The number of A_5-quintic extensions of bounded discriminant*

Manjul Bhargava, Alina Carmen Cojocaru, and Frank Thorne

December 27, 2014

Abstract

We prove that the number of quintic number fields having associated Galois group A_5 and absolute discriminant less than X is $\mathrm{O}(X^{1-\delta})$ for $\delta = \frac{1}{40}$.

1 Introduction

A central problem in arithmetic statistics is that of understanding the asymptotic behaviour of the function counting number fields with a given Galois group and a bounded discriminant. Explicitly, for a fixed positive integer n and a fixed permutation group $G \leq S_n$, let $N_n(X, G)$ denote the number of isomorphism classes of number fields K, of degree n and absolute discriminant at most X, such that the Galois closure $\hat{K}$ of K over $\mathbb{Q}$ has Galois group isomorphic to G (here, $\mathrm{Gal}(\hat{K}/\mathbb{Q})$ is viewed as a permutation group on the embeddings of K into $\overline{\mathbb{Q}}$); the aim is to understand the behaviour of $N_n(X, G)$ as $X \to \infty$.

Due to its being the smallest noncyclic finite simple group and the largest finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$, the alternating group $G = A_5$ on five letters, also called the icosahedral group, plays a rather special role. For example, via the work of Deligne and Serre, A_5-quintic fields are naturally associated to certain weight one holomorphic cuspidal newforms, referred to as "of icosahedral type". Information on $N_5(X, A_5)$ thus gives information about the existence and the number of weight one icosahedral cuspforms.

In [Bh2, Thm. 1, p. 1559] it was shown that the total number of quintic number fields having absolute discriminant at most X is asymptotically equal to cX, where $c = c(S_5)$ is given by

$$c(S_5) := \frac{13}{120} \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^4} - \frac{1}{p^5}\right) > 0.$$

Furthermore, in [Bh2, Thm. 4, p. 1561] it was shown that 100% of these quintic fields have associated Galois group S_5, i.e. that

$$N_5(X, S_5) \sim c(S_5)\, X. \tag{1}$$

Consequently,

$$N_5(X, A_5) = \mathrm{o}(X).$$

In applications it becomes important to understand the growth of $N_5(X, A_5)$ much better and it is desirable to at least have a power-saving estimate in X. The purpose of this article is precisely to prove such an estimate:

*2000 AMS Subject Classification: 11R21, 11R45

Theorem 1 *As $X \to \infty$, we have $N_5(X, A_5) = \mathrm{O}\left(X^{1-\delta}\right)$ for any $\delta < \frac{1}{40}$.*

We expect that

$$N_5(X, A_5) \sim c(A_5) X^{\frac{1}{2}} \log X \tag{2}$$

for some constant $c(A_5) > 0$; see, e.g., [Ma, p. 134] for heuristics towards this conjecture, and the rest of [Ma] and its references for general conjectures of a similar type.

To illustrate the mildly unusual nature of the problem of estimating $N_5(X, A_5)$, we give not one, but three (four?) approaches leading to three values of δ in Theorem 1. Each approach uses the results of [Bh2] in combination with a sieve: Selberg's sieve, Turán's sieve, Heath-Brown's square sieve, and Bhargava's recent quantitative version of Ekedahl's geometric sieve. It does not seem that any of our current methods is capable of proving (2), but in each section we discuss the limitations and possibilities inherent in each approach.

It seems that $\delta = \frac{1}{40}$ is a natural bottleneck, as all of our proofs use Bhargava's parametrization of quintic rings by lattice points in a 40-dimensional vector space and error terms of order $X^{\frac{39}{40}}$ naturally appear in various counts for these lattice points. This does not rule out the possibility of further improving the necessary error terms, but, for the moment, it appears rather difficult.

Rohrlich [Ro] has used Theorem 1 to prove that self-dual Artin representations of dimension two have density zero among all two-dimensional Artin representations. We expect other applications to emerge.

2 Parametrization of quintic rings and fields

We briefly recall the main results of [Bh1] and [Bh2] needed to prove Theorem 1. For any commutative, unitary ring T, let V_T denote the space $T^4 \otimes \wedge^2 T^5$ of quadruples $v = (A, B, C, D)^t$ of 5×5 skew-symmetric matrices with entries in T and let $a_{12} = a_{12}(v)$ denote the $(1, 2)$ entry of A. The group $G_T := \mathrm{GL}_4(T) \times \mathrm{SL}_5(T)$ acts on V_T via

$$(\gamma_4, \gamma_5) \cdot (A, B, C, D)^t := \gamma_4 \left(\gamma_5 A \gamma_5^t, \gamma_5 B \gamma_5^t, \gamma_5 C \gamma_5^t, \gamma_5 D \gamma_5^t\right)^t.$$

We shall abuse notation and denote by $v \in V_T$ the orbit of v under the action of G_T.

When $T = \mathbb{Z}$, the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ gives rise to a natural invariant polynomial in 40 variables and of degree 40, called the *discriminant* and denoted Disc, which generates the whole ring of polynomial invariants.[1]

For T a field, the orbits of G_T on V_T were first classified by Wright and Yukie [WrYu] and were shown to be in a natural correspondence with étale degree 5 extensions of T. For $T = \mathbb{Z}$, the orbits of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ with nonzero discriminant were classified by Bhargava [Bh1] in terms of quintic rings and their sextic resolvent rings,[2] as follows.

Theorem 2 *(Bhargava [Bh1])*
The $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$ with nonzero discriminant are in canonical bijection with the isomorphism classes of pairs (R, S), where R is a quintic ring and S is a sextic resolvent ring of R. In this

[1] Is $\mathbb{Z}$ the general T here?
[2] We actually also need this for $T = \mathbb{Z}_p$.

bijection, for an orbit $v \in V_{\mathbb{Z}}$ and its associated pair $(R(v), S(v))$, we have

$$\operatorname{Disc} v = \operatorname{Disc} R(v) = \frac{1}{16} \left(\operatorname{Disc} S(v)\right)^{\frac{1}{3}}.$$

Furthermore, every isomorphism class of a quintic ring R occurs in this bijection, and every isomorphism class of a maximal quintic ring occurs exactly once.

Here, a *quintic ring* R is a commutative, unitary ring isomorphic to $\mathbb{Z}^5$ as a $\mathbb{Z}$-module. A *sextic resolvent ring* S of a quintic ring R is a commutative, unitary ring isomorphic to $\mathbb{Z}^6$ as a $\mathbb{Z}$-module, equipped with a *resolvent mapping* $R \longrightarrow \wedge^2 S$ as defined in [Bh1, §5]. The *discriminant* $\operatorname{Disc} R$ of a ring R is defined as usual by $\det(\operatorname{Tr}(\alpha_i \alpha_j))$ for a $\mathbb{Z}$-basis (α_i) of R, where $\operatorname{Tr}(\alpha)$ is the trace of the endomorphism on R defined by multiplication by α. For complete definitions and details, see the original source, [Bh1].

Define

$$\begin{aligned} V_{\mathbb{Z}}^{\mathrm{ndeg}} &:= \{v \in V_{\mathbb{Z}} : R(v) \text{ is an order in an } S_5\text{-field}\}, \\ V_{\mathbb{Z}}^{\mathrm{deg}} &:= V_{\mathbb{Z}} \backslash V_{\mathbb{Z}}^{\mathrm{ndeg}}. \end{aligned}$$

The action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$ has three open orbits, denoted

$$V_{\mathbb{R}}^{(0)},\ V_{\mathbb{R}}^{(1)},\ V_{\mathbb{R}}^{(2)},$$

consisting of $v \in V_{\mathbb{R}}$ with nonzero discriminant[3] and having 5, 3, respectively 1 real zeroes in $\mathbb{P}^3$. For each $i = 0, 1, 2$, define

$$V_{\mathbb{Z}}^{(i)} := V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$$

and denote by n_i the cardinality of the stabilizer in $G_{\mathbb{R}}$ of any element in $V_{\mathbb{R}}^{(i)}$. As shown in [Bh2, Prop. 15, pp. 1583-1584], we have

$$n_0 = 120,\ n_1 = 12,\ n_2 = 8.$$

Let $\mathcal{F}$ be a fundamental domain for the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$. For each $i = 0, 1, 2$, let $S_i \subseteq V_{\mathbb{Z}}^{(i)}$ be a $G_{\mathbb{Z}}$-invariant set. Define $S_i^{\mathrm{ndeg}} := S_i \cap V_{\mathbb{Z}}^{\mathrm{ndeg}}$, and for $X > 0$ define

$$N(S_i, X) := \left\{ v \in S_i^{\mathrm{ndeg}} : v \text{ irreducible } G_{\mathbb{Z}}\text{-orbit}, |\operatorname{Disc} v| \leq X \right\}.$$

Here, an orbit is called *irreducible* if its associated quintic ring $R(v)$ via Theorem 2 is an integral domain.

Proposition 3 *(Bhargava [Bh2, (9)-(10), pp. 1568-1569])*
Let

$$H = H(J) := \{w \in V_{\mathbb{R}} : ||w|| \leq J, |\operatorname{Disc} w| \geq 1\},$$

[3] we do need discriminant for T a field

where $||\cdot||$ denotes the Euclidean norm on $V_{\mathbb{R}}$, fixed under the action of the special orthogonal transformations in $G_{\mathbb{R}}$, and J is sufficiently large so that H is nonempty and of nonzero volume. Let $i = 0, 1, 2$ and $X > 0$. Then there exists a constant C_i such that

$$N(S_i, X) = \frac{\displaystyle\int_{v \in H \cap V_{\mathbb{R}}^{(i)}} \#\left\{ s \in \mathcal{F}v \cap S_i^{ndeg} : |\operatorname{Disc} s| \le X \right\} \frac{dv}{|\operatorname{Disc} v|}}{n_i \displaystyle\int_{v \in H \cap V_{\mathbb{R}}^{(i)}} \frac{dv}{|\operatorname{Disc} v|}}$$

$$= C_i \int_{g \in \mathcal{F}} \#\left\{ s \in gH \cap S_i^{ndeg} : |\operatorname{Disc} s| \le X \right\} dg,$$

where dg is a left-invariant Haar measure on $G_{\mathbb{R}}$.

Now choose $\mathcal{F}$ as in [Bh2, §2.1, p. 1567], i.e. such that $\mathcal{F}$ is contained in a standard Siegel set, and, using Proposition 3, extend the definition of $N(S_i, X)$ to also include sets S_i which are not $G_{\mathbb{Z}}$-invariants. Furthermore, define

$$N^*(S_i, X) := C_i \int_{g \in \mathcal{F}} \#\left\{ s \in gH \cap S_i : |\operatorname{Disc} s| \le X \right\} d\, g. \tag{3}$$

Proposition 4 *(Bhargava [Bh2, Lem. 11, p. 1571])*
Let $i = 0, 1, 2$ and $X > 0$. Then

$$N\left(\left\{ v \in V_{\mathbb{Z}}^{(i)} : a_{12} = 0 \right\}, X \right) \ll X^{\frac{39}{40}}.$$

Proposition 5 *(Bhargava [Bh2, pp. 1582-1585])*
Let $i = 0, 1, 2$ and $X > 0$. Then

$$N^*\left(\left\{ v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0 \right\}, X \right) = c_i X + \mathrm{O}\left(X^{\frac{39}{40}} \right),$$

where

$$c_i := \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{2 n_i}.$$

To use sieve methods, we will need similar results with $V_{\mathbb{Z}}^{(i)}$ replaced by a subset defined by (finitely many) congruence conditions. They are described in what follows and summarize [Bh1, §12].

For a prime p and $v \in V_{\mathbb{Z}}$ (or $V_{\mathbb{Z}_p}$, or $V_{\mathbb{F}_p}$), we have an associated quintic $\mathbb{F}_p$-algebra[4]

$$R_{\mathbb{F}_p}(v) := R(v)/(p).$$

The *splitting symbol* (v, p) is defined by

$$(v, p) := \left(f_1^{e_1} f_2^{e_2} \ldots \right),$$

where

$$R(v)/(p) \simeq \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \ldots$$

There are 17 possible values for the symbol (v, p):

[4] What is $R(v)$ if $v \notin V_{\mathbb{Z}}$?

$$(11111),\ (1112),\ (122),\ (113),\ (23),\ (14),\ (5),\ (1^2\,111),\ (1^2\,12),\ (1^2\,3),\ (1^2\,1^2\,1),\ (2^2\,1),\ (1^3\,11),$$
$$(1^3\,2),\ (1^3\,1^2),\ (1^4\,1),\ (1^5).$$

Among these 17 values, we distinguish the following:

$$\mathcal{S}_{\max} := \{(11111), (1112), (113)(122), (23), (14), (5)\}\,; \tag{4}$$

$$\mathcal{S}_{\text{square}} := \{(11111), (113), (122), (5)\}\,; \tag{5}$$

$$\mathcal{S}_{\text{nonsquare}} := \{(1112), (23), (14)\}\,. \tag{6}$$

For $v, v' \in V_{\mathbb{Z}}$ (respectively in $V_{\mathbb{Z}_p}$ or $V_{\mathbb{F}_p}$) which are $G_{\mathbb{Z}}$-equivalent (respectively $G_{\mathbb{Z}_p}$ or $G_{\mathbb{F}_p}$-equivalent), we have $(v,p) = (v',p)$. Thus for any of the 17 possible symbols σ,

$$T_p(\sigma) := \{v \in V_{\mathbb{Z}} \text{ (respectively } \ V_{\mathbb{Z}_p} \text{ or } V_{\mathbb{F}_p}) : (v,p) = \sigma\}$$

is well-defined. With this notation, we observe that

$$\operatorname{Disc} v \not\equiv 0 (\operatorname{mod} p) \Leftrightarrow (v,p) \in \bigcup_{\sigma \in \mathcal{S}_{\max}} T_p(\sigma); \tag{7}$$

$$\operatorname{Disc} v (\operatorname{mod} p) \text{ is a nonzero square in } \mathbb{F}_p \Leftrightarrow (v,p) \in \bigcup_{\sigma \in \mathcal{S}_{\text{square}}} T_p(\sigma); \tag{8}$$

$$\operatorname{Disc} v (\operatorname{mod} p) \text{ is a nonsquare in } \mathbb{F}_p \Leftrightarrow (v,p) \in \bigcup_{\sigma \in \mathcal{S}_{\text{nonsquare}}} T_p(\sigma). \tag{9}$$

Similarly to the definition of the symbol (v,p), we can define a symbol (R,p) for a maximal quintic ring R with $\operatorname{Disc} R \neq 0$; see [Bh1, p. 91] for details. Then, on one hand, if $v \in V_{\mathbb{Z}}$ (respectively $V_{\mathbb{Z}_p}$ or $V_{\mathbb{F}_p}$) corresponds, under Theorem 2, to a maximal quintic algebra $R(v)$ over $\mathbb{Z}$ (respectively over $\mathbb{Z}_p$ or $\mathbb{F}_p$) and if $\operatorname{Disc} v \not\equiv 0 (\operatorname{mod} p)$, then $(v,p) = (R(v),p)$; on the other hand, if $v \in \bigcup_{\sigma \in \mathcal{S}_{\max}} T_p(\sigma)$, then $R(v)$ is maximal.

Denoting by $\mu_p(\cdot)$ the p-adic density of sets defined by congruence conditions in $V_{\mathbb{Z}}$, normalized such that $\mu_p(V_{\mathbb{Z}_p}) = 1$, we have the following exact formulae $\mu_p(T_p(\sigma))$ with $\sigma \in \mathcal{S}_{\max}$.

Proposition 6 *(Bhargava [Bh1, Lem. 20 p. 91])*

$$\begin{aligned} \mu_p(T_p(11111)) &= \frac{1}{120} \cdot \frac{(p-1)^8\, p^{16}\, (p+1)^4\, (p^2+1)^2\, (p^2+p+1)^2\, (p^4+p^3+p^2+p+1)}{p^{40}} \\ &= \frac{1}{120} + \mathrm{O}\left(\frac{1}{p}\right); \end{aligned}$$

$$\begin{aligned}
\mu_p(T_p(1112)) &= \frac{1}{12}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{12}+\mathrm{O}\left(\frac{1}{p}\right);\\
\mu_p(T_p(122)) &= \frac{1}{8}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{8}+\mathrm{O}\left(\frac{1}{p}\right);\\
\mu_p(T_p(113)) &= \frac{1}{6}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{6}+\mathrm{O}\left(\frac{1}{p}\right);\\
\mu_p(T_p(23)) &= \frac{1}{6}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{6}+\mathrm{O}\left(\frac{1}{p}\right);\\
\mu_p(T_p(14)) &= \frac{1}{4}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{4}+\mathrm{O}\left(\frac{1}{p}\right);\\
\mu_p(T_p(5)) &= \frac{1}{5}\cdot\frac{(p-1)^8\,p^{16}\,(p+1)^4\,(p^2+1)^2\,(p^2+p+1)^2\,(p^4+p^3+p^2+p+1)}{p^{40}}\\
&= \frac{1}{5}+\mathrm{O}\left(\frac{1}{p}\right).
\end{aligned}$$

The proof of this proposition uses the following results, also needed in the coming sections.

Proposition 7 *(Bhargava [Bh1, p. 92])*
For any $\sigma \in \mathcal{S}_{max}$, there exists a unique maximal quintic algebra $R_p(\sigma)$ over $\mathbb{Z}_p$ such that

$$(R_p(\sigma), p) = \sigma.$$

Furthermore, for $v \in V_{\mathbb{Z}_p}$ corresponding to $R_p(\sigma)$ under Theorem 2, we have

$$\#\,\mathrm{Stab}_{G_{\mathbb{Z}_p}}(v) = \#\,\mathrm{Aut}_{\mathbb{Z}_p}\,R_p(\sigma),$$

which gives

$$\mu_p(T_p(\sigma)) = \frac{\#G_{\mathbb{F}_p}}{p^{40}\,\#\,\mathrm{Aut}_{\mathbb{Z}_p}\,R_p(\sigma)}.$$

Proposition 8 *(Bhargava [Bh1, p. 92])*

$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(11111) = \frac{1}{120},$$
$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(1112) = \frac{1}{12},$$
$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(122) = \frac{1}{8},$$
$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(113) = \frac{1}{6},$$
$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(23) = \frac{1}{4},$$
$$\#\operatorname{Aut}_{\mathbb{Z}_p} R_p(5) = \frac{1}{5}.$$

Proposition 9 *(Bhargava [Bh1, p. 92])*

$$\#G_{\mathbb{F}_p} = (p-1)^8\, p^{16}\, (p+1)^4\, (p^2+1)^2\, (p^2+p+1)^2\, (p^4+p^3+p^2+p+1) = p^{40} + \mathrm{O}\left(p^{39}\right).$$

Proposition 10 *(Bhargava [Bh2, (26)-(27), pp. 1585-1586])*
Let p be a prime and $\sigma \in \mathcal{S}_{max}$. Let $v_p \in V_{\mathbb{Z}_p}$ be the unique orbit associated to σ under Theorem 2 and Proposition 9. Then, provided $p < X^{\frac{1}{40}}$, we have that, for any $i = 0, 1, 2$,

$$N^*\left(\left\{v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0, (v,p) = (v_p,p) \in T_p(\sigma)\right\}, X\right) = c_i\, \mu_p(T_p(\sigma))\, X + \mathrm{O}\left(p\, \mu_p(T_p(\sigma)) X^{\frac{39}{40}}\right).$$

3 Proof via the Selberg sieve

As noted in §1, the asymptotic formula $N_5(X, S_5) \sim c(S_5)\, X$ proven in [Bh2] immediately implies that $N_5(X, A_5) = \mathrm{o}(X)$. To improve upon this estimate we need effective versions of the asymptotic for $N_5(X, S_5)$, in particular O-estimates for the error terms coming from the contributions of A_5-fields. The basic idea to be explored in this section is that quintic extensions K with splitting types modulo a prime p forbidden by the condition $\operatorname{Gal}(\hat{K}/\mathbb{Q}) \simeq A_5$ have density equal to a constant in $(0, 1)$; then a natural tool to use for estimating $N_5(X, A_5)$ is a "small sieve".

In a recent paper [ShTs], Shankar and Tsimerman used this idea and the Selberg sieve to obtain a power-saving error term in the asymptotic formula for $N_5(X, S_5)$:

$$N_5(X, S_5) = c(S_5)\, X + \mathrm{O}_\varepsilon\left(X^{\frac{399}{400}+\varepsilon}\right), \quad \forall \varepsilon > 0. \tag{10}$$

Their proof is quite simple and flexible, and can be used to further deduce that

$$N_5(X, A_5) \ll_\varepsilon X^{\frac{199}{200}+\varepsilon} \quad \forall \varepsilon > 0. \tag{11}$$

In what follows, we present a proof of (11).

By Theorem 2,

$$\begin{aligned} N_5(X, A_5) &= \#\left\{K \supseteq \mathbb{Q} : |K:\mathbb{Q}| = 5, |\operatorname{Disc}(K/\mathbb{Q})| \leq X, \operatorname{Gal}(\hat{K}/\mathbb{Q}) \simeq A_5\right\} \\ &= \#\left\{v \in V_{\mathbb{Z}} : R(v) \text{ maximal}, |\operatorname{Disc} v| = |\operatorname{Disc} R(v)| \leq X, G(v) \simeq A_5\right\}, \end{aligned}$$

where $G(v)$ denotes the Galois group over $\mathbb{Q}$ of the Galois closure of the fraction field of $R(v)$ (which, being maximal, is also a domain). We split the above according to whether $a_{12} = a_{12}(v)$ is zero or not and use Proposition 4. Then

$$N_5(X, A_5) \ll X^{\frac{39}{40}} + \#\left\{v \in V_{\mathbb{Z}} : R(v) \text{ maximal}, |\operatorname{Disc} v| \leq X, G(v) \simeq A_5, a_{12} \neq 0\right\}. \tag{12}$$

Since $R(v)$ maximal implies v irreducible and since $G(v) \simeq A_5$ implies $(v,p) \notin T_p(1112)$ for any prime p, we obtain further that $N_5(X, A_5)$ is

$$\ll X^{\frac{39}{40}} + \sum_{i=0,1,2} \#\left\{v \in V_{\mathbb{Z}}^{(i)} : v \text{ irreducible}, |\operatorname{Disc} v| \leq X, a_{12} \neq 0, (v,p) \notin T_p(1112)\ \forall p\right\}. \tag{13}$$

To estimate the right-hand side term, we apply the Selberg sieve, a version of which we now recall.

Proposition 11 *(Selberg [Se]; version as in [CoMu, §7.2 pp. 118–124])*
Let $\mathcal{A}$ be a finite multiset and let $\mathcal{P}$ be a set of rational primes. For any $p \in \mathcal{P}$, let $\mathcal{A}_p \subseteq \mathcal{A}$. Define $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers composed of primes of $\mathcal{P}$, define $\mathcal{A}_d := \bigcap_{p|d} \mathcal{A}_p$. Let $z > 0$ and define $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} p$. Consider the sieve problem given by

$$S(\mathcal{A}, \mathcal{P}, z) := \#\left(\mathcal{A} \setminus \bigcup_{p|P(z)} \mathcal{A}_p\right).$$

Assume that there exist $X > 0$ and a multiplicative function $g : \mathrm{N}\setminus\{0\} \longrightarrow (0, \infty)$ such that

1. *$g(p) < 1 \quad \forall p \in \mathcal{P}$;*
2. *for any squarefree integer d composed of primes of $\mathcal{P}$ there exists $R_d \in \mathbb{R}$ such that*

$$\#\mathcal{A}_d = g(d)X + R_d.$$

Then

$$S(\mathcal{A}, \mathcal{P}, z) \ll \frac{X}{V(z)} + \sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 | P(z)}} |R_{[d_1, d_2]}|,$$

where

$$V(z) := \sum_{\substack{d \leq z \\ d | P(z)}} \prod_{p|d} \frac{g(p)}{1 - g(p)}.$$

To apply the Selberg sieve, we fix $i = 0, 1, 2$ and define

$$\mathcal{A}^{(i)}$$

as the multiset counted by $N^*\left(\left\{v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0\right\}, X\right)$. We let

$$\mathcal{P} := \{p \text{ prime}\}$$

and, for each $p \in \mathcal{P}$, define

$$\mathcal{A}_p := \left\{v \in \mathcal{A}^{(i)} : (v, p) \in T_p(1112)\right\}.$$

Furthermore, we let

$$0 < z = z(X) < X^{\frac{1}{40}}$$

be a parameter of x, which shall be chosen optimally later.

By Propositions 6 and 10, for any squarefree $d|P(z)$ and any $\varepsilon > 0$ we have[5]

$$\begin{aligned} \#\mathcal{A}_d &= c_i \left(\prod_{p|d} \mu_p(T_p(1112))\right) X + \mathrm{O}\left(d\left(\prod_{p|d} \mu_p(T_p(1112))\right) X^{\frac{39}{40}}\right) \\ &= c_i \left(\prod_{p|d} \mu_p(T_p(1112))\right) X + \mathrm{O}_\varepsilon\left(d^{1+\varepsilon} X^{\frac{39}{40}}\right); \end{aligned} \tag{14}$$

$$\begin{aligned} V(z) &= c_i \sum_{\substack{d \leq z \\ d \text{ squarefree}}} \prod_{p|d} \frac{\mu_p(T_p(1112))}{1 - \mu_p(1112)} \gg \prod_{p \leq \log z} \left(1 + \frac{\mu_p(T_p(1112))}{1 - \mu_p(T_p(1112))}\right) \\ &\gg \prod_{p \leq \log z} \left(\frac{11}{12} + \frac{1}{p}\right)^{-1} \gg_\varepsilon z^{1-\varepsilon}. \end{aligned} \tag{15}$$

Then, by Propositions 5 and 11[6],

$$\begin{aligned} & \#\left\{v \in V_{\mathbb{Z}}^{(i)} : v \text{ irreducible}, |\operatorname{Disc} v| \leq X, a_{12} \neq 0, (v, p) \notin T_p(1112)\ \forall p\right\} \\ \leq\ & N^*\left(\left\{v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0\right\}, z\right) + \#S\left(\mathcal{A}^{(i)}, \mathcal{P}, z\right) \\ \ll\ & z + \frac{X}{V(z)} + \sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 \text{ squarefree}}} |R_{[d_1, d_2]}| \\ \ll_\varepsilon\ & z + \frac{X}{z^{1-\varepsilon}} + z^{4+\varepsilon} X^{\frac{39}{40}}. \end{aligned}$$

Choosing

$$z \asymp X^{\frac{1}{200}}$$

and recalling (13), we deduce (11).

[5]These estimates are CRUCIAL; CHECK!

[6]We are passing to an AVERAGE; CHECK this statement!

4 Proof via the Turán sieve

In this section we shall explore the same main ideas as in Section 3 and obtain the improved bound

$$N_5(X, A_5) \ll X^{\frac{119}{120}} \log X. \tag{16}$$

Instead of the Selberg sieve, we now use a much simpler sieve emerging from Turán's normal order method and which we recall below.

Proposition 12 *(Turán [Tu]; version as in [CoMu, Thm. 4.1.1 p. 48])*
Let $\mathcal{A}$ be a finite multiset and let $\mathcal{P}$ be a set of rational primes. For any $p \in \mathcal{P}$, let $\mathcal{A}_p \subseteq \mathcal{A}$. Define $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers composed of primes of $\mathcal{P}$, define $\mathcal{A}_d := \bigcap_{p|d} \mathcal{A}_p$. Let $z > 0$ and define $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} p$. Consider the sieve problem given by

$$S(\mathcal{A}, \mathcal{P}, z) := \# \left(\mathcal{A} \backslash \bigcup_{p|P(z)} \mathcal{A}_p \right).$$

Assume that there exist $X > 0$ and a (not necessarily multiplicative) function $g : \mathrm{N}\backslash\{0\} \longrightarrow (0, \infty)$ such that

1. *$g(p) < 1 \quad \forall p \in \mathcal{P}$;*
2. *for any $p \in \mathcal{P}$ and any distinct $p_1, p_2 \in \mathcal{P}$, there exist $R_p, R_{p_1p_2} \in \mathbb{R}$ such that*

$$\#\mathcal{A}_p = g(p)X + R_p,$$

$$\#\mathcal{A}_{p_1p_2} = g(p_1)g(p_2)X + R_{p_1p_2}.$$

Then

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{U(z)} + \frac{2}{U(z)} \sum_{p|P(z)} |R_p| + \frac{1}{U(z)^2} \sum_{\substack{p_1, p_2 | P(z) \\ p_1 \neq p_2}} |R_{p_1p_2}|,$$

where

$$U(z) := \sum_{p|P(z)} g(p).$$

Note that, unlike the Selberg sieve, the Turán sieve only requires the first two steps in the inclusion-exclusion formula.

With notation $\mathcal{A}^{(i)}$, $\mathcal{P}$, $\mathcal{A}_p$ as in Section 3, by using (14), Proposition 6 and Proposition 12 we deduce that

$$S(\mathcal{A}^{(i)}, \mathcal{P}, z) \ll \frac{X \log z}{z} + zX^{\frac{39}{40}} + z^2 X^{\frac{39}{40}}.$$

Choosing

$$z \asymp \frac{X^{\frac{1}{120}}}{(\log X)^{\frac{1}{3}}},$$

the above leads to the estimate

$$S(\mathcal{A}^{(i)}, \mathcal{P}, z) \ll X^{\frac{119}{120}} \log X.$$

Recalling (13) and Proposition 5, we now deduce that

$$\begin{aligned} N_5(X, A_5) &\leq X^{\frac{39}{40}} + \sum_{i=0,1,2} \left(N^* \left(\left\{ v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0 \right\}, z \right) + \#S\left(\mathcal{A}^{(i)}, \mathcal{P}, z \right) \right) \\ &\ll X^{\frac{39}{40}} + z + X^{\frac{119}{120}} \log X \\ &\ll X^{\frac{119}{120}} \log X. \end{aligned}$$

This completes the proof of (16).

5 Proof via the square sieve

In this section we shall explore that A_5-extensions have square discriminants and obtain a bound of the same order of magnitude as (16):

$$N_5(X, A_5) \ll X^{\frac{199}{200}} (\log X)^{\frac{2}{3}} \tag{17}$$

A natural tool for detecting squares is the classical Legendre symbol. In appropriate settings, this tool can be used successfully towards estimating, from above, the number of squares in a finite sequence. Indeed, such a procedure is illustrated by what is now referred to as the *square sieve*, a version of which we now recall.

Proposition 13 *(Heath-Brown [HB]; version as in [CoMu, p. 21])*
Let $\mathcal{A}$ be a finite multiset of positive integers and let $\mathcal{P}$ be a finite set of odd rational primes. Then

$$\#\{\alpha \in \mathcal{A} : \alpha \text{ is a square}\} \leq \frac{\#\mathcal{A}}{\#\mathcal{P}} + \frac{2}{\#\mathcal{P}} \sum_{\alpha \in \mathcal{A}} \nu_{\mathcal{P}}(\alpha) + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha \in \mathcal{A}} \nu_{\mathcal{P}}(\alpha)^2 + \max_{\substack{p_1, p_2 \in \mathcal{P} \\ p_1 \neq p_2}} \left| \sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{p_1} \right) \left(\frac{\alpha}{p_2} \right) \right|,$$

where $\nu_{\mathcal{P}}(\alpha)$ is the number of distinct prime factors of α in $\mathcal{P}$.

To apply the square sieve, we fix $i = 0, 1, 2$ and define

$$\mathcal{A}^{(i)} := \left\{ |\operatorname{Disc} v| : v \text{ counted in } N^* \left(\left\{ v \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0 \right\}, X \right) \right\}.$$

Let

$$0 < z = z(X) < X^{\frac{1}{80}}$$

be a parameter of X, which shall be chosen optimally later, and define

$$\mathcal{P} := \{ z < p < 2z : p \text{ an odd prime} \}.$$

By Proposition 5, Chebyshev's theorem and elementary bounds,

$$\#\mathcal{A}^{(i)} = c_i X + \mathrm{O}\left(X^{\frac{39}{40}} \right); \tag{18}$$

$$\frac{\#\mathcal{A}^{(i)}}{\#\mathcal{P}} \ll \frac{X\log X}{z}; \tag{19}$$

$$\frac{2}{\#\mathcal{P}}\sum_{\alpha\in\mathcal{A}}\nu_{\mathcal{P}}(\alpha) \ll \frac{X\log X}{z}; \tag{20}$$

$$\frac{1}{(\#\mathcal{P})^2}\sum_{\alpha\in\mathcal{A}}\nu_{\mathcal{P}}(\alpha)^2 \ll \frac{X(\log X)^2}{z^2}. \tag{21}$$

It remains to estimate the character sum. For this, we will prove the more general estimate that, for any odd squarefree integer m such that $m < X^{\frac{1}{40}}$, we have

$$\left|\sum_{\alpha\in\mathcal{A}^{(i)}}\left(\frac{\alpha}{m}\right)\right| \ll mX^{\frac{39}{40}}. \tag{22}$$

Here, $\left(\frac{\cdot}{m}\right)$ denotes the Jacobi symbol.

We define

$$U_{m,+} := \left\{\alpha\in\mathcal{A}^{(i)} : \left(\frac{\alpha}{m}\right) = 1\right\};$$
$$U_{m,-} := \left\{\alpha\in\mathcal{A}^{(i)} : \left(\frac{\alpha}{m}\right) = -1\right\};$$
$$U_{m,0} := \left\{\alpha\in\mathcal{A}^{(i)} : \left(\frac{\alpha}{m}\right) = 0\right\}.$$

Then

$$\sum_{\alpha\in\mathcal{A}^{(i)}}\left(\frac{\alpha}{m}\right) = N^*\left(\{v\in U_{m,+} : a_{12}\neq 0\}, X\right) - N^*\left(\{v\in U_{m,-} : a_{12}\neq 0\}, X\right). \tag{23}$$

We now consider the case when $m = p$ is an odd prime. By (5) - (6) and Propositions 6 - 9, we deduce the following:

$$\mu_p(U_{p,+}) = \frac{1}{p^{40}}\sum_{\sigma\in\mathcal{S}_{\text{square}}}\frac{\#G_{\mathbb{F}_p}}{\#\operatorname{Aut}_{\mathbb{Z}_p}R_p(\sigma)} = \frac{\#G_{\mathbb{F}_p}}{p^{40}}\left(\frac{1}{120}+\frac{1}{6}+\frac{1}{8}+\frac{1}{5}\right) = \frac{\#G_{\mathbb{F}_p}}{2\,p^{40}};$$

$$\mu_p(U_{p,-}) = \frac{1}{p^{40}}\sum_{\sigma\in\mathcal{S}_{\text{nonsquare}}}\frac{\#G_{\mathbb{F}_p}}{\#\operatorname{Aut}_{\mathbb{Z}_p}R_p(\sigma)} = \frac{\#G_{\mathbb{F}_p}}{p^{40}}\left(\frac{1}{12}+\frac{1}{6}+\frac{1}{4}\right) = \frac{\#G_{\mathbb{F}_p}}{2\,p^{40}};$$

$$N^*\left(\{v\in U_{m,+} : a_{12}\neq 0\}, X\right) = c_i\,\frac{\#G_{\mathbb{F}_p}}{2\,p^{40}}\,X + \mathrm{O}\left(pX^{\frac{39}{40}}\right);$$

$$N^*\left(\{v\in U_{m,-} : a_{12}\neq 0\}, X\right) = c_i\,\frac{\#G_{\mathbb{F}_p}}{2\,p^{40}}\,X + \mathrm{O}\left(pX^{\frac{39}{40}}\right).$$

Then, by (23), (22) is proven for $m = p$.

Next we consider the case when $m = p_1\dots p_r$ is an odd squarefree integer. We denote by $p_i|m$ any collection of prime factors of m such that an even number of the associated sign in $U_{p_i},\pm$ is

negative. There are 2^{r-1} such choices. Then, by the above calculations and the Chinese Remainder Theorem,

$$\begin{aligned} N^*\left(\{v \in U_{m,+} : a_{12} \neq 0\}, X\right) &= c_i \left(\prod_{p_i|m} \mu_{p_i}(U_{p_i}, \pm)\right) X + \mathrm{O}\left(m \left(\prod_{p_i|m} \mu_{p_i}(U_{p_i}, \pm)\right) X^{\frac{39}{40}}\right) \\ &= c_i \, 2^{r-1} \frac{\#G_{\mathbb{Z}/m\mathbb{Z}}}{2^r m^{40}} X + \mathrm{O}\left(m X^{\frac{39}{40}}\right) \\ &= c_i \frac{\#G_{\mathbb{Z}/m\mathbb{Z}}}{2\, m^{40}} X + \mathrm{O}\left(m X^{\frac{39}{40}}\right). \end{aligned}$$

Similarly,

$$N^*\left(\{v \in U_{m,-} : a_{12} \neq 0\}, X\right) = c_i \frac{\#G_{\mathbb{Z}/m\mathbb{Z}}}{2\, m^{40}} X + \mathrm{O}\left(m X^{\frac{39}{40}}\right).$$

Then, by (23), (22) is proven for $m = p_1 \dots p_r$.

Using (19) - 22 in Proposition 13, we obtain that

$$N_5(X, A_5) \ll \frac{X \log X}{z} + z^2 X^{\frac{39}{40}}.$$

Choosing

$$z \asymp X^{\frac{1}{120}} (\log X)^{\frac{1}{3}},$$

we deduce (17).

6 Proof via the geometric sieve

Finally, we will obtain the strongest error terms using the *geometric* sieve of the first author [Bh3]. The idea to be pursued is the following: A_5-fields K with discriminant in $[X^{1/2}, X]$ have the property that, for some squarefree $q \gg X^{1/8}$ with $(q, 30) = 1$, we have $v_p(\mathrm{Disc}(K)) \in \{2, 4\}$ for each prime p dividing q. (We take q coprime to 30 so as to avoid complications due to wild ramification; also note that there are $\ll X^{1/2}$ A_5-fields K with discriminant $< X^{1/2}$.)

In most sieve applications, such K would constitute the 'tail' of elements to be sieved *out*; for example, in [Bh3] bounds for this tail yield asymptotics for fields with square-*free* discriminant. Here the 'tail' is precisely what we want to count.

We apply the geometric sieve as follows. Suppose that, as above, $x \in V_{\mathbb{Z}}$ corresponds to a maximal quintic order and satisfies $v_p(\mathrm{Disc}(x)) \geq 2$ (and in particular $v_p(\mathrm{Disc}(x)) \in \{2, 4\}$) for each prime $p \mid q$, for some squarefree $q > X^{1/8}$. Then, $\mathrm{Disc}(x')$ will be divisible by p^2 for each $x' \equiv x \pmod{p^2}$; in the language of [Bh3], the discriminant polynomial is strongly a multiple of p^2 at x. By Lemma 3.6 of [Bh3] it follows that there is a subscheme Y_2 of $\mathbb{A}^{40}_{\mathbb{Z}}$ such that $x \pmod{p} \in Y_2(\mathbb{F}_p)$ for each $p \mid q$; indeed, we may choose one of the 40 coordinates x_i arbitrarily, and then Y_2 is defined by $\mathrm{Disc} = \frac{\partial \mathrm{Disc}}{\partial x_i} = 0$.

Let B be the intersection of the set $\{x \in V_{\mathbb{R}} : 0 < |\mathrm{Disc}(x)| < 1\}$ and a fundamental domain for the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$. Then, with $r = X^{1/40}$, $rB \cap \mathbb{Z}^{40}$ corresponds precisely to the set of $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ with $0 < |\mathrm{Disc}(x)| < X$. By Theorem 3.3 of [Bh3], we have

$$\#\{a \in rB \cap \mathbb{Z}^{40} \mid a \pmod{p} \in Y(\mathbb{F}_p) \text{ for some prime } p > X^{1/8}\} = O(X^{39/40+\epsilon}); \tag{24}$$

the idea of the proof is to project onto one of the 40 coordinates x_i and prove that for each value a_i of the coordinate x_i, only finitely many $a \in rB \cap \mathbb{Z}^{40}$ counted above have x_i-coordinate equal to a_i.

Indeed, (24) is also valid for general squarefree q, as the proof of Theorem 3.3 of [Bh3] remains equally valid for squarefree q, except that we obtain an additional factor of X^ϵ in the error term at three locations:

- In the verification of (17) of [Bh3] for $k = 1$, $f_i(a)$ may have $\ll_\epsilon X^\epsilon$ squarefree divisors $>$, as opposed to simply $O(1)$ prime factors $p > r$.
- Similarly, in the verification of (19) of [Bh3], $f_k(b, a_n)$ may have $\ll_\epsilon X^\epsilon$ squarefree divisors $> r$, as opposed to $O(1)$ prime factors $p > r$.
- In the verification of (21) of [Bh3], the number of values of a_n such that $f_k(b, a_n) \equiv 0 \pmod{p}$ and $a = (b, a_n) \in rB \cap \mathbb{Z}^n$ is now $d^{\nu(q)} \cdot O(1)$, where $\nu(q)$ denotes the number of prime divisors of q. This quantity is once again $\ll_{\epsilon,d} X^\epsilon$.

We are therefore done, except for one technical point: Theorem 3.3 of [Bh3] assumes that B is compact, which in our case it is not. This is dealt with in [Bh3] (just before (27)) by removing a region of B of volume ϵ; however, this doesn't suffice for a power-saving error term. (**To do.** This can be dealt with following Remark 4.2; check and write up the details.)

Remark 14 *The proof of* (24) *illustrates that* $X^{39/40}$ *is a natural bottleneck with this method, as it is the volume of our projection. To go further, we would have to prove that for most* a_i, no $a \in rB \cap \mathbb{Z}^{40}$ *have* x_i*-coordinate equal to* a_i.

This completes the proof.

References

[Bh1] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings,* Ann. Math. **167** (2008), no. 1, 53–94.

[Bh2] M. Bhargava, *The density of discriminants of quintic rings and fields,* Ann. of Math. **72** (2010), 1559–1591.

[Bh3] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials,* preprint.

[BhShTs] M. Bhargava, A. Shankar and J. Tsimerman, *On the Davenport–Heilbronn theorems and second order terms,* Invent. Math. **193** (YEAR), 439-499.

[CoMu] A.C. Cojocaru and M.R. Murty, *An introduction to sieve methods and their applications,* London Mathematical Society Student Texts **66**, Cambridge University Press (2006).

[HB] D. R. Heath-Brown, *The square sieve and consecutive square-free numbers*, Math. Ann. **266** (1984), no. 3, 251–259.

[Ma] G. Malle, *On the distribution of Galois groups II,* Experiment. Math. **13** (2004), 129–135.

[Tu] P. Turán, ...

[Ro] D. Rohrlich, *Self-dual Artin representations,* REFERENCE.

[Se] A. Selberg, *On an elementary method in the theory of primes,* Norske Vid. Selsk. Forh., Trondhjem 19 (1947), no. 18, 64–67.

[ShTs] A. Shankar and J. Tsimerman, *Counting S_5-fields with a power saving error term,* preprint.

[WrYu] D. J. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions,* Invent. Math. **110** (1992), 283–314.