb{Z}[y]$ is irreducible over $\mathbb{Q}$.

Let us write

$$h(e, y) = y^6 + b_1(e)y^5 + \cdots + b_6(e),$$

where $b_1(e), \ldots, b_6(e) \in \mathbb{Z}[e]$, and suppose for a contradiction that h is reducible over $\mathbb{Q}$. Then

$$h(e, y) = (y^k + c_1(e)y^{k-1} + \cdots + c_k(e))(y^{6-k} + d_1(e)y^{5-k} + \cdots + d_{6-k}(e)) \in \mathbb{Q}[e, y],$$

for some $k \in \{1, 2, 3, 4, 5\}$ and some $c_1(e), \ldots, c_k(e), d_1(e), \ldots, d_{6-k}(e) \in \mathbb{Q}[e]$. Now

$$h(e_0, y) = (y^k + c_1(e_0)y^{k-1} + \cdots + c_k(e_0))(y^{6-k} + d_1(e_0)y^{5-k} + \cdots + d_{6-k}(e_0)),$$

contradicting the irreducibility of the univariate polynomial $h(e_0, y)$ over $\mathbb{Q}$. $\square$

As $h(e, y)$ contains the monomial y^6, Theorem 2.2 now gives

$$\#\{(e, y) \in \mathbb{Z}^2 : |e| \leqslant H, \ y \ll H^2, \ h(e, y) = 0\} \ll H^{\varepsilon+1/6}.$$

These specialisations of d therefore contribute $O(H^{\varepsilon+19/6})$ to $N(H)$.

We conclude that there are $O(H^{\varepsilon+19/6})$ quintuples $(a, b, c, d, e) \in (\mathbb{Z} \cap [-H, H])^5$, with (a, b, c) degenerate, such that $f(a, b, c, d, e; X) \in \mathbb{Z}[X]$ is solvable. This, coupled with the conclusion of §3.2, completes the proof of Theorem 1.1.

4. Separable and irreducible resolvents

Let $n \geqslant 3$ be an integer, and let G be a proper subgroup of S_n. In the sequel, we fix a total ordering of $\mathbb{C}$, so that the Galois group of an irreducible polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n = (X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{Z}[X] \tag{4.1}$$

is a well-defined subgroup of S_n, without any notion of equivalence.

A resolvent is an auxiliary polynomial whose factor type reveals information about the Galois group of the original polynomial. As a consequence of [21, Proposition 13.2.7], the

sextic resolvent that we saw in the previous section has the property of always being separable, as long as f is irreducible. It is easy to show that the quadratic resolvent $y^2 - \Delta$, where Δ is the discriminant, is a resolvent for the alternating group that also has this property. So too does the cubic resolvent of a quartic polynomial, which was used in [15], since a quartic polynomial has the same discriminant as its cubic resolvent. In general, however, it is not known whether an always separable resolvent exists for an arbitrary permutation group G.

Separability is a highly desirable property for a resolvent to have, see [21, §13.3]. It can be used to prove converse results of the type that if the resolvent has a rational root then G_f is conjugate to a subgroup of G. What we require here is stronger in a way, for example we want that if $G_f = S_n$ and the resolvent is separable then it is irreducible over the rationals. Separable resolvents are two-way bridges between Galois theory and diophantine equations. We hope that one day they will lead to Galois-theoretic Lefschetz principles, so that Cohen's p-adic machinery [17] can be brought to bear on the characteristic 0 setting. This article and the earlier works [14, 23] develop a framework for navigating some of these issues.

If $G_f = G$ then, by [23, Lemma 5], the polynomial

$$\Phi(y) = \Phi(y; a_1, \ldots, a_n) = \prod_{\sigma \in S_n/G} \left(y - \sum_{\tau \in G} \prod_{i \leqslant n} \alpha_{\sigma\tau(i)}^i \right) \in \mathbb{Z}[y; a_1, \ldots, a_n] \qquad (4.2)$$

has an integer root y. By [23, Lemma 1], if $a_1, \ldots, a_n \ll H$ then

$$y = \sum_{\tau \in G} \prod_{i \leqslant n} \alpha_{\sigma\tau(i)}^i \ll_n H^{O_n(1)} \qquad (4.3)$$

for some σ. We will see that the total degree of Φ is $O_n(1)$.

The more general family of resolvents

$$\Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}(y; a_1, \ldots, a_n) = \prod_{\sigma \in S_n/G} (y - r_{\mathbf{w},\mathbf{e},\mathfrak{g}}(\sigma)) \in \mathbb{Z}[y; a_1, \ldots, a_n],$$

where

$$r_{\mathbf{w},\mathbf{e},\mathfrak{g}}(\sigma) = \sum_{k \leqslant |G|} w_k \sum_{\tau \in G} \prod_{i \leqslant n} (\alpha_{\sigma\tau(i)} + \mathfrak{g})^{ke_i},$$

$\mathbf{w} = (w_1, \ldots, w_{|G|}) \in \mathbb{N}^{|G|}$, $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{N}^n$, and $\mathfrak{g} \in \mathbb{Z}$, was introduced in [14]. Here we establish some additional features, in particular with regards to uniformity.

Lemma 4.1. *If $G_f \leqslant G$, then Ψ has an integer root $y \ll_n \|\mathbf{w}\|_\infty (H + |\mathfrak{g}|)^{O_n(\|\mathbf{e}\|_\infty)}$. Finally, the total degree of Ψ is $O_n(1)$.*

Proof. For

$$y = \sum_{k \leqslant |G|} w_k \sum_{\tau \in G} \prod_{i \leqslant n} (\alpha_{\tau(i)} + \mathfrak{g})^{ke_i},$$

observe that if $\sigma \in G_f \leqslant G$ then $\sigma(y) = y$, and so $y \in \mathbb{Q}$ by the Galois correspondence. As Ψ is monic, we then have $y \in \mathbb{Z}$. The bound follows from [23, Lemma 1].

Put $d = [S_n : G]$. Writing

$$\Phi(y) = y^d + h_1(a_1, \ldots, a_n)y^{d-1} + \cdots + h_d(a_1, \ldots, a_n),$$

it remains to prove that $h_1, \ldots, h_d$ are bounded-degree polynomials. By Vieta's formulas, these are elementary symmetric polynomials in the roots $r_{\mathbf{w},\mathbf{e},\mathfrak{g}}(\sigma)$ of Ψ, up to sign. Given $i \in \{1, 2, \ldots, n\}$, the polynomial h_i has bounded degree in $\alpha_1, \ldots, \alpha_n$. From the proof of the fundamental theorem of symmetric polynomials [22, Chapter 7, §1, Theorem 3], any

symmetric polynomial of degree $O_n(1)$ in n variables also has degree $O_n(1)$ in the elementary symmetric polynomials. Therefore $\deg(h_i) \ll_n 1$. $\square$

The following is a refinement of [14, Lemma 3].

Lemma 4.2. *Let $C, P \in \mathbb{N}$ be large in terms of n, let $\mathfrak{g} = C^3 P$, and let $a_1, \dots, a_n \in [-P, P]$ be such that the roots $\alpha_1, \dots, \alpha_n$ of the polynomial $f(X) = X^n + a_1 X^{n-1} + \dots + a_n$ are pairwise distinct. Then there exist $\mathbf{w}, \mathbf{e}$, with $\|\mathbf{w}\|_\infty, \|\mathbf{e}\|_\infty \leqslant C$, such that $\Phi_{\mathbf{w}, \mathbf{e}, \mathfrak{g}}(y; a_1, \dots, a_n)$ is separable.*

Proof. We know from [23, Lemma 1] that if $|a_1|, \dots, |a_n| \leqslant P$ then
$$|\alpha_1|, \dots, |\alpha_n| \leqslant CP.$$

Let us introduce the notation
$$\omega_{\sigma, \tau, \mathbf{e}, \mathfrak{g}} = \prod_{i \leqslant n} (\alpha_{\sigma\tau(i)} + \mathfrak{g})^{e_i}.$$

Our immediate goal is to choose positive integers $e_1, \dots, e_n \leqslant C$ such that
$$\omega_{\sigma_1, \tau_1, \mathbf{e}, \mathfrak{g}} \neq \omega_{\sigma_2, \tau_2, \mathbf{e}, \mathfrak{g}}$$
whenever $\sigma_1 \neq \sigma_2$.

Let $\sigma_1, \sigma_2 \in S_n / G$ with $\sigma_1 \neq \sigma_2$, and let $\tau_1, \tau_2 \in G$. Then $\sigma_1 \tau_1 \neq \sigma_2 \tau_2$, so for some $i \in \{1, 2, \dots, n\}$ we have $\alpha_s \neq \alpha_t$, where $s = \sigma_1 \tau_1(i)$ and $t = \sigma_2 \tau_2(i)$. Moreover, if $\omega_{\sigma_1, \tau_1, \mathbf{e}, \mathfrak{g}} = \omega_{\sigma_2, \tau_2, \mathbf{e}, \mathfrak{g}}$ then
$$\left(\frac{\alpha_s + \mathfrak{g}}{\alpha_t + \mathfrak{g}} \right)^{e_i} = c,$$
for some $c = c(\boldsymbol{\alpha}, \mathfrak{g}, e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$. We claim that this has at most one positive integer solution $e_i \leqslant C$. The argument of $(\alpha_s + \mathfrak{g})/(\alpha_t + \mathfrak{g})$ is $O(C^{-2})$, and so its first C powers are pairwise distinct. This establishes the claim. As C is large and there are $O_n(C^{n-1})$ vectors to avoid out of C^n possibilities, we conclude that there exist $e_1, \dots, e_n \leqslant C$ with the desired property.

Finally, we may choose positive integers $w_1, \dots, w_{|G|} \leqslant C$ such that the roots
$$r_{\mathbf{w}, \mathbf{e}, \mathfrak{g}}(\sigma) = \sum_{k \leqslant |G|} w_k \sum_{\tau \in G} \omega_{\sigma, \tau, \mathbf{e}, \mathfrak{g}}^k$$
of $\Phi_{\mathbf{w}, \mathbf{e}, \mathfrak{g}}$ are pairwise distinct. This is achieved by avoiding $O_n(1)$ proper, linear subspaces, as in the proof of [14, Lemma 3]. $\square$

The following is a refinement of [14, Lemma 4].

Lemma 4.3. *Let*
$$g(T_1, \dots, T_s, X) \in \mathbb{Z}[T_1, \dots, T_s, X]$$
be separable and monic of degree $n \geqslant 1$ in the variable X, let G be its Galois group over $\mathbb{Q}(T_1, \dots, T_s)$, and let $K \leqslant G$. Let D be the total degree of g. Then there exists
$$\Phi_{g, K}(T_1, \dots, T_s, Y) \in \mathbb{Z}[T_1, \dots, T_s, Y]$$
of total degree $O_{s, D}(1)$, monic of degree $[S_n : K]$ in Y, such that:
  (i) Each irreducible divisor has degree at least $[G : K]$ in Y.
  (ii) If $t_1, \dots, t_s \in \mathbb{Z}$ and $g(t_1, \dots, t_s, X)$ has Galois group K over $\mathbb{Q}$ then $\Phi_{g, K}(t_1, \dots, t_s, Y)$ has an integer root $y \ll_D (|g| \cdot \|\mathbf{t}\|_\infty)^{O_D(1)}$.

Remark 4.4. As $n \in \{1, 2, \dots, D\}$, any dependence of implied constants on n is controlled by the dependence on D.

Proof. The discrimant Δ of g in Y is a non-zero polynomial of degree $O_D(1)$ in $T_1, \ldots, T_s$, so there exist integers $t_1, \ldots, t_s \ll_D 1$ such that $\Delta(t_1, \ldots, t_s) \neq 0$. We can then use Lemma 4.2 with $P \ll_D |g|$, in lieu of [14, Lemma 3], in the proof of [14, Lemma 4]. This constructs $\Phi_{g,K}$.

From the proof of the fundamental theorem of symmetric polynomials [22, Chapter 7, §1, Theorem 3], any symmetric polynomial of degree $O_s(1)$ in s variables also has degree $O_s(1)$ in the elementary symmetric polynomials. We will use this fact to show that the total degree of $\Phi_{g,K}$ is $O_{s,D}(1)$.

By construction, the total degree of $\Phi_{g,K}$ in $\alpha_1(T_1, \ldots, T_s), \ldots, \alpha_n(T_1, \ldots, T_s)$ from [14, Lemma 4] is $O_{s,n}(1)$. The total degree of $\Phi_{g,K}$ in $g_1(T_1, \ldots, T_s), \ldots, g_n(T_1, \ldots, T_s)$ from [14, Lemma 4] is therefore also $O_{s,n}(1)$, by the fact explained in the previous paragraph. Thus, the total degree in $T_1, \ldots, T_s$ is $O_{s,D}(1)$.

A root y of $\Phi_{g,K}$ has the form
$$y = \sum_{k \leqslant |K|} w_k \sum_{\tau \in G} \prod_{i \leqslant n} (\alpha_{\tau(i)} + \mathfrak{g})^{ke_i},$$
for some positive integers $w_1, \ldots, w_{|K|}, e_1, \ldots, e_n \ll_D 1$ and some integer $\mathfrak{g} \ll_D |g|$. By [23, Lemma 1] we have
$$\alpha_j \ll_n |g| \cdot \|\mathbf{t}\|_\infty^D \qquad (1 \leqslant j \leqslant n),$$
so $y \ll_D (|g| \cdot \|\mathbf{t}\|_\infty^D)^{O_n(1)}$. $\qquad\qquad\square$

The following lemma serves as a strong converse to Lemma 4.1.

Lemma 4.5. *If $G_f = S_n$ and $\Psi = \Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}$ is separable then Ψ is irreducible over $\mathbb{Q}$.*

Proof. Suppose for a contradiction that $\Psi(y) = \Psi_1(y)\Psi_2(y)$, where $\Psi_1(y), \Psi_2(y) \in \mathbb{Q}[y]$ are non-constant polynomials. Let $r_{\sigma_1} = r_{\mathbf{w},\mathbf{e},\mathfrak{g}}(\sigma_1)$ and $r_{\sigma_2} = r_{\mathbf{w},\mathbf{e},\mathfrak{g}}(\sigma_2)$ be roots of Ψ_1 and Ψ_2 respectively. As Ψ_1 has rational coefficients and $\sigma_2\sigma_1^{-1} \in G_f$, the complex number
$$r_{\sigma_2} = \sigma_2\sigma_1^{-1}(r_{\sigma_1})$$
must be a root of Ψ_1, contradicting the separability of Ψ. $\qquad\qquad\square$

Lemma 4.6. *Let $a_1, \ldots, a_{n-3} \in \mathbb{Z} \cap [-H, H]$, and let $L(a, b) \in \mathbb{Q}[a, b]$ be linear. Assume that*
$$\mathrm{Gal}(X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 + a X^2 + b X + L(a, b), \mathbb{Q}(a, b)) = S_n.$$
Then, associated to any proper subgroup of S_n, there exist $\mathbf{w}, \mathbf{e}, \mathfrak{g}$, with $\|\mathbf{w}\|_\infty, \|\mathbf{e}\|_\infty \ll_n 1$ and $\mathfrak{g} \ll H^{O(1)}(1 + |L|)$, such that
$$h(a, b, y) = \Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}(y; a_1, \ldots, a_{n-3}, a, b, L(a, b))$$
is irreducible over $\mathbb{Q}$. The same is true with
$$\Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}(y; a_1, \ldots, a_{n-3}, a, L(a, b), b)$$
or
$$\Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}(y; a_1, \ldots, a_{n-3}, L(a, b), a, b)$$
in place of $\Phi_{\mathbf{w},\mathbf{e},\mathfrak{g}}(y; a_1, \ldots, a_{n-3}, a, b, L(a, b))$, with the corresponding change to the hypothesis.

Proof. Let $C \in \mathbb{N}$ be a large constant, and let $P = H^C$. Write
$$L(a, b) = \lambda a + \mu b + \nu,$$
and define
$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 + \nu, \quad G_1(X) = X^2 + \lambda, \quad G_2(X) = X + \mu.$$

By [19, Theorem 2.1], there can be at most $H^{O(1)}P^{3/2}\log P$ pairs $(a, b) \in [-P, P]^2$ of integers for which $G_{G_0+aG_1+bG_2} \neq S_n$. Hence, there exist integers $a_0, b_0 \in [-P, P]$ such that $G_{G_0+a_0G_1+b_0G_2} = S_n$. Now Lemma 4.5 tells us that $h(a_0, b_0, y)$ is irreducible over $\mathbb{Q}$, when $\mathbf{w}, \mathbf{e}, \mathbf{g}$ are obtained by applying Lemma 4.2 to the polynomial

$$X^n + a_1 X^{n-1} + \cdots + a_{n-3}X^3 + a_0 X^2 + b_0 X + L(a_0, b_0).$$

Suppose for a contradiction that $h(a, b, y)$ is reducible over $\mathbb{Q}$. Then, for some positive integer $k \leqslant d - 1$ and some $b_1(a, b), \ldots, b_k(a, b), c_1(a, b), \ldots, c_{d-k}(a, b) \in \mathbb{Q}(a, b)$, we have

$$h(a, b, y) = (y^k + b_1(a, b)y^{k-1} + \cdots + b_k(a, b))(y^{k-d} + c_1(a, b)y^{k-d-1} + \cdots + c_{d-k}(a, b)).$$

Specialising $a = a_0$ and $b = b_0$ contradicts the irreducibility of $h(a_0, b_0, y)$.

The final sentence of the lemma is confirmed by imitating the proof of its first assertion. $\qquad\square$

5. SEXTIC GALOIS THEORY

In this section, we establish Theorem 1.10. Let

$$f(X) = X^6 - a_1 X^5 + a_2 X^4 - a_3 X^3 + a_4 X^2 - a_5 X + a_6 \in \mathbb{Z}[X]$$

be irreducible, and suppose its Galois group G_f is not conjugate to S_6 or A_6. Then G_f is conjugate to a subgroup of G_{72}, G_{48}, or H_{120}, in the notation of Hagedorn [28]. Note that G_{72} and G_{48} are solvable, whereas H_{120} is insolvable.

5.1. A decic resolvent.
If G_f is conjugate to a subgroup of G_{72}, then by [28, Theorem 2] the polynomial $f_{10}(X)$ from that article has a rational root. As $f_{10}(X)$ is a monic, decic polynomial with integer coefficients, it follows that $f_{10}(y) = 0$ for some $y \in \mathbb{Z}$.

5.1.1. *Non-degenerate quadruples for the decic resolvent.* Let $a_1, \ldots, a_4 \in [-H, H]$ be integers such that the vanishing of

$$g(a_5, a_6, y) = f_{10}(y; a_1, \ldots, a_6)$$

cuts out an absolutely irreducible surface with no rational lines. Expressions for the coefficients of f_{10} as polynomials in $a_1, \ldots, a_6$ are given in the appendix of [28], and we also computed them using *Mathematica*. Note that

$$f_{10}(y) = y^{10} - b_1 y^9 + \cdots - b_9 y + b_{10},$$

where $b_i \ll H^i$ for all i assuming $a_1, \ldots, a_6 \ll H$, and therefore all solutions have $y \ll H$. Note that a large part of the expression for b_{10} is missing from [28].

We adopt the strategy of §3.2. First we cover all but $O(H^{\varepsilon+2/\sqrt{10}})$ points by $O(H^{\varepsilon+1/\sqrt{10}})$ curves. Next, we eliminate y, giving $F(d, e) = 0$ with $\deg(F) \ll 1$, and let $\mathcal{F}(d, e)$ be an irreducible factor of $F(d, e)$. There are $O(H^{\varepsilon+1/2})$ zeros (d, e) unless $\mathcal{F}$ is linear, by Theorem 2.2. In the latter case we obtain

$$\mathcal{P}(d, y) = \mathcal{F}(d, e) = 0,$$

say, where $\mathcal{P}$ is irreducible over $\mathbb{Q}$. Now $\mathcal{P}$ cannot be linear, so by Theorem 2.2 we have

$$\#\{(d, y) \in (\mathbb{Z} \cap [-H, H])^2 : \mathcal{P}(d, y) = 0\} \ll H^{\varepsilon+1/2}.$$

The contribution from non-degenerate quadruples is $O(H^{\varepsilon+9/2+1/\sqrt{10}})$.

5.1.2. *Degenerate quadruples for the decic resolvent.* We begin by discussing absolute irreducibility. Note that g is decic in a_5, a_6, y, no matter the specialisation $a_1, \ldots, a_4 \in \mathbb{Z}$. Thus, by [40, Chapter V, Theorem 2A], there exist integer polynomials

$$p_1(a_1, \ldots, a_4), \ldots, p_s(a_1, \ldots, a_4)$$

of degree $O(1)$ such that if $a_1, \ldots, a_4 \in \mathbb{C}$ then

$$g \text{ is not absolutely irreducible } \Leftrightarrow p_i(a_1, \ldots, a_4) = 0 \ (1 \leqslant i \leqslant s).$$

The next lemma shows that p_i is non-zero for some i.

Lemma 5.1. *If* $a_1 = \cdots = a_4 = 0$ *then* $g(a_5, a_6, y)$ *is absolutely irreducible.*

Proof. Let $a_1 = \cdots = a_4 = 0$. Then

$$b_1 = \cdots = b_4 = 0, \qquad b_5 = -123a_5^2, \qquad b_6 = 129a_6^2, \qquad b_7 = 0,$$
$$b_8 = 66a_5^2 a_6, \qquad b_9 = 64a_6^3, \qquad b_{10} = a_5^4,$$

so

$$g(a_5, a_6, y) = y^{10} + 123a_5^2 y^5 + 129a_6^2 y^4 + 66a_5^2 a_6 y^2 - 64a_6^3 y + a_5^4.$$

This is monic in y, so it suffices to prove that

$$g(a_5, 1, y) = y^{10} + 123a_5^2 y^5 + 129y^4 + 66a_5^2 y^2 - 64y + a_5^4$$

is absolutely irreducible. *Mathematica* assures us that $g(a_5, 1, y)$ is irreducible over the rationals. Its Newton polygon is the convex hull of

$$(0, 10), (2, 5), (0, 4), (2, 2), (0, 1), (4, 0),$$

which has vertices $(0, 1), (0, 10), (4, 0)$. As $\gcd(0, 1, 0, 10, 4, 0) = 1$, absolute irreducibility is ensured by [3, Proposition 3]. $\qquad\square$

Consequently, the quadruples $(a_1, \ldots, a_4)$ such that $g(a_5, a_6, y)$ is reducible over $\overline{\mathbb{Q}}$ are all zeros of a fixed non-zero polynomial of degree $O(1)$. In particular, there are $O(H^3)$ such quadruples $(a_1, \ldots, a_4)$.

Next, we discuss lines on the surface. The idea is to show that, for generic $a_1, \ldots, a_4$, the surface $\{g(a_5, a_6, y) = 0\}$ contains no rational lines or, *a fortiori*, no complex lines. A line on the surface has one of the following parametrisations:

I. $\{(0, \beta, \gamma) + t(1, b, c) : t \in \mathbb{C}\}$, for some $\beta, \gamma, b, c \in \mathbb{C}$
II. $\{(\alpha, 0, \gamma) + t(0, 1, c) : t \in \mathbb{C}\}$, for some $\alpha, \gamma, c \in \mathbb{C}$
III. $\{(\alpha, \beta, 0) + t(0, 0, 1) : t \in \mathbb{C}\}$, for some $\alpha, \beta \in \mathbb{C}$.

We use the 'SymmetricReduction' command in *Mathematica* to evaluate and store the polynomial $g(a_5, a_6, y)$ explicitly:

```
ClearAll["Global'*"];
r1 = (x1 + x2 + x3)*(x4 + x5 + x6); r2 = (x1 + x2 + x4)*(x3 + x5 + x6); r3 = (x1 + x2 + x5)*(x3 + x4 + x6);
r4 = (x1 + x2 + x6)*(x3 + x4 + x5); r5 = (x1 + x3 + x4)*(x2 + x5 + x6); r6 = (x1 + x3 + x5)*(x2 + x4 + x6);
r7 = (x1 + x3 + x6)*(x2 + x4 + x5); r8 = (x1 + x4 + x5)*(x2 + x3 + x6); r9 = (x1 + x4 + x6)*(x2 + x3 + x5);
r10 = (x1 + x5 + x6)*(x2 + x3 + x4);
b1 = SymmetricPolynomial[1, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b2 = SymmetricPolynomial[2, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b3 = SymmetricPolynomial[3, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b4 = SymmetricPolynomial[4, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b5 = SymmetricPolynomial[5, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b6 = SymmetricPolynomial[6, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b7 = SymmetricPolynomial[7, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b8 = SymmetricPolynomial[8, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b9 = SymmetricPolynomial[9, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
b10 = SymmetricPolynomial[10, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10}];
```

```
B1  = SymmetricReduction[b1,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B2  = SymmetricReduction[b2,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B3  = SymmetricReduction[b3,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B4  = SymmetricReduction[b4,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B5  = SymmetricReduction[b5,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B6  = SymmetricReduction[b6,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B7  = SymmetricReduction[b7,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B8  = SymmetricReduction[b8,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B9  = SymmetricReduction[b9,  {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
B10 = SymmetricReduction[b10, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]];
g = y^(10) - B1*y^9 + B2*y^8 - B3*y^7 + B4*y^6 - B5*y^5 + B6*y^4 - B7*y^3 + B8*y^2 - B9*y + B10;
```

Then we expand it as a polynomial in t, in each of the three cases. In Case I, the polynomial is $c^{10}t^{10}$ plus lower-order terms, and so $c = 0$. When we specialise $c = 0$, we obtain a monic, quartic polynomial t. Such a polynomial cannot vanish identically, so there are no lines of Type I.

Similarly in Case II we must have $c = 0$, and then we obtain a polynomial of degree at most 3 in t. Setting the cubic coefficient to 0 expresses

$$\gamma = a_1^2/4.$$

We then substitute this into the equation obtained by setting the quadratic coefficient to 0, determining an equation $P(a_1, \ldots, a_4) = 0$, where $P \in \mathbb{Z}[a_1, \ldots, a_4] \setminus \{0\}$ has degree $O(1)$, because α so happens to be eliminated as a result of this substitution. Thus, there are $O(H^3)$ integer quadruples $(a_1, \ldots, a_4)$ such that $\{g(a_5, a_6, y) = 0\}$ contains a line of Type II.

In Case III the polynomial is monic of degree 10, so there are no lines of Type III. Having considered all cases, we conclude that there are $O(H^3)$ integer quadruples $(a_1, \ldots, a_4)$ such that $\{g(a_5, a_6, y) = 0\}$ contains a line.

Finally, we estimate the contribution from degenerate quadruples. We showed that there are $O(H^3)$ degenerate quadruples $(a_1, \ldots, a_4) \in [-H, H]$. Let us now fix such a quadruple. By [23, Lemma 2], there are at most $O(1)$ values of $a_5 \in \mathbb{Z}$ for which

$$X^6 - a_1 X^5 + \cdots - a_5 X + a_6 \in \mathbb{Q}(a_6)[X]$$

has non-S_6 Galois group over $\mathbb{Q}(a_6)$. The contribution from these choices of a_5 is $O(H^4)$. Now let $a_5 \in [-H, H]$ be such that the Galois group is S_6.

Let $C \in \mathbb{N}$ be a large constant, and let $P = H^C$. By [19, Theorem 2.1], there exists $a_6^* \in \mathbb{Z} \cap [-P, P]$ such that

$$\text{Gal}(X^6 - a_1 X^5 + \cdots + a_4 X^2 - a_5 X + a_6^*, \mathbb{Q}) = S_6.$$

By Lemma 4.5, the polynomial

$$\Phi_{\mathbf{w}, \mathbf{e}, \mathfrak{g}}(y; a_1, \ldots, a_5, a_6^*) \in \mathbb{Q}[y]$$

is irreducible, where $\mathbf{w}, \mathbf{e}, \mathfrak{g}$ are obtained by applying Lemma 4.2 to the polynomial

$$X^6 - a_1 X^5 + \cdots + a_4 X^2 - a_5 X + a_6^*.$$

It then follows that

$$h(a_6, y) := \Phi_{\mathbf{w}, \mathbf{e}, \mathfrak{g}}(y; a_1, \ldots, a_5, a_6) \in \mathbb{Q}[a_6, y]$$

is irreducible. Indeed, it is monic in y, and if we were to have

$$h(a_6, y) = h_1(a_6, y)h_2(a_6, y)$$

for some h_1, h_2 of positive degrees in y, then

$$h(a_6^*, y) = h_1(a_6^*, y)h_2(a_6^*, y)$$

would be a non-trivial factorisation of $h(a_6^*, y)$.

Further, by Lemma 4.1, if $a_6 \in \mathbb{Z} \cap [-H, H]$ and $G_f \leqslant G_{72}$ then $h(a_6, y)$ has an integer root $y \ll H^{O(1)}$. By Theorem 2.2, the diophantine equation $h(a_6, y) = 0$ has $O(H^{\varepsilon + |G_{72}|/720}) = O(H^{\varepsilon + 0.1})$ integer solutions a_6, y with $a_6 \ll H$ and $y \ll H^{O(1)}$. The contribution from degenerate quadruples, when $G_f \leqslant G_{72}$, is therefore $O(H^{4.1+\varepsilon})$.

We conclude that

$$N_G \ll H^{9/2+\varepsilon+1/\sqrt{10}} \qquad (G \leqslant G_{72}).$$

5.2. A resolvent of degree 15.

5.2.1. *Non-degenerate quadruples for the resolvent of degree 15.* For $G_f \leqslant G_{48}$, we use the resolvent

$$f_{15}(y) = y^{15} - c_1 y^{14} + \cdots + c_{14}y - c_{15}$$

from [28], where $c_i \ll H^i$ for all i assuming $a_1, \ldots, a_6 \ll H$. Expressions for $c_1, \ldots, c_{15}$ as polynomials in $a_1, \ldots, a_6$ are given in the appendix of [28], and we also computed them using *Mathematica*. Note that the former contains a few small errors. The argument of §5.1.1 bounds the contribution from this case by a constant times

$$H^{4+0.5+\varepsilon+1/\sqrt{15}} \ll H^{4.76}.$$

We provide the code below.

```
ClearAll["Global`*"];
r1 = (x1*x2) + (x3*x4) + (x5*x6); r2 = (x1*x2) + (x3*x5) + (x4*x6); r3 = (x1*x2) + (x3*x6) + (x4*x5);
r4 = (x1*x3) + (x2*x4) + (x5*x6); r5 = (x1*x3) + (x2*x5) + (x4*x6); r6 = (x1*x3) + (x2*x6) + (x4*x5);
r7 = (x1*x4) + (x2*x3) + (x5*x6); r8 = (x1*x4) + (x2*x5) + (x3*x6); r9 = (x1*x4) + (x2*x6) + (x3*x5);
r10 = (x1*x5) + (x2*x3) + (x4*x6); r11 = (x1*x5) + (x2*x4) + (x3*x6); r12 = (x1*x5) + (x2*x6) + (x3*x4);
r13 = (x1*x6) + (x2*x3) + (x4*x5); r14 = (x1*x6) + (x2*x4) + (x3*x5); r15 = (x1*x6) + (x2*x5) + (x3*x4);
b1 = SymmetricPolynomial[1, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b2 = SymmetricPolynomial[2, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b3 = SymmetricPolynomial[3, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b4 = SymmetricPolynomial[4, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b5 = SymmetricPolynomial[5, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b6 = SymmetricPolynomial[6, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b7 = SymmetricPolynomial[7, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b8 = SymmetricPolynomial[8, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b9 = SymmetricPolynomial[9, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b10 = SymmetricPolynomial[10, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b11 = SymmetricPolynomial[11, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b12 = SymmetricPolynomial[12, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b13 = SymmetricPolynomial[13, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b14 = SymmetricPolynomial[14, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
b15 = SymmetricPolynomial[15, {r1, r2, r3, r4, r5, r6, r7, r8, r9, r10, r11, r12, r13, r14, r15}];
B1 = SymmetricReduction[b1, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B2 = SymmetricReduction[b2, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B3 = SymmetricReduction[b3, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B4 = SymmetricReduction[b4, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B5 = SymmetricReduction[b5, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B6 = SymmetricReduction[b6, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B7 = SymmetricReduction[b7, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B8 = SymmetricReduction[b8, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B9 = SymmetricReduction[b9, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B10 = SymmetricReduction[b10, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B11 = SymmetricReduction[b11, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B12 = SymmetricReduction[b12, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B13 = SymmetricReduction[b13, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B14 = SymmetricReduction[b14, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
B15 = SymmetricReduction[b15, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]
```

5.2.2. *Degenerate quadruples for the resolvent of degree 15.* We begin by discussing absolute irreducibility. Note that g has degree 15 in a_5, a_6, y, no matter the specialisation $a_1, \ldots, a_4 \in \mathbb{Z}$. Thus, by [40, Chapter V, Theorem 2A], there exist integer polynomials $p_1(a_1, \ldots, a_4), \ldots, p_s(a_1, \ldots, a_4)$ of degree $O(1)$ such that if $a_1, \ldots, a_4 \in \mathbb{C}$ then

$$g \text{ is not absolutely irreducible } \Leftrightarrow p_i(a_1, \ldots, a_4) = 0 \ (1 \leqslant i \leqslant s).$$

The next lemma shows that p_i is non-zero for some i.

Lemma 5.2. *The polynomial*

$$g(a_5, a_6, y) := f_{15}(y; 0, 0, 0, 0, a_5, a_6)$$

is absolutely irreducible.

Proof. As $g(a_5, a_6, y)$ is monic in y, it suffices to prove that $g(a_5, 1, y)$ is absolutely irreducible. We compute using *Mathematica* that

$$g(a_5, 1, y) = 32a_5^6 + 1296a_5^2 y + 792a_5^4 y^2 - 1728y^3 - 96a_5^2 y^4 - 353a_5^4 y^5$$
$$- 1232y^6 + 288a_5^2 y^7 + 453y^9 - 21a_5^2 y^{10} - 42y^{12} + y^{15}$$

is irreducible over the rationals. Its Newton polygon is the convex hull of

$$(6, 0), (2, 1), (4, 2), (0, 3), (2, 4), (4, 5), (0, 6), (2, 7), (0, 9), (2, 10), (0, 12), (0, 15),$$

which has vertices $(6, 0), (0, 3), (0, 15), (2, 1)$. As $\gcd(6, 0, 0, 3, 0, 15, 2, 1) = 1$, absolute irreducibility is assured by [3, Proposition 3]. $\qquad\square$

Consequently, the quadruples $(a_1, \ldots, a_4)$ such that $g(a_5, a_6, y)$ is reducible over $\mathbb{C}$ are all zeros of a fixed non-zero polynomial of degree $O(1)$. In particular, there are $O(H^3)$ such quadruples $(a_1, \ldots, a_4)$.

Next, we discuss lines on the surface. We have the same trichotomy as in the previous subsection. In Case I, the polynomial is $c^{15} t^{15}$ plus lower-order terms, so $c = 0$. When we specialise $c = 0$, we obtain $32t^6$ plus lower-order terms. Such a polynomial cannot vanish identically, so there are no lines of Type I.

Similarly in Case II we must have $c = 0$, and then we obtain a polynomial of degree at most 4 in t. We set the quartic, cubic and quadratic coefficients to 0, computing them using *Mathematica*. Calling these P_4, P_3, P_2 respectively, we obtain

$$P_4(a_1, a_2, \gamma) = P_3(a_1, \ldots, a_4, \alpha, \gamma) = P_2(a_1, \ldots, a_4, \alpha, \gamma) = 0, \tag{5.1}$$

and P_4, P_3, P_2 are non-zero polynomials of degree $O(1)$. It so happens that

$$P_4(a_1, a_2, \gamma) = -49a_1^6 + 315a_1^4 a_2 - 648a_1^2 a_2^2 + 432a_2^3 + 189a_1^4 \gamma - 1080a_1^2 a_2 \gamma$$
$$+ 1296a_2^2 \gamma + 432a_1^2 \gamma^2 - 1728\gamma^3$$

does not involve a_3, a_4, α. Now $R(a_1, \ldots, a_4, \gamma) = 0$, where R is the resultant of P_3 and P_2 in the variable α. We explicitly evaluate R using *Mathematica*.

Let $P(a_1, \ldots, a_4)$ be the resultant of P_4 and R in the variable γ. We can compute $P(1, 0, 0, 0)$ using *Mathematica*, by specialising before taking the resultant. The outcome is non-zero, so P is not the zero polynomial. Furthermore

$$P(a_1, \ldots, a_4) = 0$$

whenever $(a_1, a_2, a_3, a_4, \alpha, \gamma) \in \mathbb{C}^6$ is a solution to (5.1). Thus, there are $O(H^3)$ integer quadruples $(a_1, \ldots, a_4)$ such that $\{g(a_5, a_6, y) = 0\}$ contains a line of Type II.

In Case III the polynomial is monic of degree 15, so there are no rational lines of Type III. Having considered all cases, we conclude that there are $O(H^3)$ integer quadruples $(a_1, \ldots, a_4)$ such that $\{g(a_5, a_6, y) = 0\}$ contains a complex line.

The upshot is that there are $O(H^3)$ degenerate quadruples to consider. Now the reasoning of the previous subsection bounds their contribution by $O(H^{\varepsilon+61/15})$. We conclude that if $G \leqslant G_{48}$ then
$$N_G \ll H^{4+0.5+\varepsilon+1/\sqrt{15}} \leqslant H^{4.76}.$$
This completes the proof of the second statement in Theorem 1.10.

5.3. **Insolvable sextics.** For subgroups of H_{120}, we use Stauduhar's [43] resolvent
$$\Psi(y; a_1, \ldots, a_6) = \prod_{\sigma \in S_6/H_{120}} (y - \sigma\theta) \in \mathbb{Z}[y; a_1, \ldots, a_6],$$
where
$$\theta = (\alpha_1\alpha_2 + \alpha_3\alpha_5 + \alpha_4\alpha_6)(\alpha_1\alpha_3 + \alpha_4\alpha_5 + \alpha_2\alpha_6)(\alpha_3\alpha_4 + \alpha_1\alpha_6 + \alpha_2\alpha_5)$$
$$\cdot (\alpha_1\alpha_5 + \alpha_2\alpha_4 + \alpha_3\alpha_6)(\alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_5\alpha_6).$$
Here, if
$$f(X) = X^6 - a_1 X^5 + a_2 X^4 - a_3 X^3 + a_4 X^2 - a_5 X + a_6 \in \mathbb{Z}[X]$$
is irreducible, we write $\alpha_1, \ldots, \alpha_6$ for the roots of f. At first it may appear that Stauduhar uses right cosets in [43], but in modern language these σH_{120} are more commonly referred to as left cosets; see the footnote on [43, p. 983].

As H_{120} is generated by $(126)(354)$, (12345) and (2354), from [43, Table 1] where it is denoted G_{120}, we see that θ is H_{120}-invariant. Thus, if $G_f \leqslant \tau H_{120}\tau^{-1}$ for some $\tau \in S_6$, then $\tau\theta$ is a G_f-invariant algebraic integer and so $\tau\theta \in \mathbb{Z}$. The upshot is that if G_f is conjugate to a subgroup of H_{120} then Ψ has an integer root.

One can find the cycle types of the conjugacy classes of H_{120}, which is also known as 6T14, in [12, Table 6C], to see that H_{120} has no 2-cycles and no 3-cycles. It follows that $\{(1), (12), (13), (14), (15), (16)\}$ constitutes a complete set of left coset representatives for H_{120} in S_6. This enables us to construct the resolvent in *Mathematica*:

```
ClearAll["Global`*"];
r1 = (x1*x2 + x3*x5 + x4*x6)*(x1*x3 + x4*x5 + x2*x6)*(x3*x4 + x1*x6 + x2*x5)*(x1*x5 + x2*x4 + x3*x6)
*(x1*x4 + x2*x3 + x5*x6);
r2 = (x2*x1 + x3*x5 + x4*x6)*(x2*x3 + x4*x5 + x1*x6)*(x3*x4 + x2*x6 + x1*x5)*(x2*x5 + x1*x4 + x3*x6)
*(x2*x4 + x1*x3 + x5*x6);
r3 = (x3*x2 + x1*x5 + x4*x6)*(x3*x1 + x4*x5 + x2*x6)*(x1*x4 + x3*x6 + x2*x5)*(x3*x5 + x2*x4 + x1*x6)
*(x3*x4 + x2*x1 + x5*x6);
r4 = (x4*x2 + x3*x5 + x1*x6)*(x4*x3 + x1*x5 + x2*x6)*(x3*x1 + x4*x6 + x2*x5)*(x4*x5 + x2*x1 + x3*x6)
*(x4*x1 + x2*x3 + x5*x6);
r5 = (x5*x2 + x3*x1 + x4*x6)*(x5*x3 + x4*x1 + x2*x6)*(x3*x4 + x5*x6 + x2*x1)*(x5*x1 + x2*x4 + x3*x6)
*(x5*x4 + x2*x3 + x1*x6);
r6 = (x6*x2 + x3*x5 + x4*x1)*(x6*x3 + x4*x5 + x2*x1)*(x3*x4 + x6*x1 + x2*x5)*(x6*x5 + x2*x4 + x3*x1)
*(x6*x4 + x2*x3 + x5*x1);
b1 = SymmetricPolynomial[1, {r1, r2, r3, r4, r5, r6}];
b2 = SymmetricPolynomial[2, {r1, r2, r3, r4, r5, r6}];
b3 = SymmetricPolynomial[3, {r1, r2, r3, r4, r5, r6}];
b4 = SymmetricPolynomial[4, {r1, r2, r3, r4, r5, r6}];
b5 = SymmetricPolynomial[5, {r1, r2, r3, r4, r5, r6}];
b6 = SymmetricPolynomial[6, {r1, r2, r3, r4, r5, r6}];
B1 = SymmetricReduction[b1, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B1.txt", B1];
B2 = SymmetricReduction[b2, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B2.txt", B2];
B3 = SymmetricReduction[b3, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B3.txt", B3];
B4 = SymmetricReduction[b4, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B4.txt", B4];
B5 = SymmetricReduction[b5, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B5.txt", B5];
B6 = SymmetricReduction[b6, {x1, x2, x3, x4, x5, x6}, {a1, a2, a3, a4, a5, a6}][[1]]; Export["B6.txt", B6];
```

5.3.1. *Non-degenerate quadruples.* In due course, we will define a non-zero polynomial

$$R(a_1, \ldots, a_4) \in \mathbb{Z}[a_1, \ldots, a_4]$$

with coefficients and degree $O_n(1)$. Let $a_1, \ldots, a_4 \in [-H, H]$ be integers such that the vanishing of

$$g(a_5, a_6, y) = \Psi(y; a_1, \ldots, a_6)$$

cuts out an absolutely irreducible surface with no rational lines, and such that

$$(5a_1^2 - 18a_2)R(a_1, \ldots, a_4) \neq 0. \tag{5.2}$$

We wish to count integer zeros of g with $a_5, a_6 \ll H$, and for these we have $y \ll H^M$ for some absolute constant $M \in \mathbb{N}$, by [23, Lemma 1]. Following §3.2, we can cover all but $O(H^{\varepsilon+2/\sqrt{6}})$ points by $O(H^{\varepsilon+1/\sqrt{6}})$ curves using Theorem 2.5. Then we eliminate y, giving $F(a_5, a_6) = 0$ with $\deg(F) \ll 1$, and let $\mathcal{F}(a_5, a_6)$ be an irreducible factor of $F(a_5, a_6)$. There are $O(H^{\varepsilon+1/2})$ zeros (a_5, a_6) unless $\mathcal{F}$ is linear, so we now assume the latter. We divide into two cases according to whether or not the coefficient of a_6 in $\mathcal{F}$ vanishes.

Case 1: $a_6 = \mathfrak{H}a_5 + \mathfrak{L}$. Substituting this into $g(a_5, a_6, y) = 0$ and factorising, we obtain

$$\mathcal{P}(a_5, y) = \mathcal{F}(a_5, a_6) = 0,$$

where $\mathcal{P}$ is irreducible over $\mathbb{Q}$. Moreover, since there are no rational lines, the polynomial $\mathcal{P}$ must be non-linear. By Theorem 2.2, we have

$$\#\{(a_5, y) \in \mathbb{Z}^2 \cap [-H, H] \times [-CH^M, CH^M] : \mathcal{P}(a_5, y) = 0\} \ll H^{\varepsilon+M/D},$$

where C is a large, positive constant and

$$2 \leqslant D := \max\{\deg_{a_5}(\mathcal{P}), M\deg_y(\mathcal{P})\} \ll 1.$$

If $D \geqslant 2M$ then the bound is adequate, so we may suppose that $2 \leqslant D \leqslant 2M - 1$, and in particular $\deg_y(\mathcal{P}) \leqslant 1$. As $\mathcal{P}(a_5, y)$ divides

$$g(a_5, \mathfrak{H}a_5 + \mathfrak{L}, y) = y^6 + \sum_{i=0}^{5} P_i(a_5)y^i,$$

we infer that $\mathcal{P}(a_5, y)$ is a rational multiple of $y - F(a_5)$, where $F(a_5) \in \mathbb{Q}[a_5]$ has degree $\deg_{a_5}(\mathcal{P})$. Thus, we may assume that

$$\mathcal{P}(a_5, y) = y - F(a_5).$$

Next, write

$$(y - F(a_5))\left(y^5 + \sum_{i=0}^{4} f_i(a_5)y^i\right) = y^6 + \sum_{i=0}^{5} P_i(d)y^i.$$

Equating coefficients in y yields

$$f_4(a_5) - F(a_5) = P_5(a_5)$$
$$f_3(a_5) - f_4(a_5)F(a_5) = P_4(a_5)$$
$$f_2(a_5) - f_3(a_5)F(a_5) = P_3(a_5)$$
$$f_1(a_5) - f_2(a_5)F(a_5) = P_2(a_5)$$
$$f_0(a_5) - f_1(a_5)F(a_5) = P_1(a_5)$$
$$-f_0(a_5)F(a_5) = P_0(a_5).$$

Using *Mathematica*, we compute that

$$\deg(P_i) \leqslant 2(6 - i) \qquad (0 \leqslant i \leqslant 5).$$

The argument of §3.2 then delivers a contradiction, unless $\deg(F) = 2$. We now assume the latter.

From the equations above, we have

$$f_4(a_5) = P_5(a_5) + F(a_5),$$

so

$$f_3(a_5) = P_4(a_5) + F(a_5)(P_5(a_5) + F(a_5)).$$

Continuing make the substitutions, we obtain

$$\mathfrak{P} = 0$$

for some explicit polynomial $\mathfrak{P}$ in $F(a_5), P_5(a_5), \ldots, P_0(a_5)$. Let

$$F(a_5) = \mathfrak{A}a_5^2 + \mathfrak{B}a_5 + \mathfrak{G},$$

where $\mathfrak{A}, \mathfrak{B}, \mathfrak{G} \in \mathbb{C}$, and substitute this into $\mathfrak{P}$ to give

$$P = 0 \in \mathbb{Q}[a_1, \ldots, a_4, \mathfrak{A}, \mathfrak{B}, \mathfrak{G}, \mathfrak{H}, \mathfrak{L}][a_5],$$

for some polynomial P that we computed using *Mathematica*. With the coefficients of the resolvent having been evaluated and stored, the code is as follows:

```
F = A a5^2 + B a5 + G; a6 = H a5 + L;
f4 = F - B1; f3 = f4 F + B2; f2 = f3 F - B3; f1 = f2 F + B4; f0 = f1 F - B5;
P = f0 F + B6;
```

For $i = 0, 1, \ldots, 12$, denote by c_i the coefficient of a_5^i in P. We have

$$0 = c_{12} = (\mathfrak{A} - 32)(\mathfrak{A} - 2)^5,$$

so $\mathfrak{A} \in \{2, 32\}$. If $\mathfrak{A} = 2$ then $c_{11} = -30(a_1 - 6\mathfrak{H})^5$, whereupon $\mathfrak{H} = a_1/6$ and

$$0 = c_{10} = \frac{5(5a_1^2 - 18a_2)^5}{1296},$$

contradicting (5.2).

Therefore $\mathfrak{A} = 32$. The equation $c_{11} = 0$ then enables us to write $\mathfrak{B}$ as an explicit polynomial in $\mathfrak{H}, a_1, \ldots, a_4$. We substitute both of these data into the other coefficients. Finally, taking resultants yields

$$R(a_1, a_2, a_3, a_4) = 0,$$

where

$$R_1 = \text{Res}(c_{10}, c_9, \mathfrak{G}), \quad R_2 = \text{Res}(c_{10}, c_8, \mathfrak{G}), \quad R_3 = \text{Res}(c_{10}, c_7, \mathfrak{G}), \quad R_4 = \text{Res}(c_{10}, c_6, \mathfrak{G}),$$
$$R_5 = \text{Res}(R_1, R_2, \mathfrak{H}), \qquad R_6 = \text{Res}(R_3, R_4, \mathfrak{H}), \qquad R = \text{Res}(R_5, R_6, \mathfrak{L}),$$

again contradicting (5.2). *Mathematica* assures us that $R(1, 0, 0, 1) \neq 0$, so in particular R is not the zero polynomial.

Case 2: $a_5 = \mathfrak{H}$ is constant. Substituting this into $g(a_5, a_6, y) = 0$ and factorising, we obtain

$$\mathcal{P}(a_6, y) = \mathcal{F}(a_5, a_6) = 0,$$

where $\mathcal{P}$ is irreducible over $\mathbb{Q}$. Following the argument of the previous case, we find that

$$\deg(P_i) < 2(6 - i) \qquad (0 \leqslant i \leqslant 5),$$

and the reasoning of §3.2 delivers a contradiction.

The total contribution from non-degenerate quadruples is $O(H^{\varepsilon+9/2+1/\sqrt{6}})$.

5.3.2. *Degenerate quadruples.* We begin by discussing absolute irreducibility. One can check, using *Mathematica*, that g is dodecic in a_5, a_6, y, no matter the specialisation $a_1, \ldots, a_4 \in \mathbb{Q}$. Thus, by [40, Chapter V, Theorem 2A], there exist integer polynomials

$$p_1(a_1, \ldots, a_4), \ldots, p_s(a_1, \ldots, a_4)$$

of degree $O(1)$ such that if $a_1, \ldots, a_4 \in \mathbb{C}$ then

$$g \text{ is not absolutely irreducible } \Leftrightarrow p_i(a_1, \ldots, a_4) = 0 \ (1 \leqslant i \leqslant s).$$

The next lemma shows that p_i is non-zero for some i.

Lemma 5.3. *If $a_1 = \cdots = a_4 = 0$ then $\{g(a_5, a_6, y) = 0\}$ is absolutely irreducible.*

Proof. Using *Mathematica*, we compute that

$$g(a_5, a_6, y) = \Psi(y; 0, 0, 0, 0, a_5, a_6) = y^6 - 42a_5^2 y^5 + 360a_5^4 y^4 - (1360a_5^6 - 46656a_6^5)y^3$$
$$+ (2640a_5^8 - 34992a_5^2 a_6^5)y^2 - 2592a_5^{10}y + 1024a_5^{12}.$$

As g is monic in y, it suffices to prove that

$$g(1, a_6, y) = y^6 - 42y^5 + 360y^4 - (1360 - 46656a_6^5)y^3 + (2640 - 34992a_6^5)y^2 - 2592y + 1024$$

is absolutely irreducible. *Mathematica* tells us that $g(1, a_6, y)$ is irreducible over $\mathbb{Q}$. Its Newton polygon is the convex hull of

$$(0, 6), (0, 5), (0, 4), (5, 3), (5, 2), (0, 1), (0, 0),$$

which has vertices $(0, 0), (5, 2), (5, 3), (0, 6)$. As $\gcd(0, 0, 5, 2, 5, 3, 0, 6) = 1$, absolute irreducibility is secured by [3, Proposition 3]. $\square$

Consequently, the quadruples $(a_1, \ldots, a_4)$ such that $g(a_5, a_6, y)$ is reducible over $\mathbb{C}$ are all zeros of a fixed non-zero polynomial of degree $O(1)$. In particular, there are $O(H^3)$ such quadruples $(a_1, \ldots, a_4)$.

Next, we discuss lines on the surface, using the trichotomy from the previous two subsections. If there is a line of Type I, then

$$\Psi(\gamma + ct; a_1, \ldots, a_4, t, \beta + bt) = 0,$$

for some $\beta, \gamma, b, c \in \mathbb{C}$. The left hand side is $1024t^{12}$ plus lower order terms, so there are no lines of this type. If there is a line of Type III, then

$$\Psi(t; a_1, \ldots, a_4, \alpha, \beta) = 0,$$

for some $\alpha, \beta \in \mathbb{C}$. The left hand side is monic of degree 6, so there are no lines of this type. If there is a line of Type II, then

$$\Psi(\gamma + ct; a_1, \ldots, a_4, \alpha, t) = 0$$

for some $\alpha, \gamma, c \in \mathbb{C}$. The coefficient of t^8 is

$$2401a_1^{12} - 30870a_1^{10}a_2 + 162729a_1^8 a_2^2 - 450576a_1^6 a_2^3 + 692064a_1^4 a_2^4 - 559872a_1^2 a_2^5 + 186624a_2^6,$$

so there are $O(H^3)$ integer quadruples $(a_1, \ldots, a_4)$ such that $\{g(a_5, a_6, y) = 0\}$ contains a complex line.

Finally, there are $O(H^3)$ exceptions to (5.2). Thus, there are $O(H^3)$ degenerate quadruples, and the reasoning of the previous subsections bounds their contribution by $O(H^{4+\varepsilon+1/6})$. We conclude that if $G \leqslant H_{120}$ then

$$N_G \ll H^{9/2+\varepsilon+1/\sqrt{6}}.$$

This completes the proof of Theorem 1.10.

6. Auxiliary results

6.1. An almost-uniform version of Hilbert's irreducibility theorem.

Theorem 6.1. *Let* $g(T, X_1, \ldots, X_s, Y) \in \mathbb{Z}[T, X_1, \ldots, X_s, Y]$ *be irreducible of total degree* D, *and monic of degree* $d \geqslant 2$ *in the variable* Y. *Then there are* $O_{s,D,\varepsilon}(|g|^\varepsilon H^{\varepsilon+1/2})$ *integers* $t \in [-H, H]$ *such that*

$$g(t, X_1, \ldots, X_s, Y) \in \mathbb{Z}[X_1, \ldots, X_s, Y]$$

is reducible.

Remark 6.2. The point is that we have exerted strong quantitative control over the dependence on the coefficients of g. In S. D. Cohen's work [19] the dependence is $|g|^{O(1)}$, but in practice it is more useful to have $O(|g|^\varepsilon)$ dependence. As $d \in \{2, 3, \ldots, D\}$, any dependence on d is controlled by the arbitrary dependence on D.

Proof. We begin by reducing to the case $s = 0$. By [19, Theorem 2.1], there exist integers $x_1, \ldots, x_s \ll |g|^{O_{s,D}(1)}$ such that $g(T, x_1, \ldots, x_s, Y)$ is irreducible. Suppose $t \in \mathbb{Z}$ and $g(t, X_1, \ldots, X_s, Y)$ is reducible. Then there exist

$$g_1(X_1, \ldots, X_s, Y), g_2(X_1, \ldots, X_s, Y) \in \mathbb{Z}[X_1, \ldots, X_s, Y],$$

monic of positive degrees in Y, such that

$$g(t, X_1, \ldots, X_s, Y) = g_1(X_1, \ldots, X_s, Y)g_2(X_1, \ldots, X_s, Y).$$

Now

$$g(t, x_1, \ldots, x_s, Y) = g_1(x_1, \ldots, x_s, Y)g_2(x_1, \ldots, x_s, Y)$$

is a non-trivial factorisation, so we have indeed reduced the problem to the $s = 0$ case.

As $g(T, Y) \in \mathbb{Z}[T, Y]$ is irreducible, its discriminant in Y is a non-zero polynomial in $\mathbb{Z}[T]$. Hence, there are $O_d(1)$ integers t such that $g(t, Y) \in \mathbb{Z}[Y]$ is inseparable. Let us denote by G the Galois group of $g(T, Y)$ over $\mathbb{Q}(T)$. Given $t \in \mathbb{Z}$ such that $g(t, Y)$ is separable, its Galois group G_t is a subgroup of G via the embedding in [14, Lemma 1]. There are $O_d(1)$ possibilities for G_t, and if $g(t, Y)$ is reducible then G_t must be a proper subgroup of G, since a polynomial is irreducible if and only if its Galois group is transitive.

Let us now fix a proper subgroup K of G, and count integers $t \in [-H, H]$ such that $G_t = K$. Applying Lemma 4.3, we obtain a polynomial $\Phi(T, Y) \in \mathbb{Z}[T, Y]$ of total degree $O_D(1)$, monic of degree $[S_d : K]$ in Y, such that:

(i) If $t \in \mathbb{Z} \cap [-H, H]$ and $G_t = K$ then $\Phi(t, Y) \in \mathbb{Z}[Y]$ has an integer root

$$y \ll_D (|g|H)^{O_D(1)}.$$

(ii) Any irreducible divisor of $\Phi(T, Y)$ has degree at least $[G : K]$ in Y.

Finally, by Theorem 2.2, any irreducible divisor of $\Phi(T, Y)$ has $O_{D,\varepsilon}(|g|^\varepsilon H^{\varepsilon+1/2})$ integer roots (t, y) with $|t| \leqslant H$ and $y \ll_D (|g|H)^{O_D(1)}$. $\square$

6.2. A lopsided version of Pila's theorem.

Theorem 6.3. *Let* $g(A, B, Y) \in \mathbb{Z}[A, B, Y]$ *be irreducible of total degree* D, *and monic of degree* $d \geqslant 2$ *in the variable* Y. *Then* g *has* $O_{D,\varepsilon}(|g|^\varepsilon H^{1+\varepsilon+1/d})$ *integer roots* (a, b, y) *with* $|a|, |b| \leqslant H$.

The bound is essentially sharp, for example if $g(a, b, y) = a - y^d$ then there are at least a positive constant times $H^{1+1/d}$ solutions. Before proceeding towards the proof, we provide some context. By [23, Lemma 1], if $|a|, |b| \leqslant H$ and $g(a, b, y) = 0$ then $y \ll_D |g|H^D$. If g were irreducible over $\mathbb{R}$, then an application of Pila's Theorem 2.3 would reveal that g has

$O_{D,\varepsilon}(H^{1+\varepsilon+1/d})$ integer roots (a, b, y) with $|a|, |b|, |y| \leqslant H$. Theorem 6.3 is a variant of this for which y is not constrained to lie in $[-H, H]$.

Proof. Let $C = C_D$ be a large, positive constant, so that if $|a|, |b| \leqslant H$ and $g(a, b, y) = 0$ then $|y| \leqslant C|g|H^D$. We classify $b \in \mathbb{Z}$ as being:

- *good*, if $g(A, b, Y) \in \mathbb{Z}[A, Y]$ is irreducible;
- *bad*, if $g(A, b, Y) \in \mathbb{Z}[A, Y]$ is reducible but has no linear divisor;
- *superbad*, if $g(A, b, Y) \in \mathbb{Z}[A, Y]$ has a linear divisor.

Let $b \in [-H, H]$ be good. In Theorem 2.2 we have $T \geqslant (C|g|H^D)^d$, so there are at most $O(|g|^\varepsilon H^{\varepsilon+1/d})$ integer zeros $(a, y) \in [-H, H] \times [-C|g|H^D, C|g|H^D]$. Thus, there are at most $O(H^{1+\varepsilon+1/d})$ integer triples $(a, b, y) \in [-H, H]^2 \times [-C|g|H^D, C|g|H^D]$ such that b is good and $g(a, b, y) = 0$.

Next, let us suppose instead that $b \in [-H, H]$ is bad. By [19, Theorem 2.1], there exists an integer $a_0 \ll |g|^{O(1)}$ such that $g(a_0, B, Y) \in \mathbb{Z}[B, Y]$ is irreducible. As b is bad and g is monic in Y, the polynomial $g(a_0, b, Y) \in \mathbb{Z}[Y]$ is reducible, so by Theorem 6.1 there are $O(|g|^\varepsilon H^{\varepsilon+1/2})$ such choices of b. Let $h(A, Y) \in \mathbb{Z}[A, Y]$ be an irreducible divisor of $g(A, b, Y)$, and note from the choice of b that $\deg(h) \geqslant 2$. By Theorem 2.2, there are $O(H^{\varepsilon+1/2})$ zeros $(a, y) \in [-H, H] \times [-C|g|H^D, C|g|H^D]$ of h. Whence, there are $O(|g|^\varepsilon H^{1+\varepsilon})$ integer triples $(a, b, y) \in [-H, H]^2 \times \mathbb{R}$ such that b is bad and $g(a, b, y) = 0$.

Finally, we bound the number $\mathcal{N}$ of superbad integers $b \in [-H, H]$, and use this to estimate their contribution to the number of roots of g that we are counting. By [19, Theorem 2.1], choose an integer $a_0 \ll |g|^{O(1)}$ such that $g(a_0, B, Y) \in \mathbb{Z}[B, Y]$ is irreducible. If b is superbad then $g(A, b, Y) \in \mathbb{Z}[A, Y]$ has a divisor of the form $Y - tA$, for some $t \in \mathbb{Z}$, and in particular $g(a_0, b, Y) \in \mathbb{Z}[Y]$ has an integer root. Thus, by Theorem 2.2, we have

$$\mathcal{N} \leqslant \#\{(b, y) \in \mathbb{Z}^2 : |b| \leqslant H, \ |y| \leqslant C|g|H^D, \ g(a_0, b, y) = 0\} \ll |g|^\varepsilon H^{\varepsilon+1/d}.$$

There are $O(H)$ possibilities for a, and then there are at most d possibilities for y such that $h(a, b, y) = 0$. Hence, there are $O(|g|^\varepsilon H^{1+\varepsilon+1/d})$ integer triples $(a, b, y) \in [-H, H]^2 \times \mathbb{R}$ such that b is superbad and $h(a, b, y) = 0$.

We have considered all cases, and conclude that there are $O(|g|^\varepsilon H^{1+\varepsilon+1/d})$ integer triples $(a, b, y) \in [-H, H]^2 \times \mathbb{R}$ such that $h(a, b, y) = 0$. $\square$

6.3. Algebraic toolkit.

In the course of our treatment of higher-degree polynomials, we will work with Galois groups over two-parameter function fields, using the method of Uchida [44], Smith [42] and Cohen [17, 18]. Here we review some of the theory, following Cohen [17, 18]. A polynomial is *normal* if its factor type is $(1, \ldots, 1)$ or $(1, \ldots, 1, 2)$. The following criterion is similar to [17, Lemma 2].

Lemma 6.4 (Normality criterion). *Let $\mathcal{G}(X), \mathcal{H}(X) \in \mathbb{C}(X) \setminus \{0\}$ be coprime polynomials, and put $r = \mathcal{G}/\mathcal{H}$. Then $f := \mathcal{G} + b\mathcal{H}$ is normal for all $b \in \mathbb{C}$ if the following two statements hold:*

- *The system*

$$r'(x) = r''(x) = 0, \qquad \mathcal{H}(x) \neq 0 \tag{6.1}$$

  has no solution $x \in \mathbb{C}$.
- *The system*

$$r(x) - r(y) = r'(x) = r'(y) = 0, \qquad x \neq y, \qquad \mathcal{H}(x)\mathcal{H}(y) \neq 0 \tag{6.2}$$

  has no solution $(x, y) \in \mathbb{C}^2$.

Proof. Let $b \in \mathbb{C}$. First suppose f has a triple root $x \in \mathbb{C}$. Then

$$f(x) = f'(x) = f''(x) = 0, \qquad \mathcal{H}(x) \neq 0,$$

since $\mathcal{G}$ and $\mathcal{H}$ are coprime, and so

$$\mathcal{G}(x) = -b\mathcal{H}(x), \qquad \mathcal{G}'(x) = -b\mathcal{H}'(x), \qquad \mathcal{G}''(x) = -b\mathcal{H}''(x).$$

By the quotient rule

$$r'(x) = \frac{\mathcal{H}(x)\mathcal{G}'(x) - \mathcal{G}(x)\mathcal{H}'(x)}{\mathcal{H}(x)^2} = 0$$

and

$$r''(x) = \frac{\mathcal{H}(x)^2(\mathcal{H}(x)\mathcal{G}''(x) - \mathcal{G}(x)\mathcal{H}''(x)) - 2\mathcal{H}(x)\mathcal{H}'(x)(\mathcal{H}(x)\mathcal{G}'(x) - \mathcal{G}(x)\mathcal{H}'(x))}{\mathcal{H}(x)^4}$$

$$= 0.$$

In this case $x \in \mathbb{C}$ is a solution to (6.1).

Now suppose $x, y \in \mathbb{C}$ are distinct double roots of f. Then

$$f(x) = f'(x) = f(y) = f'(y) = 0, \qquad \mathcal{H}(x)\mathcal{H}(y) \neq 0,$$

since $\mathcal{G}$ and $\mathcal{H}$ are coprime, and so

$$\mathcal{G}(x) = -b\mathcal{H}(x), \quad \mathcal{G}'(x) = -b\mathcal{H}'(x), \quad \mathcal{G}(y) = -b\mathcal{H}(y), \quad \mathcal{G}'(y) = -b\mathcal{H}'(y).$$

By the quotient rule $r'(x) = r'(y) = 0$. Moreover, we have

$$r(x) - r(y) = -b + b = 0.$$

In this case $(x, y) \in \mathbb{C}^2$ is a solution to (6.2). $\qquad \square$

The following standard consequence of Bézout's theorem is a special case of [17, Lemma 3].

Lemma 6.5. *Let $n \in \mathbb{N}$, and let $f(X, Y), g(X, Y) \in \mathbb{C}(X, Y)$ be coprime polynomials of degree at most n. Then there are $O_n(1)$ solutions $(x, y) \in \mathbb{C}^2$ to*

$$f(x, y) = g(x, y).$$

If $P(X) \in \mathbb{C}[X]$ and $Q(X) \in \mathbb{C}[X] \setminus \{0\}$ are coprime and $R = P/Q$, we write

$$\deg(R) = \max\{\deg(P), \deg(Q)\},$$

as well as

$$B_R(X, Y) = Q(X)P(Y) - P(X)Q(Y) \in \mathbb{C}[X, Y]/\sim$$

and

$$B_R^*(X, Y) = \frac{B_R(X, Y)}{X - Y} \in \mathbb{C}[X, Y]/\sim,$$

where the equivalence relation is multiplication by a unit.

Lemma 6.6. *For $i = 1, 2$, let $P_i(X) \in \mathbb{C}[X]$ and $Q_i(X) \in \mathbb{C}[X] \setminus \{0\}$ be relatively prime, and suppose*

$$x, y \in \mathbb{C}, \qquad x \neq y, \qquad Q_1(x)Q_1(y)Q_2(x)Q_2(y) \neq 0.$$

Put $f_i = P_i/Q_i$ for $i = 1, 2$, and assume that

$$f_1(x)f_2(y) = f_1(y)f_2(x), \qquad f_2(x)f_2(y) \neq 0.$$

Then, with $R = f_1/f_2$, we have $B_R^*(x, y) = 0$.

Proof. Put

$$g = (P_1, P_2), \qquad P_1 = gp_1, \qquad P_2 = gp_2$$

and

$$h = (Q_1, Q_2), \qquad Q_1 = hq_1, \qquad Q_2 = hq_2.$$

Then

$$\frac{g(x)g(y)p_1(x)p_2(y)}{h(x)h(y)q_1(x)q_2(y)} = \frac{g(x)g(y)p_1(y)p_2(x)}{h(x)h(y)q_1(y)q_2(x)}.$$

As $g(x)g(y) \mid P_2(x)P_2(y)$, we have $g(x)g(y) \neq 0$, so

$$R(x) = \frac{p_1(x)q_2(x)}{q_1(x)p_2(x)} = \frac{p_1(y)q_2(y)}{q_1(y)p_2(y)} = R(y),$$

and so $B_R(x, y) = 0$. As $x \neq y$, we finally have $B_R^*(x, y) = 0$. $\qquad \square$

The following lemma is essentially [17, Lemma 4].

Lemma 6.7. *Let $R_1(X) \in \mathbb{C}(X)$, and suppose $D(X, Y) \in \mathbb{C}[X, Y]$ is a non-constant divisor of $B_{R_1}^*(X, Y)$. Then there exists $R(X) \in \mathbb{C}(X)$ with the following properties:*
  (i) If $R_2(X) \in \mathbb{C}(X)$, then $D(X, Y)$ divides $B_{R_2}^*(X, Y)$ if and only if $R_2(X) \in \mathbb{C}(R(X))$.
  (ii) $\deg(R) \geqslant 2$.
  (iii) $R = P/Q$, where $P(X), Q(X) \in \mathbb{C}[X] \setminus \{0\}$ and $\deg(P) > \deg(Q)$.

Proof. Let $\alpha_1, \ldots, \alpha_u \in \overline{\mathbb{C}(X)}$ be the roots of $D(X, Y)$, regarded as a polynomial in Y with coefficients in $\mathbb{C}[X]$, and let $\alpha_{u+1}, \ldots, \alpha_v \in \overline{\mathbb{C}(X)}$ be the other roots of $B_{R_1}^*(X, Y)$. Set

$$E = \mathbb{C}(X, \alpha_1, \ldots, \alpha_v),$$

and write $R_1(Y) = f_1(Y)/g_1(Y)$ with $f_1(Y), g_1(Y) \in \mathbb{C}[Y]$ relatively prime. The polynomial

$$f_1(Y) - R_1(X)g_1(Y) \in \mathbb{C}(R_1(X))[Y]$$

is irreducible over $\mathbb{C}(R_1(X))$, and is therefore separable over this perfect field. Therefore E, being its splitting field, is a Galois extension of $\mathbb{C}(R_1(X))$, and moreover $X, \alpha_1, \ldots, \alpha_v$ are pairwise distinct. Let G be the Galois group of E over $\mathbb{C}(R_1(X))$, and denote by S the set of $\sigma \in G$ such that

$$\sigma(X) \in \{X, \alpha_1, \ldots, \alpha_u\}.$$

As S contains the stabiliser of X, the field $E_1 := E^S$ lies between $\mathbb{C}$ and $\mathbb{C}(X) = E^{\text{Stab}(X)}$. Thus, by Lüroth's theorem [20, Chapter 4, Theorem 6.8], there exists $R(X) \in \mathbb{C}(X)$ such that $E_1 = \mathbb{C}(R(X))$. Moreover, as $R_1(X) \in E_1 \setminus \mathbb{C}$, we know that $R(X)$ is non-constant.

As $f_1(Y) - R_1(X)g_1(Y)$ is irreducible over $\mathbb{C}(R_1(X))$, its Galois group G acts transitively on its roots $X, \alpha_1, \ldots, \alpha_v$. Thus, for each $i \in \{1, 2, \ldots, u\}$ there exists $\sigma_i \in S$ such that $\sigma_i(X) = \alpha_i$. Finally, for $R_2(X) \in \mathbb{C}(X)$, we have

$$\begin{aligned} D(X, Y) \mid B_{R_2}^*(X, Y) &\Leftrightarrow B_{R_2}(X, \alpha_i) = 0 \qquad (1 \leqslant i \leqslant u) \\ &\Leftrightarrow R_2(X) = R_2(\alpha_i) \qquad (1 \leqslant i \leqslant u) \\ &\Leftrightarrow R_2(X) \in E^S = \mathbb{C}(R(X)). \end{aligned}$$

To see that $\deg(R) \geqslant 2$, observe that $D(X, Y)$ does not divide $B_X^*(X, Y) = 1$. Therefore $X \notin \mathbb{C}(R(X))$, so $\deg(R) \neq 1$. As R is not constant and $\deg(R) \neq 1$, we must have $\deg(R) \geqslant 2$.

For the third property, we can swap P and Q if necessary to ensure that $\deg(P) \geqslant \deg(Q)$. If $\deg(P) = \deg(Q)$ then we can subtract a linear multiple of P from Q to reduce the degree of Q below that of P, securing the third property. All of this leaves $\mathbb{C}(R(X))$ unchanged, so our modified rational function R still has the first two properties. $\qquad \square$

We also require the following standard, elementary fact.

Lemma 6.8. *If a group G acts doubly-transitively on $\{1, 2, \ldots, n\}$ and contains a transposition, then G is the full symmetric group.*

Proof. By symmetry, we may suppose that $n \geqslant 2$ and $(12) \in G$. Let $i, j \in \{1, 2, \ldots, n\}$ be distinct. As G acts doubly-transitively, there exists $\sigma \in G$ with $\sigma(1) = i$ and $\sigma(2) = j$. Now $(ij) = \sigma(12)\sigma^{-1} \in G$. $\qquad\square$

7. Higher-degree polynomials

In this section, we establish Theorem 1.9. Let us start by showing that $d \geqslant 240$, which is the first assertion of the theorem. By [23, Lemma 3], if $n \geqslant 12$ then

$$d \geqslant \frac{1}{2}\binom{n}{\lfloor n/2 \rfloor} \geqslant 462.$$

We see from the classification by Butler and McKay [12] that if $n \in \{9, 11\}$ then $d \geqslant 240$. In particular, we have secured the inequality $d \geqslant 240$ in all cases covered by the theorem. It remains to show that

$$N_{G,n} \ll_{n,\varepsilon} H^{n+\varepsilon - 3/2 + 3d^{-1/3}}. \tag{7.1}$$

We use the notation (4.1).

7.1. **Non-degenerate tuples.**
We wish to count monic, irreducible polynomials f of degree n, with integer coefficients in $[-H, H]$, for which $G_f = G$. Recalling (4.2) and (4.3), given such a polynomial f, the associated resolvent Φ has an integer root $y \ll_n H^{O_n(1)}$. To ease notation, we write

$$a = a_{n-2}, \qquad b = a_{n-1}, \qquad c = a_n,$$

so that

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 + aX^2 + bX + c. \tag{7.2}$$

Let us choose

$$(a_1, \ldots, a_{n-3}) \in (\mathbb{Z} \cap [-H, H])^{n-3}$$

non-degenerate, meaning that

$$-2a_3 \neq \binom{n}{3}(-2a_1/n)^3 + \binom{n-1}{2}(-2a_1/n)^2 a_1 + (n-2)(-2a_1/n)a_2 \tag{7.3}$$

and the vanishing of $g(a, b, c, y) = \Phi(y; a_1, \ldots, a_{n-3}, a, b, c)$ cuts out an absolutely irreducible affine threefold $\mathcal{Y} = \mathcal{Y}_{a_1, \ldots, a_{n-3}}$. By Theorem 2.4, there exist

$$g_1(a, b, c, y), \ldots, g_J(a, b, c, y) \in \mathbb{Z}[a, b, c, y],$$

coprime to $g(a, b, c, y)$ and of degree $O_{n,\varepsilon}(1)$, where $J \ll H^{\varepsilon + 3d^{-1/3}}$, such that if $(a, b, c, y) \in \mathcal{Y}$ and

$$|a|, |b|, |c| \leqslant H, \qquad y \ll_n H^{O_n(1)}$$

then

$$g(a, b, c, y) = g_j(a, b, c, y) = 0 \tag{7.4}$$

for some j. Now we fix j and count solutions to (7.4).

Note that $\deg_y(g) = d > 0$. If $\deg_y(g_j) = 0$ then let $F(a, b, c) = g_j(a, b, c, y)$, and otherwise let $F(a, b, c)$ be the resultant of g and g_j in the variable y. By [22, Chapter 3, §6, Proposition 3], applied with $k = \mathbb{Q}(a, b, c)$, this is a non-zero element of $\mathbb{Z}[a, b, c]$. By [22, Chapter 3, §6, Proposition 5], we have $F(a, b, c) = 0$ for any solution (a, b, c, y) to (7.4).

Next, we factorise over the reals. For $a, b, c \in \mathbb{Z}$, observe that $F(a, b, c) = 0$ if and only if we have $\mathcal{F}(a, b, c) = 0$ for some irreducible divisor $\mathcal{F}(a, b, c) \in \mathbb{R}[a, b, c]$ of $F(a, b, c)$. By Theorem 2.3, if $\mathcal{F}$ is non-linear then

$$\#\{(a, b, c) \in (\mathbb{Z} \cap [-H, H])^3 : \mathcal{F}(a, b, c) = 0\} \ll H^{\varepsilon + 3/2}.$$

Then y is determined from $g(a, b, c, y) = 0$ in at most d ways, so the number of solutions (a, b, c, y) counted in this case is $O(H^{\varepsilon + 3/2})$. The total contribution to $N_{G,n}$ from this non-linear case is therefore

$$O(H^{n-3} H^{\varepsilon + 3d^{-1/3}} H^{\varepsilon + 3/2}) \ll H^{2\varepsilon + n - 3/2 + 3d^{-1/3}}. \tag{7.5}$$

Next, suppose $\mathcal{F}$ is linear. Then

$$\mathcal{F}(a, b, c) = \alpha a + \beta b + \gamma c + \delta = 0,$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ with $(\alpha, \beta, \gamma) \neq (0, 0, 0)$. Supposing for the time being that $\mathcal{F}$ is not a multiple of a rational polynomial, we can write

$$\mathcal{F} = \sum_{i \leqslant r} \lambda_i F_i,$$

where $r \in \{2, 3, 4\}$, the F_i are linear polynomials with rational coefficients, and $\lambda_1, \ldots, \lambda_r$ are linearly independent over $\mathbb{Q}$. Following the argument presented in the proof of [29, Corollary 1], some F_i is not a multiple of $\mathcal{F}$, and any rational root of $\mathcal{F}$ must also be a root of this F_i. It then follows from linear algebra that there are $O(H)$ possibilities for (a, b, c). The contribution to $N_{G,n}$ from this situation is $O(H^{n-2+\varepsilon + 3d^{-1/3}})$.

Thus, we may assume in the sequel that $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Moreover, if $\mathcal{F}(a, b, c) = 0$ has an integer solution then $(\alpha, \beta, \gamma) \mid \delta$, so we may divide through by (α, β, γ) and assume that $(\alpha, \beta, \gamma) = 1$.

Lemma 7.1. *If* $\max\{|\alpha|, |\beta|, |\gamma|\} > H$ *then*

$$\#\{(a, b, c) \in (\mathbb{Z} \cap [-H, H]^3) : \alpha a + \beta b + \gamma c + \delta = 0\} \ll H.$$

Proof. By symmetry, we may assume that $\gamma > H$. We may also assume that there exists $(a_0, b_0, c_0) \in (\mathbb{Z} \cap [-H, H])^3$ for which

$$\alpha a_0 + \beta b_0 + \gamma c_0 + \delta = 0.$$

Now

$$\alpha x + \beta y + \gamma z = 0,$$

where $x = a - a_0$, $y = b - b_0$ and $z = c - c_0$ lie in $[-2H, 2H]$, and in particular

$$\alpha x + \beta y \equiv 0 \bmod \gamma.$$

This condition defines a full-rank lattice Λ of determinant γ, by [16, Lemma 2.14]. Its first successive minimum satisfies $\lambda_1 \geqslant 1$, since $\Lambda \subset \mathbb{Z}^2$. Thus, by [41, Lemma 2], we have

$$\#\{(x, y) \in \Lambda \cap [-2H, 2H]^2\} \ll \frac{H^2}{\gamma} + H \ll H.$$

$\square$

The contribution to $N_{G,n}$ from the scenario $\max\{|\alpha|, |\beta|, |\gamma|\} > H$ is therefore

$$O(H^{n-2+\varepsilon + 3d^{-1/3}}),$$

which is negligible for the purposes of proving (7.1). We may therefore suppose that $|\alpha|, |\beta|, |\gamma| \leqslant H$. Now there are no solutions $(a, b, c) \in [-H, H]^3$ to

$$\alpha a + \beta b + \gamma c + \delta = 0$$

unless $|\delta| \leqslant 3H^2$. Henceforth, we assume that

$$|\alpha|, |\beta|, |\gamma| \leqslant H, \qquad |\delta| \leqslant 3H^2. \tag{7.6}$$

Polynomials $G_0(X), G_1(X), G_2(X) \in \mathbb{C}[X]$ are *strongly totally composite* if there exist a rational function $R = P/Q$, where $P(X) \in \mathbb{C}[X]$ and $Q(X) \in \mathbb{C}[X] \setminus \{0\}$ are coprime, and $P_0(X), P_1(X), P_2(X) \in \mathbb{C}[X]$, such that

$$\deg(R) \geqslant 2, \qquad \deg(P) > \deg(Q), \qquad L := \max\{\deg(P_0), \deg(P_1), \deg(P_2)\} \geqslant 2,$$

and

$$G_i(X) = Q(X)^L P_i(R(X)) \qquad (i = 0, 1, 2).$$

The analysis naturally divides into three cases. The overall structure of the argument will be the same in the three cases, but some details will differ.

7.1.1. *Case 1: $\gamma \neq 0$.* Then

$$\begin{aligned} f(X) &= X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 + a X^2 + b X - \gamma^{-1}(\alpha a + \beta b + \delta) \\ &= G_0(X) + a G_1(X) + b G_2(X), \end{aligned}$$

where

$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 - \delta/\gamma, \quad G_1(X) = X^2 - \alpha/\gamma, \quad G_2(X) = X - \beta/\gamma.$$

We study $\mathrm{Gal}(f, \mathbb{C}(a, b))$ using the method of Uchida [44], Smith [42] and Cohen [17, 18]. As we only wish to count irreducible polynomials, we may assume that there exists an irreducible specialisation over the rationals. Whence f is irreducible over $\mathbb{Q}(a, b)$, and is therefore also separable. Note that G_0, G_1, G_2 are coprime, and that they are linearly independent over $\mathbb{C}$.

Recall the following elementary fact.

Lemma 7.2. *Let $n \geqslant 3$ be an integer, and let G be a group. Then the action of G on $\{1, 2, \ldots, n\}$ is doubly-transitive if and only if the stabiliser subgroup of any point acts transitively on the remaining points.*

Proof. The forward direction is clear. For the backward direction, let $i_1 \neq i_2$ and $j_1 \neq j_2$ be elements of $\{1, 2, \ldots, n\}$, and let $k \in \{1, 2, \ldots, n\} \setminus \{i_1, j_1\}$. Then the composition

$$\begin{aligned} i_1 &\mapsto i_1 \mapsto j_1 \mapsto j_1 \\ i_2 &\mapsto k \mapsto k \mapsto j_2 \end{aligned}$$

maps (i_1, i_2) to (j_1, j_2). $\square$

In light of this, the Galois group of f is doubly-transitive if and only if $f(X)/(X - x)$ is irreducible over $\mathbb{C}(a, b, x)$ for any root $x \in \overline{\mathbb{C}(a, b)}$. Note that any root of f must be transcendental over $\mathbb{C}$.

Lemma 7.3. *The permutation group $\mathrm{Gal}(f, \mathbb{C}(a, b))$ is doubly-transitive.*

This is analogous to [18, Lemma 4].

Proof. Assume for a contradiction that $\mathrm{Gal}(f, \mathbb{C}(a, b))$ is not doubly-transitive. Then there exists a root $x \in \overline{\mathbb{C}(a, b)}$ of f such that $f(X)/(X - x)$ is reducible over $\mathbb{C}(a, b, x)$. By Gauss's lemma, the polynomial $f(X)/(X - x)$ is reducible over $\mathbb{C}[a, b, x]$. As $f(x) = 0$, we have

$$bG_2(x) = -G_0(x) - aG_1(x),$$

so

$$G_2(x)f(X) = G_2(x)(G_0(X) + aG_1(X) + bG_2(X))$$
$$= G_2(x)G_0(X) - G_0(x)G_2(X) + a(G_2(x)G_1(X) - G_1(x)G_2(X)).$$

This is linear in a and separable in X, so for $f(X)/(X - x)$ to be reducible there must exist $\xi \in \overline{\mathbb{C}(x)} \setminus \{x\}$ for which

$$G_2(x)G_i(\xi) = G_2(\xi)G_i(x) \qquad (i = 0, 1).$$

Note that $x \neq \beta/\gamma$, being transcendental over $\mathbb{C}$. The equation with $i = 1$ is quadratic in ξ, with one of the roots being x. Therefore ξ equals the other root:

$$\xi = \frac{x^2 - \alpha/\gamma}{x - \beta/\gamma} - x = \frac{\beta x - \alpha}{\gamma x - \beta}.$$

Substituting this into the equation with $i = 0$ yields

$$\left(x - \frac{\beta}{\gamma}\right) G_0\left(\frac{\beta x - \alpha}{\gamma x - \beta}\right) = \left(\frac{\beta x - \alpha}{\gamma x - \beta} - \frac{\beta}{\gamma}\right) G_0(x) = \frac{\beta^2 - \alpha\gamma}{\gamma(\gamma x - \beta)} G_0(x),$$

or equivalently

$$(\gamma x - \beta)^n G_0\left(\frac{\beta x - \alpha}{\gamma x - \beta}\right) - (\beta^2 - \alpha\gamma)(\gamma x - \beta)^{n-2} G_0(x) = 0.$$

As x is transcendental over $\mathbb{C}$, it cannot be the root of a non-zero polynomial over $\mathbb{C}$, and whence

$$(\gamma X - \beta)^n G_0\left(\frac{\beta X - \alpha}{\gamma X - \beta}\right) - (\beta^2 - \alpha\gamma)(\gamma X - \beta)^{n-2} G_0(X) = 0 \in \mathbb{C}[X],$$

or equivalently

$$G_0\left(\frac{\beta X - \alpha}{\gamma X - \beta}\right) = \frac{(\beta^2 - \alpha\gamma)G_0(X)}{(\gamma X - \beta)^2} \in \mathbb{C}(X).$$

Taking $X \to \infty$ yields $\beta^2 - \alpha\gamma = 0$ and $G_0(\beta/\gamma) = 0$. As

$$G_1(\beta/\gamma) = \beta^2/\gamma^2 - \alpha/\gamma = \gamma^{-2}(\beta^2 - \alpha\gamma) = 0, \qquad G_2(\beta/\gamma) = 0,$$

we now have $f(\beta/\gamma) = 0$, contradicting the irreducibility of f over $\mathbb{Q}(a, b)$. $\qquad \square$

We will show that the permutation group $\mathrm{Gal}(f, \mathbb{C}(a, b))$ contains a transposition, but first we require a preparatory result.

Lemma 7.4. *The polynomials G_0, G_1, G_2 are not strongly totally composite.*

Proof. Suppose for a contradiction that

$$G_2(X) = Q(X)^L P_2(R(X)), \qquad R = P/Q,$$

where $P(X), Q(X) \in \mathbb{C}[X] \setminus \{0\}$ are coprime, $P_2(X) \in \mathbb{C}[X]$, and

$$\deg(P) > \max\{\deg(Q), 1\}, \qquad L \geq s := \deg(P_2), \qquad L \geq 2.$$

Writing

$$P_2(X) = b_s X^s + \cdots + b_0, \qquad b_0, \ldots, b_s \in \mathbb{C}, \qquad b_s \neq 0,$$

we have
$$X - \beta/\gamma = Q(X)^{L-s}(b_s P(X)^s + \cdots + b_0 Q(X)^s).$$
The right hand side has degree $(L-s)\deg(Q) + s \cdot \deg(P) \geqslant (L-s)\deg(Q) + 2s$. Now $s = 0$ and $\deg(Q) = 0$, and we reach a contradiction, completing the proof. $\qquad\square$

Lemma 7.5. *The permutation group* $\mathrm{Gal}(f, \mathbb{C}(a,b))$ *contains a transposition.*

This is analogous to [18, Corollary 6 and Lemma 7].

Proof. By [18, Corollary 6], it suffices to establish the existence of $a, b \in \mathbb{C}$ for which f has factor type $(1, \ldots, 1, 2)$. We proceed in two steps. The first is to show that, for all but finitely many $a \in \mathbb{C}$, there exists $b \in \mathbb{C}$ such that $\Delta = 0$. To achieve this, we need to demonstrate the existence of $x, b \in \mathbb{C}$ such that
$$G_0(x) + aG_1(x) + bG_2(x) = 0, \qquad G_0'(x) + aG_1'(x) + b = 0.$$
We choose $b = -(G_0'(x) + aG_1'(x))$, and now we need to solve
$$G_0(x) + aG_1(x) - (G_0'(x) + aG_1'(x))G_2(x) = 0.$$
As $G_1(X) - G_1'(X)G_2(X) = X^2 - \alpha/\gamma - 2X(X - \beta/\gamma)$ is non-constant, there can be at most one value of a for which
$$G_0(X) + aG_1(X) - (G_0'(X) + aG_1'(X))G_2(X)$$
is constant. For any other value of $a \in \mathbb{C}$, there must exist a solution $x \in \mathbb{C}$. This completes the first step.

The remaining second step is to show that, for all but finitely many $a \in \mathbb{C}$, for any $b \in \mathbb{C}$ the polynomial f is normal. For this we will apply Lemma 6.4 with $\mathcal{G} = G_0 + aG_1$ and $\mathcal{H} = G_2$. As
$$\mathcal{G}\left(\frac{\beta}{\gamma}\right) = G_0\left(\frac{\beta}{\gamma}\right) + a\left(\frac{\beta^2}{\gamma^2} - \frac{\alpha}{\gamma}\right)$$
is a non-zero polynomial of degree at most 1 in the variable a, there is at most one value of $a \in \mathbb{C}$ such that $\mathcal{G}$ and $\mathcal{H}$ are not coprime over $\mathbb{C}$.

Suppose $a, x \in \mathbb{C}$ and that we have (6.1), where $r = \mathcal{G}/\mathcal{H}$. Then
$$0 = \mathcal{H}(x)^2 r'(x) = \mathcal{H}(x)\mathcal{G}'(x) - \mathcal{G}(x)\mathcal{H}'(x)$$
$$= (x - \beta/\gamma)(G_0'(x) + 2xa) - (G_0(x) + a(x^2 - \alpha/\gamma))$$
and
$$0 = \mathcal{H}(x)^3 r''(x) = \mathcal{H}(x)(\mathcal{H}(x)\mathcal{G}''(x) - \mathcal{G}(x)\mathcal{H}''(x)) - 2\mathcal{H}'(x)(\mathcal{H}(x)\mathcal{G}'(x) - \mathcal{G}(x)\mathcal{H}'(x))$$
$$= (x - \beta/\gamma)^2(G_0''(x) + 2a) - 2((x - \beta/\gamma)(G_0'(x) + 2xa) - (G_0(x) + a(x^2 - \alpha/\gamma))),$$
so
$$(x - \beta/\gamma)(G_0''(x) + 2a) = 0.$$
By (6.1), we have $x \neq \beta/\gamma$. Hence $2a = -G_0''(x)$, and so
$$2(x - \beta/\gamma)(G_0'(x) - G_0''(x)x) - 2G_0(x) + G_0''(x)(x^2 - \alpha/\gamma) = 0.$$
The polynomial has degree exactly n, so there are at most n solutions $(a, x) \in \mathbb{C}^2$ to (6.1).

Now suppose instead that we have (6.2) for some $a, x, y \in \mathbb{C}$. With
$$r_0 = G_0/\mathcal{H}, \qquad r_1 = G_1/\mathcal{H},$$

we have

$$M \begin{pmatrix} 1 \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

where

$$M = \begin{pmatrix} r_0(x) - r_0(y) & r_1(x) - r_1(y) \\ r_0'(x) & r_1'(x) \\ r_0'(y) & r_1'(y) \end{pmatrix}.$$

Assume for a contradiction that $\operatorname{rank}(M) = 0$. Then

$$2x = \frac{x^2 - \alpha/\gamma}{x - \beta/\gamma} = \frac{y^2 - \alpha/\gamma}{y - \beta/\gamma} = 2y,$$

contradicting (6.2). The upshot is that $\operatorname{rank}(M) \geqslant 1$.

There are no solutions $a \in \mathbb{C}$ if $\operatorname{rank}(M) = 2$, so we may assume in the sequel that $\operatorname{rank}(M) = 1$, in which case there is at most one solution $a \in \mathbb{C}$. Next, we use an argument from [17]. Considering minors yields

$$r_0'(x)r_1'(y) = r_1'(x)r_0'(y)$$

and

$$r_0'(x)(r_1(x) - r_1(y)) = r_1'(x)(r_0(x) - r_0(y)),$$

as well as

$$r_0'(y)(r_1(x) - r_1(y)) = r_1'(y)(r_0(x) - r_0(y)).$$

Solutions with $r_0'(x)r_0'(y) = 0$. By symmetry, it suffices to consider solutions with $r_0'(y) = 0$. As

$$\mathcal{H}(y)^2 r_0'(y) = \mathcal{H}(y)G_0'(y) - G_0(y)$$

has degree n in y, there are only finitely many possibilities for y. Then

$$\mathcal{H}(x)^3 \mathcal{H}(y)(r_0'(x)(r_1(x) - r_1(y)) - r_1'(x)(r_0(x) - r_0(y)))$$
$$= (\mathcal{H}(x)G_0'(x) - G_0(x))(\mathcal{H}(y)G_1(x) - G_1(y)\mathcal{H}(x))$$
$$- (\mathcal{H}(x)G_1'(x) - G_1(x))(\mathcal{H}(y)G_0(x) - G_0(y)\mathcal{H}(x))$$

is a degree $n + 2$ polynomial in x, so it has finitely many zeros. We conclude that there are finitely many solutions (a, x, y) of this type.

Solutions with $r_0'(x)r_0'(y) \neq 0$. We have

$$r_0'(x)r_1(x) - r_0(x)r_1'(x) = r_0'(x)r_1(y) - r_0(y)r_1'(x),$$

and so

$$r_0'(y)(r_0'(x)r_1(x) - r_0(x)r_1'(x)) = r_0'(y)(r_0'(x)r_1(y) - r_0(y)r_1'(x))$$
$$= r_0'(x)(r_0'(y)r_1(y) - r_0(y)r_1'(y)).$$

Thus, by Lemma 6.6, we have

$$B_{R_1}^*(x, y) = B_{R_2}^*(x, y) = 0,$$

where

$$R_1 = \frac{r_1'}{r_0'}, \qquad R_2 = \frac{r_0 r_1' - r_0' r_1}{r_0'}.$$

By Lemma 6.5, this has at most finitely many solutions unless the polynomials $B_{R_1}^*(X, Y)$ and $B_{R_2}^*(X, Y)$ have a common divisor of positive degree. Let us now assume the latter, for

a contradiction. By Lemma 6.7, there exist $R(X), \theta(X), \phi(X) \in \mathbb{C}(X)$ such that $\deg(R) \geqslant 2$ and

$$r_1'(X) = \theta(R(X))r_0'(X), \qquad r_0(X)r_1'(X) - r_0'(X)r_1(X) = \phi(R(X))r_0'(X), \qquad (7.7)$$

and furthermore

$$R = P/Q, \qquad P(X), Q(X) \in \mathbb{C}[X] \setminus \{0\}, \qquad \deg(P) > \deg(Q),$$

and P, Q are coprime.

Assume for a contradiction that θ is constant. Then, by the quotient rule, we have

$$\mathcal{H}G_1' - G_1\mathcal{H}' = \lambda(\mathcal{H}G_0' - G_0\mathcal{H}')$$

for some $\lambda \in \mathbb{C}$. More explicitly, we have

$$2X(X - \beta/\gamma) - (X^2 - \alpha/\gamma) = \lambda((X - \beta/\gamma)G_0'(X) - G_0(X)).$$

Equating X^n coefficients yields $\lambda = 0$, and then equating X^2 coefficients delivers a contradiction. Therefore θ is non-constant.

Next, we substitute the first equation of (7.7) into the second. As $r_0'(X) \neq 0$, this gives

$$\theta(R(X))r_0(X) - r_1(X) = \phi(R(X)).$$

Differentiating yields

$$r_1'(X) = \theta'(R(X))R'(X)r_0(X) + \theta(R(X))r_0'(X) - \phi'(R(X))R'(X).$$

Since $R', \theta' \neq 0$ and $r_1'(X) = \theta(R(X))r_0'(X)$, we now have

$$r_0(X) = \frac{\phi'(R(X))}{\theta'(R(X))}.$$

We had observed that there is at most one value of $a \in \mathbb{C}$ for which $\mathcal{G}$ and $\mathcal{H}$ are not coprime over $\mathbb{C}$. Let us now suppose that $a \in \mathbb{C}$ takes any other value. From the previous paragraph, we see that $r_0(X)$, and hence also $r_0(X) + ar_1(X)$, is a rational function of $R(X)$. Thus, for some coprime polynomials $g_0(X), g_1(X) \in \mathbb{C}[X]$, we have

$$\frac{\mathcal{G}(X)}{\mathcal{H}(X)} = \frac{g_0(R(X))}{g_1(R(X))}.$$

Put

$$L = \max\{\deg(g_0), \deg(g_1)\} \geqslant 1,$$

and observe that

$$\frac{\mathcal{G}(X)}{\mathcal{H}(X)} = \frac{Q(X)^L g_0(R(X))}{Q(X)^L g_1(R(X))}.$$

Suppose for a contradiction that the polynomials $Q(X)^L g_0(R(X))$ and $Q(X)^L g_1(R(X))$ are not coprime. Then some $x \in \mathbb{C}$ is a common root. If $Q(x) \neq 0$ then $R(x)$ is a common root of g_0 and g_1, which is impossible because g_0 and g_1 are coprime. Therefore $Q(x) = 0$. Let $i \in \{0, 1\}$ be such that $L = \deg(g_i)$, and write

$$g_i(X) = b_L X^L + b_{L-1} X^{L-1} + \cdots + b_0, \qquad b_0, \ldots, b_L \in \mathbb{C}, \qquad b_L \neq 0.$$

Then

$$0 = Q(x)^L g_i(P(x)/Q(x)) = b_L P(x)^L,$$

so $P(x) = 0$, contradicting the coprimality of P and Q. Hence $Q(X)^L g_0(R(X))$ and $Q(X)^L g_1(R(X))$ are coprime.

Now

$$\mathcal{G}(X) = \tau Q(X)^L g_0(R(X)), \qquad \mathcal{H}(X) = \tau Q(X)^L g_1(R(X)),$$

for some $\tau \in \mathbb{C} \setminus \{0\}$. We also know that $r_0(X)$ and $r_1(X)$ are rational functions of $R(X)$. Therefore

$$G_0(X) = Q(X)^L g_2(R(X)), \qquad G_1(X) = Q(X)^L g_3(R(X)),$$

for some rational functions g_2, g_3.

Let $g_2 = P_2/Q_2$, where $P_2(X), Q_2(X) \in \mathbb{C}[X]$ are coprime and $Q_2 \neq 0$, and let

$$L_2 = \deg(g_2).$$

Write

$$Q_2(X) = c_s X^s + c_{s-1} X^{s-1} + \cdots + c_0, \qquad c_s, \ldots, c_0 \in \mathbb{C}, \qquad c_s \neq 0.$$

Assume for a contradiction that $s > 0$. Arguing as before, the polynomial $Q_2(R(X))Q(X)^{L_2}$ is coprime to $P_2(R(X))Q(X)^{L_2}$. Therefore $Q_2(R(X))Q(X)^{L_2}$ divides $Q(X)^L$ in $\mathbb{C}[X]$. Whence $L \geqslant L_2 - s$, and

$$c_s P(X)^s + c_{s-1} P(X)^{s-1} Q(X) + \cdots + c_0 Q(X)^s = Q_2(R(X))Q(X)^s \mid Q(X)^{L-L_2+s}.$$

The polynomial $Q_2(R(X))Q(X)^s$ has degree $s \cdot \deg(P) > 0$. Therefore $L > L_2 - s$ and, for some $x \in \mathbb{C}$, we have

$$c_s P(x)^s + c_{s-1} P(x)^{s-1} Q(x) + \cdots + c_0 Q(x)^s = 0,$$

so $Q(x)^{L-L_2+s} = 0$. Now $Q(x) = 0$, which implies that $c_s P(x)^s = 0$ and so $P(x) = 0$, this being impossible because P and Q are coprime.

Hence $s = 0$. The upshot is that g_2 is a polynomial, and similarly g_3 is a polynomial. Recall that

$$G_0(X) = Q(X)^L g_2(R(X)), \qquad G_1(X) = Q(X)^L g_3(R(X))$$

and

$$G_2(X) = \mathcal{H}(x) = Q(X)^L \cdot \tau g_1(R(X)),$$

where $\tau \in \mathbb{C} \setminus \{0\}$. As

$$G_0(X) + aG_1(X) = Q(X)^L g_0(R(X)),$$

we deduce that

$$\deg(g_0) = \deg(g_2) > \deg(g_3),$$

whereupon

$$L = \max\{\deg(g_1), \deg(g_2), \deg(g_3)\},$$

and finally

$$L \geqslant 2$$

by the linear independence of G_0, G_1, G_2. This contradicts Lemma 7.4, that G_0, G_1, G_2 are not strongly totally composite.

We conclude that, for all but finitely many values of $a \in \mathbb{C}$, the systems (6.1) and (6.2) each have no solutions $x, y \in \mathbb{C}$. Thus, by Lemma 6.4, for any $b \in \mathbb{C}$ the polynomial f is normal. This completes the second step, and with it the proof of the lemma. $\qquad \square$

By Lemmas 6.8, 7.3, and 7.5, we have $\mathrm{Gal}(f, \mathbb{C}(a,b)) = S_n$. As $\mathrm{Gal}(f, \mathbb{Q}(a,b))$ contains $\mathrm{Gal}(f, \mathbb{C}(a,b))$, we conclude that

$$\mathrm{Gal}(f, \mathbb{Q}(a,b)) = S_n.$$

Let h be as in Lemma 4.6, and note that $\deg(h) \ll_n 1$. By Lemma 4.1, if $G_f = G$ then $h(a,b,y) = 0$ for some $y \in \mathbb{Z}$. This has $O(H^{1+\varepsilon+1/d})$ integer roots (a,b,y) with $|a|, |b| \leqslant H$, by (7.6) and Theorem 6.3. In summary, this case $\gamma \neq 0$ contributes $O(H^{\varepsilon+n-2+3d^{-1/3}+d^{-1}})$ to $N_{G,n}$.

7.1.2. *Case 2: $\gamma = 0$ and $\beta \neq 0$.* Then

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 + a X^2 - \beta^{-1}(\alpha a + \delta) X + c$$
$$= G_0(X) + a G_1(X) + c G_2(X),$$

where

$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3} X^3 - \frac{\delta}{\beta} X, \quad G_1(X) = X^2 - \frac{\alpha}{\beta} X, \quad G_2(X) = 1.$$

We may assume that f is irreducible over $\mathbb{Q}(a, c)$, and therefore also separable.

Lemma 7.6. *The permutation group* $\mathrm{Gal}(f, \mathbb{C}(a, c))$ *is doubly-transitive.*

Proof. We imitate the proof of Lemma 7.3. Assume for a contradiction that $\mathrm{Gal}(f, \mathbb{C}(a, c))$ is not doubly-transitive. Then there exists a root $x \in \overline{\mathbb{C}(a, b)}$ of f such that $f(X)/(X - x)$ is reducible over $\mathbb{C}[a, b, x]$. Now

$$c G_2(x) = -G_0(x) - a G_1(x),$$

so

$$G_2(x) f(X) = G_2(x) G_0(X) - G_0(x) G_2(X) + a(G_2(x) G_1(X) - G_1(x) G_2(X)).$$

This is linear in a and separable in X, so for $f(X)/(X - x)$ to be reducible there must exist $\xi \in \overline{\mathbb{C}(x)} \setminus \{x\}$ such that

$$G_2(x) G_i(\xi) = G_2(\xi) G_i(x) \qquad (i = 0, 1).$$

The equation with $i = 1$, namely

$$\xi^2 - \frac{\alpha}{\beta} \xi = x^2 - \frac{\alpha}{\beta} x,$$

is quadratic in ξ with one of the roots being x. Therefore ξ equals the other root:

$$\xi = \frac{\alpha}{\beta} - x.$$

Substituting this into the equation with $i = 0$ yields

$$G_0\left(\frac{\alpha}{\beta} - x\right) = G_0(x).$$

As x is transcendental over $\mathbb{C}$, it cannot be the root of a non-zero polynomial over $\mathbb{C}$, and whence

$$G_0\left(\frac{\alpha}{\beta} - X\right) = G_0(X). \tag{7.8}$$

Equating X^n coefficients tells us that n is even. Then, equating X^{n-1} coefficients gives

$$-n\alpha/\beta - a_1 = a_1,$$

so $\alpha/\beta = -2a_1/n$. Finally, equating X^{n-3} coefficients yields

$$-2a_3 = \binom{n}{3}(\alpha/\beta)^3 + \binom{n-1}{2}(\alpha/\beta)^2 a_1 + (n-2)(\alpha/\beta) a_2$$
$$= \binom{n}{3}(-2a_1/n)^3 + \binom{n-1}{2}(-2a_1/n)^2 a_1 + (n-2)(-2a_1/n) a_2,$$

contradicting (7.3) and completing the proof. $\qquad \square$

Lemma 7.7. *The polynomials G_0, G_1, G_2 are not strongly totally composite.*

Proof. Suppose for a contradiction that

$$G_i(X) = Q(X)^L P_i(R(X)) \qquad (i = 0, 1, 2), \qquad R = P/Q,$$

where $P(X), Q(X) \in \mathbb{C}[X] \setminus \{0\}$ are coprime,

$$P_0(X), P_1(X), P_2(X) \in \mathbb{C}[X], \qquad s_1 := \deg(P_1), \qquad s_2 := \deg(P_2),$$

and

$$\deg(P) > \max\{\deg(Q), 1\}, \qquad L \geqslant \max\{s_1, s_2, 2\}.$$

Writing

$$P_2(X) = b_{s_2} X^{s_2} + \cdots + b_0, \qquad b_0, \ldots, b_{s_2} \in \mathbb{C}, \qquad b_{s_2} \neq 0$$

and

$$P_1(X) = c_{s_1} X^{s_1} + \cdots + c_{s_1}, \qquad c_{s_1}, \ldots, c_{s_1} \in \mathbb{C}, \qquad c_{s_1} \neq 0$$

we have

$$1 = Q(X)^{L-s_2}(b_{s_2} P(X)^{s_2} + \cdots + b_0 Q(X)^{s_2})$$

and

$$X(X - \alpha/\beta) = Q(X)^{L-s_1}(c_{s_1} P(X)^{s_1} + \cdots + c_0 Q(X)^{s_1}).$$

Therefore

$$0 = (L - s_2)\deg(Q) + s_2 \cdot \deg(P)$$

and

$$2 = (L - s_1)\deg(Q) + s_1 \cdot \deg(P).$$

The only possibility is

$$s_2 = 0, \qquad \deg(Q) = 0, \qquad s_1 = 1, \qquad \deg(P) = 2.$$

Now, for some $\lambda_0 \in \mathbb{C}$, we have

$$X(X - \alpha/\beta) = \lambda_0^{L-1}(c_1 P(X) + c_0 \lambda_0).$$

As $\lambda_0, c_1 \neq 0$, this enables us to write G_0 as a polynomial in $X(X - \alpha/\beta)$. In particular, we have (7.8), and this leads to a contradiction in the same way as in Case 1. $\qquad \square$

Lemma 7.8. *The permutation group* $\mathrm{Gal}(f, \mathbb{C}(a, c))$ *contains a transposition.*

Proof. Following the proof of Lemma 7.5, the first step is to show that if $a \in \mathbb{C}$ then there exist $x, c \in \mathbb{C}$ such that

$$G_0(x) + aG_1(x) + c = 0, \qquad G_0'(x) + aG_1'(x) = 0.$$

The second equation is the vanishing of a non-zero polynomial, so it has a solution x, and then the first equation has a solution c. The rest of the proof is essentially the same as in Case 1. $\qquad \square$

By Lemmas 6.8, 7.6, and 7.8, we have $\mathrm{Gal}(f, \mathbb{C}(a, c)) = S_n$. Arguing as in the previous case, we find that this case, too, contributes $O(H^{\varepsilon + n - 2 + 3d^{-1/3} + d^{-1}})$ to $N_{G,n}$.

7.1.3. *Case 3: $\beta = \gamma = 0$ and $\alpha \neq 0$.* Then

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3}X^3 - \alpha^{-1}\delta X^2 + bX + c$$
$$= G_0(X) + bG_1(X) + cG_2(X),$$

where

$$G_0(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3}X^3 - \alpha^{-1}\delta X^2, \quad G_1(X) = X, \quad G_2(X) = 1.$$

Similarly to the previous cases, or directly from [18, Theorem 1], we have $\mathrm{Gal}(f, \mathbb{C}(b,c)) = S_n$. Arguing as in the previous cases, we find that this case also contributes $O(H^{\varepsilon+n-2+3d^{-1/3}+d^{-1}})$ to $N_{G,n}$.

We conclude that non-degenerate tuples contribute $O(H^{\varepsilon+n-3/2+3d^{-1/3}})$ to $N_{G,n}$, the dominant contribution coming from (7.5).

7.2. Degenerate tuples. We begin by counting degenerate tuples. There are $O(H^{n-4})$ integer vectors $(a_1, \ldots, a_{n-3}) \in [-H, H]^{n-3}$ **not** satisfying (7.3).

For the degenerate tuples with (7.3), the idea is to show that $\mathcal{Y}_{a_1,\ldots,a_{n-3}}$ is absolutely irreducible for generic $a_1, \ldots, a_{n-3}$. Let

$$\mathcal{D}(a_1, \ldots, a_n) \in \mathbb{Z}[a_1, \ldots, a_n]$$

be the discriminant of $\Phi(y)$. As Φ has total degree $O_n(1)$, so too does $\mathcal{D}$. Further, we know from [23, Lemma 7] that $\mathcal{D}$ is not the zero polynomial. Whence, for all but $O(H^{n-4})$ integer vectors $(a_1, \ldots, a_{n-3}) \in [-H, H]^{n-3}$, the polynomial $g(a,b,c,y) = \Phi(y; a_1, \ldots, a_{n-3}, a, b, c)$ is separable in y.

Let $a_1, \ldots, a_{n-3}$ be integers such that $g(a, b, c, y)$ is separable in y, and recall (7.2). By [18, Theorem 1], applied to the field $F = \overline{\mathbb{Q}}(a)$, we have

$$\mathrm{Gal}(f, \overline{\mathbb{Q}}(a, b, c)) = S_n.$$

Suppose for a contradiction that

$$g(a, b, c, y) = g_1(y; a, b, c)g_2(y; a, b, c) \in \overline{\mathbb{Q}}(a, b, c)[y],$$

for some non-constant polynomials g_1, g_2. Let r_{σ_i} be a root of g_i ($i = 1, 2$), where for $\sigma \in S_n$ we write

$$r_\sigma = \sum_{\tau \in G}\prod_{i \leqslant n} \alpha^i_{\sigma\tau(i)},$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f in $\overline{\mathbb{Q}(a, b, c)}$. Then for $\kappa = \sigma_2 \sigma_1^{-1} \in \mathrm{Gal}(f, \overline{\mathbb{Q}}(a, b, c))$ we have $\kappa(r_{\sigma_1}) = r_{\sigma_2}$. As g_1 has coefficients in $\overline{\mathbb{Q}}(a, b, c)$, we now see that g_1 and g_2 have a common root $\kappa(r_{\sigma_1}) = r_{\sigma_2}$, which is impossible because g is separable.

We conclude that there are $O(H^{n-4})$ integer tuples

$$(a_1, \ldots, a_{n-3}) \in [-H, H]^{n-3}$$

such that $\mathcal{Y}_{a_1,\ldots,a_{n-3}}$ is reducible over $\overline{\mathbb{Q}}$. The upshot is that there are $O(H^{n-4})$ degenerate tuples $(a_1, \ldots, a_{n-3}) \in [-H, H]^{n-3}$ in total. Now let us fix such a tuple.

Write

$$\mathfrak{F}(a, b, c, X) = X^n + a_1 X^{n-1} + \cdots + a_{n-3}X^3 + aX^2 + bX + c.$$

By [23, Lemma 2], there are at most $O(H)$ values of $a, b \in \mathbb{Z} \cap [-H, H]$ for which the polynomial $\mathfrak{F}(a, b, c, X) \in \mathbb{Q}(c)[X]$ has non-S_n Galois group, where the implied constant is uniform in $a_1, \ldots, a_{n-3}$. The total contribution from these $O(H)$ special choices of a, b is $O(H^{n-2})$, since there are $O(H)$ possibilities for c.

For the other $O(H^2)$ specialisations of a, b, the polynomial

$$\mathcal{F}(c, X) := \mathfrak{F}(a, b, c, X) \in \mathbb{Q}(c)[X]$$

is separable with Galois group S_n. By Lemma 4.3, the polynomial

$$h(c, y) := \Phi_{\mathcal{F}, G}(c, y) \in \mathbb{Z}[c, y]$$

is irreducible, so by Theorem 2.2 there are $O(H^{\varepsilon+1/d})$ pairs $(c, y) \in \mathbb{Z}^2$ such that

$$h(c, y) = 0, \qquad |c| \leqslant H, \qquad y \ll_n H^{O_n(1)}.$$

We conclude that there are $O(H^{\varepsilon+n-2+1/d})$ tuples $(a_1, \ldots, a_n) \in (\mathbb{Z} \cap [-H, H])^n$, with $(a_1, \ldots, a_{n-3})$ degenerate, such that $G_f = G$.

In total there are $O(H^{\varepsilon+n-3/2+3d^{-1/3}})$ irreducible polynomials (4.1) with $\max_i |a_i| \leqslant H$ and Galois group G.

8. Even permutation groups

In this section, we establish Theorem 1.12. The inequality $d \geqslant 6$ follows from Theorem 1.9 when $n \geqslant 11$, and from the classification of transitive groups of low degree [12] when $3 \leqslant n \leqslant 10$. Let $(a_1, \ldots, a_{n-2}) \in (\mathbb{Z} \cap [-H, H])^{n-2}$, and let

$$g(a, b, y) = \Phi(y; a_1, \ldots, a_{n-2}, a, b).$$

First suppose $(a_1, \ldots, a_{n-2})$ is non-degenerate, meaning that g is absolutely irreducible. Denote by $\mathcal{Y}$ the affine surface cut out by the vanishing of g. By Theorem 2.5, there exist $g_1, \ldots, g_J \in \mathbb{Z}[a, b, y]$ with $J \ll H^{\varepsilon+1/\sqrt{d}}$, and a finite set $\mathcal{Z} \subset \mathcal{Y}$, such that

(1) Each g_j is coprime to g and has degree $O(1)$;
(2) $|\mathcal{Z}| \ll H^{\varepsilon+2/\sqrt{d}}$;
(3) If $(a, b, y) \in \mathcal{Y} \cap \mathbb{Z}^3 \setminus \mathcal{Z}$ and

$$|a|, |b| \leqslant H, \qquad y \ll_n H^{O_n(1)}$$

then

$$g(a, b, y) = g_j(a, b, y) = 0 \tag{8.1}$$

for some j.

The contribution to $N_{G,n}$ from $(a, b, y) \in \mathcal{Z}$ is $O(H^{\varepsilon+n-2+2/\sqrt{d}}) \ll H^{\varepsilon+n-3/2+1/\sqrt{d}}$, so in the non-degenerate case it remains to consider (8.1) for j fixed.

If $\deg_y(g_j) = 0$ then let $F(a, b) = g_j(a, b)$, and otherwise let $F(a, b)$ be the resultant of g and g_j in the variable y. Then $F(a, b) = 0$ whenever we have (8.1), whereupon $\mathcal{F}(a, b) = 0$ for some irreducible divisor $\mathcal{F}(a, b) \in \mathbb{Q}[a, b]$ of F. If $\mathcal{F}$ is non-linear, then Theorem 2.2 yields

$$\#\{(a, b) \in (\mathbb{Z} \cap [-H, H])^2 : \mathcal{F}(a, b) = 0\} \ll H^{\varepsilon+1/2},$$

and the contribution to $N_{G,n}$ from this case is $O(H^{\varepsilon+n-2+1/\sqrt{d}+1/2}) = O(H^{\varepsilon+n-3/2+1/\sqrt{d}})$. In the non-degenerate case, it remains to treat the scenario in which $\mathcal{F}$ is linear.

If the a coefficient of $\mathcal{F}(a, b)$ is non-zero, then we have $a = c_1 b + c_2$ for some $c_1, c_2 \in \mathbb{Q}$. As $G < A_n$, we have

$$P(b, z) := z^2 - \Delta(a_1, \ldots, a_{n-2}, c_1 b + c_2, b) = 0$$

for some $z \in \mathbb{N}$, where $\Delta(a_1, \ldots, a_n)$ denotes the discriminant of $X^n + a_1 X^{n-1} + \cdots + a_n$. The polynomial P is irreducible, by [24, Lemma 5], see [25, §6] for why we assume (1.4).

Let $C > 0$ be large, and note that Δ has total degree $2n - 2$, so if $|a_1|, \ldots, |a_n| \leqslant H$ then $|\Delta(a_1, \ldots, a_n)| \leqslant CH^{2n-2}$. Now Theorem 2.2 yields

$$\#\{(b, z) \in \mathbb{Z}^2 : |b| \leqslant H, |z| \leqslant CH^{n-1}, P(b, z) = 0\} \ll H^{\varepsilon + 1/2},$$

and the contribution to $N_{G,n}$ from this case is $O(H^{\varepsilon + n - 3/2 + 1/\sqrt{d}})$.

Otherwise $\mathcal{F}(a, b) = \lambda(b - \mu)$, for some $\mu \in \mathbb{Q}$ and some $\lambda \in \mathbb{Q} \setminus \{0\}$, and

$$Q(a, z) := z^2 - \Delta(a_1, \ldots, a_{n-2}, a, \mu) = 0$$

for some $z \in \mathbb{N}$. The polynomial Q is irreducible, by [24, Lemma 6], see [25, §6] for why we assume (1.4). Now Theorem 2.2 yields

$$\#\{(a, z) \in \mathbb{Z}^2 : |a| \leqslant H, |z| \leqslant CH^{n-1}, Q(a, z) = 0\} \ll H^{\varepsilon + 1/2},$$

and the contribution to $N_{G,n}$ from this case is $O(H^{\varepsilon + n - 3/2 + 1/\sqrt{d}})$.

For degenerate tuples, we can follow §7.2 with minimal changes. We find that their contribution to $N_{G,n}$ is $O(H^{\varepsilon + n - 2 + 1/d})$.

We have considered all cases, completing the proof of Theorem 1.12.

References

[1] L. Bary-Soroker, D. Koukoulopoulos and G. Kozma, *Irreducibility of random polynomials: general measures*, arXiv:2007.14567.

[2] L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height*, Duke Math. J. **169** (2020), 579–598.

[3] C. Bertone, G. Chèze and A. Galligo, *Modular Las Vegas algorithms for polynomial absolute factorization*, J. Symbolic Comput. **45** (2010), 1280–1295.

[4] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063.

[5] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's Conjecture*, arXiv:2111.06507.

[6] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), 191–242.

[7] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc. **33** (2020), 1087–1099.

[8] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.

[9] E. Breuillard and P. Varjú, *Irreducibility of random polynomials of large degree*, Acta Math. **223** (2019), 195–249.

[10] T. D. Browning, *Power-free values of polynomials*, Arch. Math. **96** (2011), 139–150.

[11] T. D. Browning and D. R. Heath-Brown, *Plane curves in boxes and equal sums of two powers*, Math. Z. **251** (2005), 233–247.

[12] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.

[13] R. Chela, *Reducible polynomials*, J. Lond. Math. Soc. **38** (1963), 183–188.

[14] A. Castillo and R. Dietmann, *On Hilbert's irreducibility theorem*, Acta Arith. **180** (2017), 1–14.

[15] S. Chow and R. Dietmann, *Enumerative Galois theory for cubics and quartics*, Adv. Math. **372** (2020).

[16] S. Chow and N. Technau, *Littlewood and Duffin–Schaeffer-type problems in diophantine approximation*, Mem. Amer. Math. Soc., to appear, arXiv:2010.09069.

[17] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) **6** (1972), 93–102.

[18] S. D. Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math. **90** (1980), 63–76.

[19] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3) **43** (1981) 227–250.

[20] P. M. Cohn, *Algebraic numbers and algebraic functions*, Chapman and Hall Mathematics Series, London, 1991.

[21] D. A. Cox, *Galois theory*, second edition, Wiley and Sons, Hoboken, NJ, 2012.

[22] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, fourth edition, Undergraduate Texts in Mathematics, Springer, Cham, 2015.

[23] R. Dietmann, *On the distribution of Galois groups*, Mathematika **58** (2012), 35–44.

[24] R. Dietmann, *Probabilistic Galois theory*, Bull. Lond. Math. Soc. **45** (2013), 453–462.

[25] R. Dietmann, A. Ostafe and I. E. Shparlinski, *Discriminants of fields generated by polynomials of given height*, Israel J. Math., to appear, arXiv:1909.00135.

[26] S. Eberhard, *The characteristic polynomial of a random matrix*, Combinatorica (2022), 1–37.

[27] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 91–101, Amer. Math. Soc., Providence, RI, 1973.

[28] T. R. Hagedorn, *General Formulas for Solving Solvable Sextic Equations*, J. Algebra **233** (2000), 704–757.

[29] D. R. Heath-Brown, *The Density of Rational Points on Curves and Surfaces*, Ann. of Math. (2) **155** (2002), 553–598.

[30] D. R. Heath-Brown, *Counting Rational Points on Algebraic Varieties*, Analytic Number Theory, pp. 51–95, Lecture Notes in Mathematics **1891,** Springer, Berlin–Heidelberg, 2006.

[31] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[32] F. Jouve, E. Kowalski and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), 263–307.

[33] H. W. Knobloch, *Die Seltenheit der reduziblen Polynome*, Jber. Deutsch. Math. Verein. **59** (1956), Abt. 1, 12–19.

[34] A. Landesman, R. J. Lemke Oliver and F. Thorne, *Improved lower bounds for the number of fields with alternating Galois group*, Bull. Lond. Math. Soc. **53** (2021) 1159–1173.

[35] P. Lefton, *On the Galois groups of cubics and trinomials*, Acta Arith. **XXXV** (1979), 239–246.

[36] R. J. Lemke Oliver and F. Thorne, *Upper bounds on polynomials with small Galois group*, Mathematika **66** (2020), 1054–1059.

[37] H. T. Pham and M. W. Xu, *Irreducibility of random polynomials of bounded degree*, Discrete Analysis 2021:7, 16 pp.

[38] J. Pila, *Density of integral and rational points on varieties*, Asterisque **228** (1995), 183–187.

[39] I. Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. **142** (2008), 353–379.

[40] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer–Verlag, Berlin–New York, 1976.

[41] W. M. Schmidt, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.

[42] J. H. Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc. **63** (1977), 208–212.

[43] R. P. Stauduhar, *The Determination of Galois Groups*, Math. Comp. **27** (1973), 981–996.

[44] K. Uchida, *Galois group of an equation $X^n - aX + b = 0$*, Tohoku Math. J. **22** (1970), 670–678.

[45] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt*, Monatsh. Math. **43** (1936), 137–147.

[46] Wolfram Research, Inc., *Mathematica*, Version 12.3, Champaign, IL, 2021.

[47] S. Wong, *Densities of quartic fields with even Galois groups*, Proc. Amer. Math. Soc. **133** (2005), 2873–2881.

[48] S. Xiao, *On monic abelian cubics*, Compos. Math., **158** (2022), 550–567.

[49] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1010.6465.

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, United Kingdom

Email address: Sam.Chow@warwick.ac.uk

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, EGHAM TW20 0EX, UNITED KINGDOM

Email address: Rainer.Dietmann@rhul.ac.uk