Journal of Number Theory 269 (2025) 157–202

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

# Counting wild quartics with prescribed discriminant and Galois closure group

Sebastian Monnet

*University College London, United Kingdom*

ARTICLE INFO

*Article history:*
Received 7 February 2024
Received in revised form 8 September 2024
Accepted 27 October 2024
Available online 20 November 2024
Communicated by F. Pellarin

*Keywords:*
Arithmetic statistics
Local fields
$p$-Adic fields
Serre's mass formula
Counting number fields

ABSTRACT

Given a 2-adic field $K$, we give a formula for the number of totally ramified quartic field extensions $L/K$ with a given discriminant valuation and Galois closure group. We use these formulae to prove refinements of Serre's mass formula, which will have applications to the arithmetic statistics of number fields.



## 1. Introduction

Throughout this paper, we use the term 2-*adic field* for a finite field extension of the 2-adic numbers $\mathbb{Q}_2$, and all the fields we consider will be 2-adic. Once and for all, fix a 2-adic field $K$.

Let $L/K$ be a finite field extension. The *Galois closure group* of $L/K$ is the Galois group $\mathrm{Gal}(\widetilde{L}/K)$, where $\widetilde{L}$ is the normal closure of $L$ over $K$. Write $\Sigma_m^G$ for the set of isomorphism classes of totally ramified quartic field extensions $L/K$ with $v_K(d_{L/K}) = m$,

*E-mail address:* sebastian.monnet.21@ucl.ac.uk.

https://doi.org/10.1016/j.jnt.2024.10.008

such that the Galois closure group of $L/K$ is isomorphic to $G$. We allow ourselves to drop either or both of the decorators $G$ and $m$, with the obvious meanings.

Using his eponymous lemma, Krasner [Kra66, Théorème 1] found a formula, in terms of $m$, for the size of the set $\Sigma_m$. More recently, Sinclair [Sin15] and Pauli–Sinclair [PS15] gave refinements of Krasner's formula, enumerating (among other things) the elements of $\Sigma_m$ that have a prescribed ramification polygon. In a different direction, Wei and Ji [WJ07] counted the elements of $\Sigma^{S_4}$ and $\Sigma^{A_4}$, without any conditions on discriminant valuation. In this paper, we combine the flavours of [PS15] and [WJ07] to give new refinements of Krasner's result: formulae for the sizes of the sets $\Sigma_m^G$, for all $m$ and $G$. These results in hand, we prove novel refinements of Serre's mass formula, which will have applications in the arithmetic statistics of number fields.

### *1.1. Outline and key results*

Write $e_K$ and $f_K$ for the absolute ramification index and absolute inertia degree of $K$, respectively, and let $q$ be the size $2^{f_K}$ of its residue field. In Section 2, we use a result of Serre to relate

$$\#\left(\Sigma_m^{S_4} \cup \Sigma_m^{A_4}\right)$$

to the density of the corresponding Eisenstein polynomials. We then find explicit congruence conditions for this set of Eisenstein polynomials and use them to compute the required density. Finally, we establish conditions for distinguishing between $\Sigma_m^{A_4}$ and $\Sigma_m^{S_4}$, which we use to obtain the following two results:

**Theorem 1.1.** *Suppose that $f_K$ is even. Then $\Sigma_m^{S_4}$ is empty for all $m$. Moreover, $\Sigma_m^{A_4}$ is nonempty if and only if $m$ is an even integer with $4 \leq m \leq 6e_K + 2$. In that case, we have*

$$\#\Sigma_m^{A_4} = \begin{cases} \frac{1}{3}q^{\lfloor \frac{m}{3} \rfloor - 2}(q^2 - 1) & \text{if } 3 \mid m, \\ q^{\lfloor \frac{m}{3} \rfloor - 1}(q-1) & \text{if } 3 \nmid m. \end{cases}$$

**Theorem 1.2.** *Suppose that $f_K$ is odd.*

- *The set $\Sigma_m^{S_4}$ is nonempty if and only if $m \in 2\mathbb{Z} \setminus 6\mathbb{Z}$ and $4 \leq m \leq 6e_K + 2$. In that case, we have*

$$\#\Sigma_m^{S_4} = q^{\lfloor \frac{m}{3} \rfloor - 1}(q-1).$$

- *The set $\Sigma_m^{A_4}$ is nonempty if and only if $m$ is a multiple of 6 and $6 \leq m \leq 6e_K$. In that case, we have*

$$\#\Sigma_m^{A_4} = \frac{1}{3} \cdot q^{\lfloor \frac{m}{3} \rfloor - 2}(q^2 - 1).$$

The case $V_4$ was addressed by Tunnell in [Tun78]. We repackage his result in Section 3 as the following theorem:

**Theorem 1.3.** *If $\Sigma_m^{V_4}$ is nonempty, then $m$ is an even integer with $6 \leq m \leq 6e_K + 2$. For all such $m$, we have*

$$\#\Sigma_m^{V_4} = 2(q-1)q^{\frac{m-4}{2}}\left(q^{-\lfloor \frac{m}{6} \rfloor}(1 + \mathbb{1}_{3|m} \cdot \frac{q-2}{3}) - \mathbb{1}_{m \leq 4e_K+2} \cdot q^{-\lfloor \frac{m-2}{4} \rfloor}\right).$$

The bulk of our work goes into the $C_4$ case. In [CDO05], Cohen, Diaz y Diaz, and Olivier obtain asymptotic formulae for the number of $C_4$-extensions of a number field. We adapt their methods to compute the size of $\Sigma_m^{C_4}$. Our formula depends on the discriminant valuation

$$d_{(-1)} = v_K(d_{K(\sqrt{-1})/K}),$$

which is an even integer by Lemma 4.20.

**Theorem 1.4.** *If $\Sigma_m^{C_4}$ is nonempty, then either $m = 8e_K + 3$ or $m$ is an even integer with $8 \leq m \leq 8e_K$. For even $m$ with $8 \leq m \leq 8e_K$, the number $\#\Sigma_m^{C_4}$ is the sum of the following four quantities:*

1. $\mathbb{1}_{8 \leq m \leq 5e_K-2} \cdot \mathbb{1}_{m \equiv 3 \pmod 5} \cdot 2q^{\frac{3m-14}{10}}(q-1)$.
2. $\mathbb{1}_{4e_K+4 \leq m \leq 5e_K+2} \cdot 2q^{\frac{m}{2}-e_K-2}(q-1)$.
3. $\mathbb{1}_{5e_K+3 \leq m \leq 8e_K} \cdot \mathbb{1}_{m \equiv 2e_K \pmod 3} \cdot 2q^{\frac{m+4e_K}{6}-1}(1+\mathbb{1}_{m \leq 8e_K-3d_{(-1)}})(q-1-\mathbb{1}_{m=8e_K-3d_{(-1)}+6})$.
4. $\mathbb{1}_{10 \leq m \leq 5e_K} \cdot 2(q-1)(q^{\lfloor \frac{3m}{10} \rfloor - 1} - q^{\max\{\lceil \frac{m+2}{4} \rceil, \frac{m}{2}-e_K\}-2})$.

*We also have*

$$\#\Sigma_{8e_K+3}^{C_4} = \begin{cases} 4q^{2e_K} & \text{if } -1 \in K^{\times 2}, \\ 2q^{2e_K} & \text{if } K(\sqrt{-1})/K \text{ is quadratic and totally ramified}, \\ 0 & \text{if } K(\sqrt{-1})/K \text{ is quadratic and unramified.} \end{cases}$$

Finally, in Section 5, we compute the number of towers of two quadratic extensions $L/E/K$ with $v_K(d_{L/K}) = m$ and express this number in terms of $\#\Sigma_m^{C_4}$, $\#\Sigma_m^{V_4}$, and $\#\Sigma_m^{D_4}$. Rearranging, we obtain:

**Theorem 1.5.** *If $\Sigma_m^{D_4}$ is nonempty, then one of the following holds:*

1. *$m$ is an even integer with $6 \leq m \leq 8e_K + 2$.*
2. *$m \equiv 1 \pmod 4$ and $4e_K + 5 \leq m \leq 8e_K + 1$.*
3. *$m = 8e_K + 3$.*

*For even $m$ with $6 \leq m \leq 8e_K + 2$, we have*

$$\begin{aligned}\#\Sigma_m^{D_4} &= 2(q-1)q^{\frac{m}{2}-2} \\ &\quad \times \left(\mathbb{1}_{m \geq 4e_K+4} \cdot q^{-e_K} + \mathbb{1}_{m \leq 8e_K} \cdot \left(q^{\min\{0, e_K+1-\lceil \frac{m}{4} \rceil\}} - q^{-\min\{\lfloor \frac{m-2}{4} \rfloor, e_K\}}\right)\right) \\ &\quad - \frac{1}{2}\#\Sigma_m^{C_4} - \frac{3}{2}\#\Sigma_m^{V_4}.\end{aligned}$$

*For $m \equiv 1 \pmod 4$ with $4e_K + 5 \leq m \leq 8e_K + 1$, we have*

$$\#\Sigma_m^{D_4} = 2(q-1)q^{e_K + \frac{m-1}{4} - 1} - \frac{1}{2}\#\Sigma_m^{C_4} - \frac{3}{2}\#\Sigma_m^{V_4}.$$

*If $m = 8e_K + 3$, then*

$$\#\Sigma_m^{D_4} = 2q^{3e_K} - \frac{1}{2}\#\Sigma_{8e_K+3}^{C_4}.$$

*Theorems 1.3 and 1.4 make these expressions completely explicit.*

### *1.2. Application: refinements of Serre's mass formula*

Our main application is to prove refinements of Serre's mass formula. Define the *mass* of a set $S$ of field extensions $L/K$ to be

$$\widetilde{m}(S) = \sum_{L \in S} \frac{(\#\operatorname{Aut}(L/K))^{-1}}{q^{v_K(d_{L/K})}}.$$

This quantity was first studied by Serre, who proved his famous "mass formula" [Ser78, Theorem 2]. In [Bha07], Bhargava generalised Serre's formula to sets of étale algebras over $K$ and developed the so-called "Malle–Bhargava heuristics" which predict the asymptotic number of degree $n$ number fields with Galois closure group $S_n$, when ordered by discriminant. Essentially, Bhargava predicts that the probability of a "randomly selected" such number field having a prescribed local completion is proportional to the mass of that local completion.

Bhargava, Shankar, and Wang proved these heuristics for $n = 2, 3, 4, 5$ in [BSW15, Theorem 2], replacing degree $n$ number fields by degree $n$ extensions of an arbitrary base number field. Recently, in [Alb23], Alberts extended the Malle–Bhargava heuristics, replacing $S_n$ with more general classes of Galois closure groups. Aside from the mass's general importance in arithmetic statistics, the original motivation for our refinements comes from our earlier preprint [Mon22]; our formula for the local masses at primes $\mathfrak{p}$ lying over 2 (called $m_{\mathcal{A},\mathfrak{p}}$ in [Mon22]) is woefully inexplicit, and we intend to use the formulae in this paper to remedy that shortcoming. Similarly, upcoming work of Newton–Varma uses a modified version of Corollary 1.9, and more generally we expect

our refined mass formulae to be useful for obtaining explicit masses when counting $S_4$-quartic extensions with local conditions.

We find explicit formulae for $\widetilde{m}(\Sigma^G)$ for each $G$, which we now state. The proofs are deferred to later sections of the paper.

**Corollary 1.6.** *If $f_K$ is even, then*

$$\widetilde{m}(\Sigma^{S_4}) = 0,$$

*and*

$$\widetilde{m}(\Sigma^{A_4}) = \frac{1}{3}(q-1)\cdot\frac{q^{4e_K}-1}{q^4-1}\cdot q^{-4e_K-3}\Big(3q^3+q^2+q+3\Big).$$

**Corollary 1.7.** *Suppose that $f_K$ is odd. Then*

$$\widetilde{m}(\Sigma^{S_4}) = \frac{q^3+1}{q^3+q^2+q+1}\cdot(q^{-3}-q^{-4e_K-3}),$$

*and*

$$\widetilde{m}(\Sigma^{A_4}) = \frac{1}{3}\cdot\frac{1}{q^2+1}\cdot(q^{-2}-q^{-4e_K-2}).$$

**Corollary 1.8.** *We have*

$$\widetilde{m}(\Sigma^{V_4}) = \frac{q-1}{6}\cdot\Big(q^{-4e_K-3}\cdot\frac{q^{4e_K}-1}{q^4-1}\cdot(3q^3+q^2+q+3)-3q^{-3e_K-3}\cdot\frac{q^{3e_K}-1}{q^3-1}\cdot(q^2+1)\Big).$$

**Corollary 1.9.** *The mass $\widetilde{m}(\Sigma^{C_4})$ is the sum of the following nine quantities:*

1. $$\frac{1}{2}\cdot\frac{(q-1)(1-q^{-7\lfloor\frac{e_K}{2}\rfloor})}{q^7-1}.$$

2. $$\frac{1}{2}\cdot q^{-3e_K-3}(1-q^{-\lfloor\frac{e_K}{2}\rfloor}).$$

3. $$\mathbb{1}_{d_{(-1)}<e_K}\cdot\frac{(q-1)(q^{-5\lfloor\frac{e_K}{2}\rfloor-e_K-1}-q^{\frac{5}{2}d_{(-1)}-6e_K-1})}{q^5-1}.$$

4. $$\frac{1}{2}\cdot\mathbb{1}_{d_{(-1)}\geq 2}\cdot q^{-6e_K+\frac{5}{2}d_{(-1)}-6}(q-2).$$

5. $$\frac{1}{2}\cdot\mathbb{1}_{d_{(-1)}\geq 4}\cdot\frac{(q-1)(q^{\frac{5}{2}d_{(-1)}-6e_K-6}-q^{-6e_K-1})}{q^5-1}.$$

6. $$\mathbb{1}_{e_K\geq 2}\cdot\frac{1}{2}(q-1)q^{-7\lfloor\frac{e_K}{2}\rfloor-1}$$
$$\times\Big(\frac{q(q^{7\lfloor\frac{e_K}{2}\rfloor-7}-1)(q^6+q^4+q^3+q+1)}{q^7-1}+1+\mathbb{1}_{2\nmid e_K}(q^{-2}+q^{-3})\Big).$$

7. $$-\mathbb{1}_{e_K\geq 2}\cdot\frac{1}{2}\cdot\frac{(q-1)(q+1)(q^{-7}-q^{-3e_K-1})}{q^3-1}.$$

8. $$-\frac{1}{2}q^{-3e_K-2}(1-q^{-\lfloor\frac{e_K}{2}\rfloor}).$$

9. $$\begin{cases} q^{-6e_K-3} & \text{if } -1\in K^{\times 2},\\ \frac{1}{2}q^{-6e_K-3} & \text{if } K(\sqrt{-1})/K \text{ is quadratic and totally ramified},\\ 0 & \text{otherwise.}\end{cases}$$

**Corollary 1.10.** *We have the following formula for $\widetilde{m}(\Sigma^{D_4})$, which is made completely explicit by Corollaries 1.8 and 1.9.*

$$\widetilde{m}(\Sigma^{D_4})=\frac{1}{q^2+q+1}\cdot(q^{-3e_K-3}+q^{-3e_K-1}+q^{-2})-\widetilde{m}(\Sigma^{C_4})-3\widetilde{m}(\Sigma^{V_4}).$$

### *1.3. Correctness of results*

Using MAGMA [BCP97] and the LMFDB [LMFDB], we have verified Theorems 1.1-1.5 and Corollaries 1.6-1.10 for all extensions $K/\mathbb{Q}_2$ of degree at most 3. Whenever $e_K\leq 10$ and $f_K\leq 10$, we have also checked numerically the deduction of Corollaries 1.6-1.10 from Theorems 1.1-1.5. Our code is available at https://github.com/Sebastian-Monnet/Mass-Formula-Checks.

### *1.4. Index of notation*

We fix the following notation.

1. For a 2-adic field $F$, write:
   (a) $\mathcal{O}_F$ for its ring of integers.
   (b) $\pi_F$ for a uniformiser of $\mathcal{O}_F$.
   (c) $\mathfrak{p}_F$ for the maximal ideal of $\mathcal{O}_F$.
   (d) $\mathbb{F}_F$ for the residue field $\mathcal{O}_F/\mathfrak{p}_F$.
   (e) $q_F$ for the cardinality of $\mathbb{F}_F$.
   (f) $e_F$ for the absolute ramification index $e(F/\mathbb{Q}_2)$.
   (g) $f_F$ for the inertia degree $f(F/\mathbb{Q}_2)$.
   (h) $v_F$ for the unique 2-adic valuation on $F$, normalised such that $v_F(\pi_F)=1$.
   (i) $U_F^{(i)}$ for the group $1+\mathfrak{p}_F^i$ in the unit filtration, where $i>0$.

(j) $U_F^{(0)}$ for the unit group $\mathcal{O}_F^\times$.

2. Given an extension $E/F$ of 2-adic fields, write:
   (a) $d_{E/F}$ for its discriminant ideal.
   (b) $e(E/F)$ for its ramification index.
   (c) $f(E/F)$ for its inertia degree.
3. $K$: A fixed 2-adic field.
4. $q$: Shorthand for $q_K$.
5. $\Sigma$: The set of isomorphism classes of totally ramified quartic extensions $L/K$.
6. $\widetilde{L}$: For an extension $L/K$ of $K$, write $\widetilde{L}$ for the normal closure of $L$ over $K$.
7. For a group $G \in \{S_4, A_4, D_4, V_4, C_4\}$ and positive integer $m$, write:
   (a) $\Sigma^G := \{L \in \Sigma : \mathrm{Gal}(\widetilde{L}/K) \cong G\}$.
   (b) $\Sigma_m := \{L \in \Sigma : v_K(d_{L/K}) = m\}$.
   (c) $\Sigma_m^G := \Sigma_m \cap \Sigma^G$.
8. $d_{(-1)}$: The discriminant valuation $v_K(d_{K(\sqrt{-1})/K})$.
9. $\widetilde{m}(S)$: For $S \subseteq \Sigma$, the *mass* of $S$ is

$$\widetilde{m}(S) = \sum_{L \in S} \frac{(\#\operatorname{Aut}(L/K))^{-1}}{q^{v_K(d_{L/K})}}.$$

10. $\Sigma^{1-\mathrm{Aut}}$ and $\Sigma_m^{1-\mathrm{Aut}}$: The sets $\Sigma^{A_4} \cup \Sigma^{S_4}$ and $\Sigma^{1-\mathrm{Aut}} \cap \Sigma_m$ respectively.
11. $P$: The set of monic, quartic Eisenstein polynomials in $K[X]$.
12. $L_f$: For $f \in P$, write $L_f$ for the field extension $K[X]/(f)$ of $K$.
13. $P_m, P^G$ and $P_m^G$: For $G \in \{S_4, A_4, D_4, V_4, C_4\}$, define $P_m, P^G$, and $P_m^G$ to be the sets of $f \in P$ such that $L_f$ is in $\Sigma_m, \Sigma^G$, and $\Sigma_m^G$ respectively.
14. $P^{1-\mathrm{Aut}}$ and $P_m^{1-\mathrm{Aut}}$: The sets of $f \in P$ such that $L_f \in \Sigma^{1-\mathrm{Aut}}$ and $L_f \in \Sigma_m^{1-\mathrm{Aut}}$, respectively.
15. $\mu$: Haar measure on $\mathcal{O}_K^4$, normalised so that $\mu(\mathcal{O}_K^4) = 1$.
16. $v_\pi$: Given an extension $L/K$, such that $\pi$ is a uniformiser of $L$, we write $v_\pi$ for the 2-adic valuation on $L$, normalised so that $v_\pi(\pi) = 1$.
17. $T_m$: For even integers $4 \le m \le 6e_K+2$, this is the set of $a_0+a_1X+a_2X^2+a_3X^3+X^4$ in $P$ such that

$$\begin{cases} v_K(a_1) = \frac{m}{4}, \quad v_K(a_2) \ge \frac{m}{6}, \quad v_K(a_3) \ge \frac{m}{4}, & \text{if } m \equiv 0 \pmod 4, \\ v_K(a_1) \ge \frac{m+2}{4}, \quad v_K(a_2) \ge \frac{m}{6}, \quad v_K(a_3) = \frac{m-2}{4}, & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

18. $\mathcal{R}$: System of representatives for $(\mathcal{O}_K/\mathfrak{p}_K)^\times$.
19. $g_f^{(u)}$: When $m$ is a multiple of 6 with $6 \le m \le 6e_K$ and we have $u \in \mathcal{R}$ and $f \in P_m$, define

$$g_f^{(u)}(X) = f(X + \pi + u\pi^{\frac{m}{3}}).$$

20. $b_i^{(u)}$: The $X^i$ coefficient of $g_f^{(u)}$.

21. $\mu_3 \subseteq K$: Shorthand for "$K$ contains three distinct cube roots of unity".
22. Let $F$ be a 2-adic field. Write:
    (a) $\mathrm{Ext}_{2/F}$ for the set of isomorphism classes of quadratic extensions of $F$.
    (b) $\mathrm{Ext}_{2/F,m}$ (respectively $\mathrm{Ext}_{2/F,\leq m}$) for the set of $E \in \mathrm{Ext}_{2/F}$ such that we have $v_F(d_{E/F}) = m$ (respectively $v_F(d_{E/F}) \leq m$).
23. Let $E/K$ be a quadratic extension. Write:
    (a) $\mathrm{Ext}_{2/E}^{G/K}$ for the set of $L \in \mathrm{Ext}_{2/E}$ such that the Galois closure group of $L/K$ is isomorphic to $G$.
    (b) $\mathrm{Ext}_{2/E,m_2}^{G/K}$ (respectively $\mathrm{Ext}_{2/E,\leq m_2}^{G/K}$) for the set of $L \in \mathrm{Ext}_{2/E}^{G/K}$ such that $v_E(d_{L/E}) = m_2$ (respectively $v_E(d_{L/E}) \leq m_2$).
24. $\mathrm{Ext}_{2/K,m_1}^{\uparrow C_4}$ (respectively $\mathrm{Ext}_{2/K,\leq m_1}^{\uparrow C_4}$): Set of $C_4$-extendable quadratic extensions $E/K$ such that $v_K(d_{E/K}) = m_1$ (respectively $v_K(d_{E/K}) \leq m_1$).
25. $N_{\mathrm{ext}}(m_1)$: Function explicitly defined in Definition 4.1.
26. $N^{C_4}(m_1, m_2)$: Function explicitly defined in Definition 4.3.
27. $\alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_F^l}$: Given a $p$-adic field $F$, a nonnegative integer $l$, and elements $\alpha, x \in F$, this means that $x \neq 0$ and
$$v_F(\alpha/x^2 - 1) \geq l.$$
28. $S_{F/K,t}$: For an extension $F/K$ and an integer $1 \leq t \leq v_F(2)$, we define
$$S_{F/K,t} = \{u \in K^\times/K^{\times 2} : u/x^2 \equiv 1 \pmod{\mathfrak{p}_F^{2t}} \text{ for some } x \in F^\times\}.$$
    For $t = 0$, define
$$S_{F/K,0} = \{u \in K^\times/K^{\times 2} : v_F(u) \text{ is even}\}.$$
29. Let $\mathcal{A}$ be a subgroup of $K^\times/K^{\times 2}$. Then write:
    (a) $K(\sqrt{\mathcal{A}}) = K(\{\sqrt{\alpha} : [\alpha] \in \mathcal{A}\})$.
    (b) $\mathcal{O}_K^{\mathcal{A}} = \mathcal{O}_K^\times \cap \mathrm{Nm}\, K(\sqrt{\mathcal{A}})$.
    (c) $S_{K/K,t}^{\mathcal{A}} = S_{K/K,t} \cap \left(\mathrm{Nm}\, K(\sqrt{\mathcal{A}})/K^{\times 2}\right)$, where $0 \leq t \leq e_K$.
    (d) $\mathrm{Ext}_{2/K,\leq m_1}^{\mathcal{A}}$ for the set of $E \in \mathrm{Ext}_{2/K,\leq m_1}$ with $\mathcal{A} \subseteq \mathrm{Nm}\, E$.
    (e) $(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}$ for the image of the map $\mathcal{O}_K^{\mathcal{A}} \to (\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times$.
    (f) $\mathcal{A}_t = \mathcal{A} \cap \left(U_K^{(2t)}K^{\times 2}/K^{\times 2}\right)$, where $0 \leq t \leq e_K$.
30. $\mathrm{Ext}_{2/K}^{\hookrightarrow L}$: For $G \in \{V_4, C_4, D_4\}$ and $L \in \Sigma^G$, this is the set of $E \in \mathrm{Ext}_{2/K}$ such that there exists a $K$-morphism $E \hookrightarrow L$.
31. $\mathrm{Twist}_K(L/E)$: For $G \in \{V_4, C_4, D_4\}$, $L \in \Sigma^G$, and $E \in \mathrm{Ext}_{2/K}^{\hookrightarrow L}$, this is the set of $L' \in \mathrm{Ext}_{2/E}$ such that there is a $K$-isomorphism $L \to L'$, where $L$ is viewed as an extension of $E$ via the unique embedding $E \hookrightarrow L$.
32. $\mathrm{Tow}_m$: The set of pairs $(E, L)$, where $L/E/K$ is a tower of totally ramified quadratic extensions and $v_K(d_{L/K}) = m$.
33. $\Phi_m$: The forgetful map $\mathrm{Tow}_m \to \Sigma_m$, taking $(E, L)$ to the extension $L$ of $K$.

*1.5. Acknowledgements*

I am grateful to my supervisor, Rachel Newton, for her support and enthusiasm throughout the project. Thanks also to Melanie Matchett Wood and Takehiko Yasuda for helpful suggestions, especially in the Galois cases, and to John Voight for suggesting I use the LMFDB to check my results. I am particularly indebted to Lee Berry, Ross Paterson, and Tim Santens for some very helpful conversations.

This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], via the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London. Finally, many thanks to the reviewer for their helpful comments. I appreciated and agreed with all of their suggestions, and I'm grateful for their help in improving the work.

## 2. The cases $G = S_4$ and $G = A_4$

Throughout this paper, all Eisenstein polynomials are taken to be monic. Write $P$ for the set of quartic Eisenstein polynomials in $K[X]$. For $f \in P$, let $L_f$ be the field $K[X]/(f)$, which is a totally ramified quartic extension of $K$. Given a finite group $G$, let $P^G$ be the set of $f \in P$ such that $L_f/K$ has Galois closure group isomorphic to $G$. For any integer $m$, let $P_m$ be the set of $f \in P$ such that $v_K(d_{L_f/K}) = m$, or equivalently such that $v_K(\mathrm{disc}(f)) = m$. For each $G$, write $P_m^G$ for the intersection $P^G \cap P_m$. Write $P^{1-\mathrm{Aut}}$ and $P_m^{1-\mathrm{Aut}}$ as shorthand[1] for $P^{S_4} \cup P^{A_4}$ and $P_m^{S_4} \cup P_m^{A_4}$ respectively. Similarly, write $\Sigma^{1-\mathrm{Aut}}$ and $\Sigma_m^{1-\mathrm{Aut}}$ for $\Sigma^{S_4} \cup \Sigma^{A_4}$ and $\Sigma_m^{S_4} \cup \Sigma_m^{A_4}$ respectively.

The quartic Eisenstein polynomials in $K[X]$ embed naturally into $\mathcal{O}_K^4$ via

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \mapsto (a_3, a_2, a_1, a_0).$$

Write $\mu$ for the Haar measure on $\mathcal{O}_K^4$, normalised such that $\mu(\mathcal{O}_K^4) = 1$. We will apply this Haar measure to sets of Eisenstein polynomials, viewed as subsets of $\mathcal{O}_K^4$ via the embedding described above.

**Lemma 2.1.** *Let $G \in \{S_4, A_4\}$ let $m$ be a positive integer. We have*

$$\#\Sigma_m^G = \frac{q^{m+2}}{q-1} \cdot \mu(P_m^G).$$

**Proof.** This follows easily from [Ser78, Equation 13].

[1] The $1-$ Aut refers to the fact that $\#\,\mathrm{Aut}(L/K) = 1$ if and only if $L \in \Sigma^{S_4} \cup \Sigma^{A_4}$.

### 2.1. Congruence conditions for $P_m^{1-\mathrm{Aut}}$

In [Lbe09, Theorem 2.9], Lbekkouri gives congruence conditions for a quartic Eisenstein polynomial $f(X) \in \mathbb{Q}_2[X]$ to define a Galois extension. We extend his methods to Eisenstein polynomials over arbitrary 2-adic base fields, to obtain congruence conditions for the set $P_m^{1-\mathrm{Aut}}$, which we will state in Lemma 2.4 and Corollary 2.7.

It should be noted that Lbekkouri's statement of [Lbe09, Theorem 2.9] is incorrect. In items (2i) and (2ii), both instances of "$a_0 + a_2$" should read "$a_0 + 2$". This typo is first introduced in the statement of Proposition 2.8 and is carried over into Theorem 2.9.

For $f \in P$, we will always denote the coefficients of $f$ by

$$f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0.$$

Whenever we refer to the coefficients $a_i$, the choice of $f$ will be clear. Let $\pi_f = X + (f)$ be the natural uniformiser of $L_f$. We will always drop the subscript and denote $\pi_f$ by $\pi$, since our choice of $f$ will be clear. Write $v_\pi$ for the 2-adic valuation on $L_f$, normalised such that $v_\pi(\pi) = 1$. Fix an algebraic closure $\overline{K}$ of $L_f$, and let

$$\sigma_i : L_f \to \overline{K}, \quad i = 1, 2, 3, 4$$

be the four embeddings of $L_f$, where $\sigma_1$ is the identity embedding. For elements $\alpha$ of algebraic extensions of $K$, we will write $v_K(\alpha)$ as shorthand for $\widetilde{v}_K(\alpha)$, where $\widetilde{v}_K$ is the unique extension of $v_K$ to the algebraic closure $\overline{K}$ of $K$.

**Lemma 2.2.** *For all $f \in P^{1-\mathrm{Aut}}$, the three valuations*

$$v_K(\sigma_i(\pi) - \pi), \quad i = 2, 3, 4$$

*are equal.*

**Proof.** Suppose that $f \in P$ and the quantities $v_K(\sigma_i(\pi) - \pi)$ are not all equal for the values $i = 2, 3, 4$. Reordering the $\sigma_i$ if necessary, we have

$$v_K(\sigma_2(\pi) - \pi) \neq v_K(\sigma_i(\pi) - \pi)$$

for $i = 3, 4$. The cubic polynomial $X^{-1}f(X + \pi) \in L_f[X]$ has roots

$$\sigma_i(\pi) - \pi, \quad i = 2, 3, 4.$$

The minimal polynomial of $\sigma_2(\pi) - \pi$ over $L_f$ therefore divides $X^{-1}f(X + \pi)$, and all its roots have the same valuation, so

$$\sigma_2(\pi) - \pi \in L_f,$$

and therefore $f$ has at least two roots in $L_f$, so $f \notin P^{1-\mathrm{Aut}}$.

For each even integer $4 \leq m \leq 6e_K + 2$, define $T_m$ to be the set of $f \in P$ such that

$$\begin{cases} v_K(a_1) = \frac{m}{4}, \quad v_K(a_2) \geq \frac{m}{6}, \quad v_K(a_3) \geq \frac{m}{4}, & \text{if } m \equiv 0 \pmod 4, \\ v_K(a_1) \geq \frac{m+2}{4}, \quad v_K(a_2) \geq \frac{m}{6}, \quad v_K(a_3) = \frac{m-2}{4}, & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

**Lemma 2.3.** *The following two statements are true:*

1. *Let $m$ be an even integer with $4 \leq m \leq 6e_K + 2$ and let $f \in P_m$. Then $f \in T_m$ if and only if*
$$v_K(\sigma_i(\pi) - \pi) = \frac{m}{12}$$
*for $i = 2, 3, 4$.*
2. *Let $m$ be a positive integer. If $P_m^{1-\mathrm{Aut}}$ is nonempty then $m$ is even, $4 \leq m \leq 6e_K + 2$, and $P_m^{1-\mathrm{Aut}} \subseteq T_m$.*

**Proof.** Let $f \in P_m$ for any positive integer $m$, not necessarily even. Define the polynomial

$$g(X) := X^{-1} f(X + \pi),$$

and write $g(X) = \sum_{i=0}^{3} b_i X^i$ for $b_i \in L_f$. It is easy to see that

$$\begin{aligned} b_0 &= a_1 + 2\pi a_2 + 3\pi^2 a_3 + 4\pi^3, \\ b_1 &= a_2 + 3\pi a_3 + 6\pi^2, \\ b_2 &= a_3 + 4\pi. \end{aligned}$$

Since the $v_\pi(a_i)$ are all multiples of 4, we have

$$\begin{aligned} v_\pi(b_0) &= \min\{v_\pi(a_1), v_\pi(2\pi a_2), v_\pi(3\pi^2 a_3), v_\pi(4\pi^3)\}, \\ v_\pi(b_1) &= \min\{v_\pi(a_2), v_\pi(3\pi a_3), v_\pi(6\pi^2)\}, \\ v_\pi(b_2) &= \min\{v_\pi(a_3), v_\pi(4\pi)\}. \end{aligned}$$

The polynomial $g(X) \in L_f[X]$ has roots $\sigma_i(\pi) - \pi$ for $i = 2, 3, 4$. Suppose that

$$v_K(\sigma_i(\pi) - \pi) = \frac{m}{12}$$

for each $i$. Then the Newton polygon of $g(X)$ consists of one line segment $(0, m) \leftrightarrow (3, 0)$, so

$$\begin{cases} m = \min\{v_\pi(a_1), v_\pi(2\pi a_2), v_\pi(3\pi^2 a_3), v_\pi(4\pi^3)\}, \\ \frac{2m}{3} \leq \min\{v_\pi(a_2), v_\pi(3\pi a_3), v_\pi(6\pi^2)\}, \\ \frac{m}{3} \leq \min\{v_\pi(a_3), v_\pi(4\pi)\}, \end{cases} \qquad (*)$$

and for even $m$ this implies membership of $T_m$. Reversing the argument, it is easy to see that for even $m$ with $4 \leq m \leq 6e_K + 2$, every $f \in T_m$ has

$$v_K(\sigma_i(\pi) - \pi) = \frac{m}{12}, \quad i = 2, 3, 4.$$

Thus we have proven (1). Now let $f \in P_m^{1-\mathrm{Aut}}$ for some positive integer $m$. Then Lemma 2.2 implies that

$$v_K(\sigma_i(\pi) - \pi) = \frac{m}{12}$$

for $i = 2, 3, 4$, and we have shown that this implies Equation $(*)$, so

$$\begin{cases} m = \min\{v_\pi(a_1), v_\pi(a_2) + 4e_K + 1, v_\pi(a_3) + 2, 8e_K + 3\}, \\ \frac{2m}{3} \leq \min\{v_\pi(a_2), 4e_K + 2\}. \end{cases}$$

Since $f$ is Eisenstein, $v_\pi(a_i) \geq 4$ for each $i$, and therefore $4 \leq m \leq 6e_K + 3$. Moreover, $v_\pi(a_2) \geq \frac{2m}{3}$ implies that $m \leq v_\pi(a_2) + 2e_K + 1$, so $m \neq v_\pi(a_2) + 4e_K + 1$. Since $m < 8e_K + 3$, we obtain

$$m = \min\{v_\pi(a_1), v_\pi(a_3) + 2\},$$

so $m$ is even, so in fact $4 \leq m \leq 6e_K + 2$. Finally, Part (1) of this lemma shows that $f \in T_m$, completing the proof of (2).

**Lemma 2.4.** *Let $m$ be an even integer with $4 \leq m \leq 6e_K + 2$. If $m$ is not a multiple of 3, then $P_m^{1-\mathrm{Aut}} = T_m$.*

**Proof.** Lemma 2.3 tells us that $P_m^{1-\mathrm{Aut}} \subseteq T_m$, so we just need to show that $T_m \subseteq P_m^{1-\mathrm{Aut}}$. Let $f \in T_m$. Lemma 2.3 tells us that

$$v_\pi(\sigma_i(\pi) - \pi) = \frac{m}{3}, \quad i = 2, 3, 4,$$

so $\sigma_i(\pi) \notin L_f$ for each $i$, since $\frac{m}{3}$ is not an integer, and therefore $T_m \subseteq P_m^{1-\mathrm{Aut}}$.

From now on, fix a system of representatives $\mathcal{R}$ for $(\mathcal{O}_K/\mathfrak{p}_K)^\times$. When $3 \mid m$, for each $u \in \mathcal{R}$ and $f \in P_m$, define the polynomial

$$g_f^{(u)}(X) := f(X + \pi + u\pi^{\frac{m}{3}}),$$

and write $g_f^{(u)}(X) = \sum_{i=0}^4 b_i^{(u)} X^i$ for $b_i^{(u)} \in L_f$. We will always omit the subscript and write $g^{(u)}(X)$ for $g_f^{(u)}(X)$, leaving $f$ implicit.

**Lemma 2.5.** *Let $m$ be a multiple of 6 with $4 \leq m \leq 6e_K + 2$. Let $f \in T_m$ and $u \in \mathcal{R}$. We have:*

1. $v_K(b_3^{(u)}) \geq \frac{m-2}{4}$.
2. $v_K(b_2^{(u)}) \geq \frac{m}{6}$.
3. $v_K(b_1^{(u)}) = \frac{m}{4}$.
4. 

$$v_K(b_0^{(u)}) \begin{cases} \geq \frac{m}{3}+1 & \text{if } 4 \mid m \text{ and } a_1 + ua_2 a_0^{\frac{m}{12}} + u^3 a_0^{\frac{m}{4}} \equiv 0 \pmod{\mathfrak{p}_K^{\frac{m}{4}+1}}, \\ \geq \frac{m}{3}+1 & \text{if } 4 \nmid m \text{ and } a_3 + ua_2 a_0^{\lfloor \frac{m}{12} \rfloor} + u^3 a_0^{\lfloor \frac{m}{4} \rfloor} \equiv 0 \pmod{\mathfrak{p}_K^{\lfloor \frac{m}{4} \rfloor+1}}, \\ = \frac{m}{3} & \text{otherwise.} \end{cases}$$

**Proof.** It is easy to see that for each $i$ and $u$, we have

$$b_i^{(u)} = \sum_{j=i}^{4} \binom{j}{i} a_j (\pi + u\pi^{\frac{m}{3}})^{j-i},$$

where we adopt the convention that $a_4 = 1$. Using this formula for the $b_i^{(u)}$, along with the congruence conditions defining $T_m$, gives us the following three congruences:

$$b_3^{(u)} \equiv a_3 \pmod{\pi^{m+1}}.$$

$$b_2^{(u)} \equiv a_2 \pmod{\pi^{\frac{2m}{3}+1}}.$$

$$b_1^{(u)} \equiv \begin{cases} a_1 \pmod{\pi^{m+1}} & \text{if } m \equiv 0 \pmod 4, \\ 3\pi^2 a_3 \pmod{\pi^{m+1}} & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

We can read off the first three claims from these congruences. Expanding the formula for $b_0^{(u)}$ and ignoring the high-valuation terms, we obtain

$$b_0^{(u)} \equiv \begin{cases} ua_1\pi^{\frac{m}{3}} + u^2 a_2 \pi^{\frac{2m}{3}} + u^4 \pi^{\frac{4m}{3}} \pmod{\pi^{\frac{4m}{3}+1}} & \text{if } m \equiv 0 \pmod 4, \\ u^2 a_2 \pi^{\frac{2m}{3}} + ua_3 \pi^{\frac{m}{3}+2} + u^4 \pi^{\frac{4m}{3}} \pmod{\pi^{\frac{4m}{3}+1}} & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

It follows that $v_K(b_0^{(u)}) \geq \frac{m}{3}$, and $v_K(b_0^{(u)}) \geq \frac{m}{3}+1$ if and only if

$$\begin{cases} a_1 + ua_2\pi^{\frac{m}{3}} + u^3\pi^m \equiv 0 \pmod{\pi^{m+1}} & \text{if } m \equiv 0 \pmod 4, \\ a_3 + ua_2\pi^{\frac{m}{3}-2} + u^3\pi^{m-2} \equiv 0 \pmod{\pi^{m-1}} & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

The result then follows from the fact that,[2] for any positive integer $k$, we have

$$\pi^{4k} \equiv (-a_0)^k \pmod{\pi^{4k+\frac{2m}{3}-2}}.$$

**Lemma 2.6.** *Let $4 \leq m \leq 6e_K + 2$ be a multiple of 6 and let $f \in T_m$. Then $f \notin P_m^{1-\mathrm{Aut}}$ if and only if $v_K(b_0^{(u)}) \geq \frac{m}{3} + 1$ for some $u \in \mathcal{R}$.*

**Proof.** Suppose that $f \notin P_m^{1-\mathrm{Aut}}$. Then $f$ has at least two roots in $L_f$. Reordering the $\sigma_i$ if necessary, we may assume that $\sigma_2(\pi) \in L_f$. Since $f \in T_m$, Lemma 2.3 tells us that $v_K(\sigma_2(\pi) - \pi) = \frac{m}{12}$, so

$$\sigma_2(\pi) = \pi + \tilde{u}\pi^{\frac{m}{3}}$$

for some $\tilde{u} \in \mathcal{O}_{L_f}^{\times}$. Since $L_f/K$ is totally ramified, there is some element $u \in \mathcal{R}$ with $u \equiv \tilde{u} \pmod{\pi}$, which means that

$$v_K(\sigma_2(\pi) - \pi - u\pi^{\frac{m}{3}}) > \frac{m}{12}.$$

The other three roots of $g^{(u)}$ all have valuation at least $\frac{m}{12}$, so

$$v_K(b_0^{(u)}) \geq \frac{m}{3} + 1.$$

Suppose conversely that $v_K(b_0^{(u)}) \geq \frac{m}{3} + 1$ for some $u \in \mathcal{R}$. Lemma 2.5 tells us that $v_K(b_1^{(u)}) = \frac{m}{4}$ and $v_K(b_2^{(u)}) \geq \frac{m}{6}$, so considering the Newton polygon of $g^{(u)}$ tells us that it has exactly one root $\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}}$ with

$$v_\pi(\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}}) \geq \frac{m}{3} + 1.$$

Therefore we have

$$\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}} \in L_f,$$

so $\sigma_i(\pi) \in L_f$, which means that $f \notin P^{1-\mathrm{Aut}}$.

**Corollary 2.7.** *Let $m$ be a multiple of 6 with $4 \leq m \leq 6e_K + 2$, and let $f \in T_m$. The following are equivalent:*

1. *We have $f \notin P_m^{1-\mathrm{Aut}}$.*

[2] This follows from expanding the binomial on the right-hand side of

$$(\pi^4)^k = ((-a_0) + (-a_1\pi - a_2\pi^2 - a_3\pi^3))^k.$$

2. *There is some $u \in \mathcal{R}$ such that*

$$\begin{cases} a_1 + ua_2 a_0^{\lfloor \frac{m}{12} \rfloor} + u^3 a_0^{\lfloor \frac{m}{4} \rfloor} \equiv 0 \pmod{\mathfrak{p}_K^{\lfloor \frac{m}{4} \rfloor + 1}} & \text{if } m \equiv 0 \pmod 4, \\ a_3 + ua_2 a_0^{\lfloor \frac{m}{12} \rfloor} + u^3 a_0^{\lfloor \frac{m}{4} \rfloor} \equiv 0 \pmod{\mathfrak{p}_K^{\lfloor \frac{m}{4} \rfloor + 1}} & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

**Proof.** This is immediate from Lemmas 2.5 and 2.6.

### *2.2. Computing the densities*

**Lemma 2.8.** *Let $m$ be an even integer with $4 \leq m \leq 6e_K + 2$. Then*

$$\mu(T_m) = q^{-\lceil \frac{2m}{3} \rceil - 3}(q-1)^2.$$

**Proof.** This is easy to see from the definition of $T_m$.

Since $\mathbb{F}_K \cong \mathbb{F}_{2^{f_K}}$, the trace map $\mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2} : \mathbb{F}_K \to \mathbb{F}_2$ is given by

$$\mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(x) = x + x^2 + \ldots + x^{2^{f_K - 1}}.$$

**Lemma 2.9.** *Let $\alpha, \beta, \gamma \in \mathbb{F}_K$ with $\alpha \neq 0$, and let $g$ be the polynomial $\alpha X^2 + \beta X + \gamma$ in $\mathbb{F}_K[X]$. The number of roots of $g$ in $\mathbb{F}_K$ is*

$$\begin{cases} 1 & \text{if } \beta = 0, \\ 2 & \text{if } \beta \neq 0 \text{ and } \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(\alpha\gamma/\beta^2) = 0, \\ 0 & \text{if } \beta \neq 0 \text{ and } \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(\alpha\gamma/\beta^2) = 1. \end{cases}$$

**Proof.** The case with $\beta = 0$ is clear, so assume $\beta \neq 0$. Let $u$ be a root of $g$ in a splitting field over $\mathbb{F}_K$, and let $\theta = \frac{\alpha u}{\beta}$. Clearly $u \in \mathbb{F}_K$ if and only if $\theta \in \mathbb{F}_K$, which is equivalent to $\theta + \theta^q = 0$. Since

$$\mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_2) = \{x \mapsto x^{2^i} : i = 0, 1, \ldots, f_K - 1\},$$

it is easy to see that

$$\mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(\theta + \theta^2) = \theta + \theta^q,$$

and also that

$$\theta + \theta^2 = \frac{\alpha\gamma}{\beta^2}.$$

Therefore, $u \in \mathbb{F}_K$ if and only if $\mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(\frac{\alpha\gamma}{\beta^2}) = 0$, and the result follows.

**Lemma 2.10.** *Let $n \geq 0$ be an integer and let $\lambda, \mu \in \mathfrak{p}_K^n$, with $\mu \notin \mathfrak{p}_K^{n+1}$. Define the map*

$$\alpha : \mathcal{O}_K/\mathfrak{p}_K \to \mathcal{O}_K/\mathfrak{p}_K^{n+1}, \quad c \mapsto \lambda c + \mu c^3.$$

*The following two statements are true:*

1. *For $c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times$, we have*

$$\#\{c' \in (\mathcal{O}_K/\mathfrak{p}_K)^\times : \alpha(c') = \alpha(c)\} = \begin{cases} 1 & \text{if } c^2 \equiv \lambda/\mu \pmod{\mathfrak{p}_K}, \\ 1 & \text{if } c^2 \neq \lambda/\mu \text{ and } \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}\left(\frac{\lambda}{c^2\mu}\right) \not\equiv f_K \pmod 2, \\ 3 & \text{if } c^2 \neq \lambda/\mu \text{ and } \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}\left(\frac{\lambda}{c^2\mu}\right) \equiv f_K \pmod 2. \end{cases}$$

2. *We have*

$$\#\operatorname{im}\alpha = \begin{cases} \frac{2q+(-1)^{f_K}}{3} & \text{if } \lambda \notin \mathfrak{p}_K^{n+1}, \\ \frac{q+1+(-1)^{f_K}}{2+(-1)^{f_K}} & \text{if } \lambda \in \mathfrak{p}_K^{n+1}. \end{cases}$$

**Proof.** It is easy to see that for $c, c' \in (\mathcal{O}_K/\mathfrak{p}_K)^\times$, we have $\alpha(c) = \alpha(c')$ if and only if

$$(c-c')\Big((c')^2 + cc' + \frac{\lambda}{\mu} + c^2\Big) \equiv 0 \pmod{\mathfrak{p}_K}.$$

The first statement then follows from Lemma 2.9. For the second statement, suppose first that $\lambda \notin \mathfrak{p}_K^{n+1}$. Then there is some $c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times$ with $\alpha(c) = 0$, so

$$\begin{aligned} \#\operatorname{im}\alpha &= \sum_{c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times} \frac{1}{\#\{c' \in (\mathcal{O}_K/\mathfrak{p}_K)^\times : \alpha(c') = \alpha(c)\}} \\ &= 1 + (q-2-a) + \frac{a}{3}, \end{aligned}$$

where

$$a = \#\{c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times : c^2 \neq \frac{\lambda}{\mu} \text{ and } \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}\left(\frac{\lambda}{c^2\mu}\right) \equiv f_K \pmod 2\}.$$

Since $\lambda \notin \mathfrak{p}_K^{n+1}$, the map

$$(\mathfrak{p}_K/\mathcal{O}_K)^\times \to (\mathfrak{p}_K/\mathcal{O}_K)^\times, \quad c \mapsto \frac{\lambda}{c^2\mu}$$

is a bijection, so

$$\begin{aligned} a &= \#\{u \in (\mathcal{O}_K/\mathfrak{p}_K)^\times \setminus \{1\} : \mathrm{Tr}_{\mathbb{F}_K/\mathbb{F}_2}(u) \equiv f_K \pmod 2\} \\ &= \frac{1}{2}(q - 3 - (-1)^{f_K}), \end{aligned}$$

and the result follows. Now suppose that $\lambda \in \mathfrak{p}_K^{n+1}$. Then $\alpha(c) = 0$ if and only if $c = 0$, so

$$\#\operatorname{im}\alpha = 1 + \sum_{c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times} \frac{1}{\#\{c' \in (\mathcal{O}_K/\mathfrak{p}_K)^\times : \alpha(c') = \alpha(c)\}}.$$

We have $\frac{\lambda}{c^2\mu} \equiv 0 \pmod{\mathfrak{p}_K}$ for all $c \in (\mathcal{O}_K/\mathfrak{p}_K)^\times$, so

$$\#\{c' \in (\mathcal{O}_K/\mathfrak{p}_K)^\times : \alpha(c') = \alpha(c)\} = 2 + (-1)^{f_K},$$

and the result follows.

**Lemma 2.11.** *Let $a, b > 0$ be integers, and let $S$ be the set of triples $(x_0, x_1, x_2) \in \mathcal{O}_K^3$ such that the following two conditions hold:*

1. $v_K(x_0) = 1, \quad v_K(x_1) = a + b, \quad v_K(x_2) \geq b.$
2. *There is some $u \in \mathcal{R}$ such that $x_1 + ux_2x_0^a + u^3x_0^{a+b} \equiv 0 \pmod{\mathfrak{p}_K^{a+b+1}}$.*

*Then $\mu(S) = \frac{1}{3}q^{-a-2b-4}(q-1)^2(2q-1)$.*

**Proof.** Suppose that, for $x_i$ and $x_i'$ in $\mathcal{O}_K$, we have $x_i \equiv x_i' \pmod{\mathfrak{p}_K^{a+b+1}}$ for $i = 0, 1, 2$. Then $(x_0, x_1, x_2) \in S$ if and only if $(x_0', x_1', x_2') \in S$, so

$$\mu(S) = \frac{\#\overline{S}}{q^{3a+3b+3}},$$

where $\overline{S}$ is the set of triples

$$(\bar{x}_0, \bar{x}_1, \bar{x}_2) \in \left((\mathfrak{p}_K/\mathfrak{p}_K^{a+b+1}) \setminus (\mathfrak{p}_K^2/\mathfrak{p}_K^{a+b+1})\right) \times \left((\mathfrak{p}_K^{a+b}/\mathfrak{p}_K^{a+b+1}) \setminus \{0\}\right) \times (\mathfrak{p}_K^b/\mathfrak{p}_K^{a+b+1})$$

such that there is some $u \in \mathcal{R}$ with

$$\bar{x}_1 + u\bar{x}_2\bar{x}_0^a + u^3\bar{x}_0^{a+b} = 0.$$

For each $\bar{x}_0 \in (\mathfrak{p}_K/\mathfrak{p}_K^{a+b+1}) \setminus (\mathfrak{p}_K^2/\mathfrak{p}_K^{a+b+1})$ and $\bar{x}_2 \in \mathfrak{p}_K^b/\mathfrak{p}_K^{a+b+1}$, define the map

$$\alpha_{\bar{x}_0,\bar{x}_2} : \mathcal{O}_K/\mathfrak{p}_K \to \mathfrak{p}_K^{a+b}/\mathfrak{p}_K^{a+b+1}, \quad u \mapsto -u\bar{x}_2\bar{x}_0^a - u^3\bar{x}_0^{a+b}.$$

Then

$$\overline{S} = \bigsqcup_{\substack{\bar{x}_0 \in (\mathfrak{p}_K/\mathfrak{p}_K^{a+b+1}) \setminus (\mathfrak{p}_K^2/\mathfrak{p}_K^{a+b+1}) \\ \bar{x}_2 \in \mathfrak{p}_K^b/\mathfrak{p}_K^{a+b+1}}} \{\bar{x}_0\} \times \Big( \operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2} \setminus \{0\} \Big) \times \{\bar{x}_2\}.$$

Since $\alpha_{\bar{x}_0,\bar{x}_2}(0) = 0$, we always have $0 \in \operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2}$, so

$$\#\Big( \operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2} \setminus \{0\} \Big) = \#\operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2} - 1,$$

and therefore

$$\#\overline{S} = \sum_{\substack{\bar{x}_0 \in (\mathfrak{p}_K/\mathfrak{p}_K^{a+b+1}) \setminus (\mathfrak{p}_K^2/\mathfrak{p}_K^{a+b+1}) \\ \bar{x}_2 \in \mathfrak{p}_K^b/\mathfrak{p}_K^{a+b+1}}} (\#\operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2} - 1),$$

Lemma 2.10 tells us that

$$\#\operatorname{im} \alpha_{\bar{x}_0,\bar{x}_2} = \begin{cases} \frac{2q+(-1)^{f_K}}{3} & \text{if } \bar{x}_2 \notin \mathfrak{p}_K^{b+1}/\mathfrak{p}_K^{a+b+1}, \\ \frac{q+1+(-1)^{f_K}}{2+(-1)^{f_K}} & \text{if } \bar{x}_2 \in \mathfrak{p}_K^{b+1}/\mathfrak{p}_K^{a+b+1}. \end{cases}$$

It follows that

$$\#\overline{S} = \frac{1}{3} q^{2a+b-1}(q-1)^2(2q-1),$$

so

$$\mu(S) = \frac{1}{3} q^{-a-2b-4}(q-1)^2(2q-1).$$

**Corollary 2.12.** *Let $4 \leq m \leq 6e_K + 2$ be a multiple of 6. Then*

$$\mu(T_m \setminus P_m^{1-\mathrm{Aut}}) = \frac{1}{3} q^{-\frac{2m}{3}-4}(q-1)^2(2q-1).$$

**Proof.** Suppose first that $4 \mid m$. Setting $x_i = a_i$ for $i = 0, 1, 2$ and $(a, b) = (\frac{m}{12}, \frac{m}{6})$, Corollary 2.7 tells us that $T_m \setminus P_m^{1-\mathrm{Aut}}$ is the set $S$ from Lemma 2.11, together with the added congruence condition that $v_K(a_3) \geq \frac{m}{4}$, so

$$\mu(T_m \setminus P_m^{1-\mathrm{Aut}}) = \mu(S) \cdot q^{-\frac{m}{4}} = \frac{1}{3} q^{-\frac{2m}{3}-4}(q-1)^2(2q-1).$$

If $4 \nmid m$, then set

$$(x_0, x_1, x_2) := (a_0, a_3, a_2), \quad (a, b) = \Big( \frac{m-6}{12}, \frac{m}{6} \Big),$$

and proceed similarly.

**Corollary 2.13.** *Let $4 \leq m \leq 6e_K + 2$ be an even integer. Then*

$$\mu(P_m^{1-\mathrm{Aut}}) = q^{-\lceil \frac{2m}{3} \rceil - 3}(q-1)^2 \cdot \Big(1 + \mathbb{1}_{6|m} \cdot \Big(\frac{1-2q}{3q}\Big)\Big).$$

**Proof.** This is immediate from Corollary 2.12 and Lemma 2.8.

**Corollary 2.14.** *If $\Sigma_m^{1-\mathrm{Aut}}$ is nonempty, then $m$ is an even integer with $4 \leq m \leq 6e_K + 2$, and*

$$\#\Sigma_m^{1-\mathrm{Aut}} = q^{\lfloor \frac{m}{3} \rfloor - 1}(q-1)\Big(1 + \mathbb{1}_{6|m} \cdot \Big(\frac{1-2q}{3q}\Big)\Big).$$

**Proof.** This is immediate from Lemma 2.1 and Corollary 2.13.

### *2.3. Distinguishing between $A_4$ and $S_4$*

Write "$\mu_3 \subseteq K$" as shorthand for "$K$ contains three distinct cube roots of unity".

**Lemma 2.15.** *The following three statements are true:*

1. *(Tower law for discriminant) Let $M/L/K$ be extensions of 2-adic fields. Then*
$$v_K(d_{M/K}) = [M : L] \cdot v_K(d_{L/K}) + f(L/K) \cdot v_L(d_{M/L}).$$
2. *We have $\mu_3 \subseteq K$ if and only if $f_K$ is even.*
3. *If $\mu_3 \not\subseteq K$, then $K$ has only one $C_3$-extension up to isomorphism, namely the unramified extension.*

**Proof.** Claim (1) is [Ser95, Proposition III.8]. Claim (2) follows from Hensel's Lemma. Finally, Claim (3) comes from class field theory, along with the fact that we have $K^\times/K^{\times 3} \cong \mathbb{Z}/3\mathbb{Z}$, which follows from [Neu13, Proposition 3.7].

**Lemma 2.16.** *If $\mu_3 \subseteq K$, then $K$ has no $S_4$-extensions.*

**Proof.** This is part of [WJ07, Theorem 1.2].

**Proof** *(Proof of Theorem 1.1).* By Lemma 2.15 (2), we have $\mu_3 \subseteq K$, so Lemma 2.16 tells us that $\Sigma_m^{A_4} = \Sigma_m^{1-\mathrm{Aut}}$, and the result follows by Corollary 2.14.

**Lemma 2.17.** *Let $M/F$ be a $V_4$-extension of 2-adic fields, and let $E_1, E_2, E_3$ be its three quadratic intermediate extensions. Then*

$$v_F(d_{M/F}) = \sum_{i=1}^{3} v_F(d_{E_i/F}).$$

**Proof.** This follows easily from [Keu23, Theorem 17.50].

**Lemma 2.18.** *Suppose that $\mu_3 \not\subseteq K$ and let $L \in \Sigma^{A_4}$. Then $3 \mid v_K(d_{L/K})$.*

**Proof.** Let $M$ be a normal closure of $L$ over $K$, so $\mathrm{Gal}(M/K) \cong A_4$, and let $F = M^{V_4}$. The extension $F/K$ is a $C_3$-extension, so it is unramified by Lemma 2.15, Part (3). Since $L/K$ is totally ramified, we have $e(M/K) = 4$ and $f(M/K) = 3$, so $V_4$ is the inertia group of $M/K$. Since $F/K$ is unramified, the tower law for discriminant gives

$$v_K(d_{M/K}) = 3v_F(d_{M/F}).$$

Let $E_1, E_2, E_3$ be the three intermediate extensions of the $V_4$-extension $M/F$. Since the three double transpositions in $A_4$ are conjugate, the extensions $E_i/K$ are isomorphic, so they have the same discriminant. By the tower law for discriminant, it follows that the valuations

$$v_F(d_{E_i/F}), \quad i = 1, 2, 3$$

are all equal. By Lemma 2.17, we have

$$v_F(d_{M/F}) = \sum_{i=1}^{3} v_F(d_{E_i/F}) = 3v_F(d_{E_1/F}),$$

so

$$v_K(d_{M/K}) = 9v_F(d_{E_1/F}).$$

Since $M/L$ is unramified, the tower law also gives

$$v_K(d_{M/K}) = 3v_K(d_{L/K}),$$

and the result follows.

In the statement and proof of the following lemma, the term "$A_4$-extension" refers to a Galois extension with Galois group $A_4$.

**Lemma 2.19.** *Suppose that $\mu_3 \not\subseteq K$. Then there is a bijection between $\Sigma^{A_4}$ and the set of isomorphism classes of $A_4$-extensions of $K$.*

**Proof.** For an $A_4$-quartic extension $L/K$, let $\widetilde{L}$ be the normal closure of $L$ over $K$. The map $L \mapsto \widetilde{L}$ is a well-defined bijection between the set of isomorphism classes of $A_4$-quartics and the set of isomorphism classes of $A_4$-extensions. Therefore, to prove the lemma, it suffices to show that every $A_4$-quartic is totally ramified.

Let $L/K$ be an $A_4$-quartic. Then there is an extension $M/L$ such that $M/K$ is an $A_4$-extension and $L = M^{A_3}$ for some choice of embedding $A_3 \subseteq A_4$. Let $G_0 \subseteq A_4$ be the inertia group of $M/K$. Since $M^{V_4}/K$ is a $C_3$-extension, it is unramified by Lemma 2.15, Part (3), and therefore $G_0 \subseteq V_4$. Since $M/K$ is not cyclic, it is ramified, so $\#G_0 \geq 2$. Since $G_0$ is a normal subgroup of $A_4$, we must have $G_0 = V_4$, so $e(M/K) = 4$. Since $M/L$ is a $C_3$-extension, it is unramified by Lemma 2.15, Part (3), so $L/K$ is totally ramified, as required.

**Lemma 2.20.** *Suppose that $\mu_3 \not\subseteq K$. We have*

$$\Sigma^{A_4} = \bigcup_{\substack{m \\ 6|m}} \Sigma_m^{1-\mathrm{Aut}}.$$

**Proof.** By Corollary 2.14 and Lemma 2.18, we have

$$\Sigma^{A_4} \subseteq \bigcup_{\substack{m \\ 6|m}} \Sigma_m^{1-\mathrm{Aut}}.$$

Lemma 2.19 and [WJ07, Theorem 1.2] tell us that

$$\#\Sigma^{A_4} = \frac{q^{2e_K} - 1}{3}.$$

From Corollary 2.14, we obtain

$$\sum_{\substack{m \\ 6|m}} \#\Sigma_m^{1-\mathrm{Aut}} = \frac{q^{2e_K} - 1}{3},$$

and the result follows.

**Proof** *(Proof of Theorem 1.2).* Lemma 2.15(2) tells us that $\mu_3 \not\subseteq K$. The result then follows from Corollary 2.14 and Lemma 2.20.

**Proof** *(Proof of Corollary 1.6).* Theorem 1.1 tells us that $\widetilde{m}(\Sigma^{S_4}) = 0$ and

$$\widetilde{m}(\Sigma^{A_4}) = \sum_{\substack{4 \leq m \leq 6e_K+2 \\ m \text{ even}}} q^{-\lceil \frac{2m}{3} \rceil - 1}(q-1)\Big(1 + \mathbb{1}_{6|m} \cdot \big(\frac{1-2q}{3q}\big)\Big).$$

The result then follows from a tedious computation, which we omit since it is straightforward.

**Proof** *(Proof of Corollary 1.7).* By Theorem 1.2, we have

$$\widetilde{m}(\Sigma^{S_4}) = \sum_{\substack{4\leq m\leq 6e_K+2\\ 2|m,\ 3\nmid m}} q^{\lfloor \frac{m}{3}\rfloor - m - 1}(q-1),$$

which can easily be rearranged into the required form. The computation of $\widetilde{m}(\Sigma^{A_4})$ is similar.

## 3. The case $G = V_4$

**Lemma 3.1.** *Let $d \in K^\times \setminus K^{\times 2}$ and let $E = K(\sqrt{d})$. If $v_K(d)$ is even, then $v_K(d_{E/K})$ is an even integer with $0 \leq v_K(d_{E/K}) \leq 2e_K$. If $v_K(d)$ is odd, then $v_K(d_{E/K}) = 2e_K + 1$.*

**Proof.** This is part of the $p = 2$ case of [Dab01, Theorem 2.4].

**Lemma 3.2.** *If $\Sigma_m^{V_4}$ is nonempty, then $m$ is an even integer and $6 \leq m \leq 6e_K + 2$.*

**Proof.** Let $L \in \Sigma_m^{V_4}$, and let $E_1, E_2$ and $E_3$ be the intermediate quadratic subfields of $L$. Let $c_i = v_K(d_{E_i/K})$ for each $i$, so that

$$m = c_1 + c_2 + c_3,$$

by Lemma 2.17. We may write $E_i = K(\sqrt{d_i})$, for $d_i \in K^\times \setminus K^{\times 2}$, such that $d_1 d_2 d_3 \in K^{\times 2}$. Since $v_K(d_1 d_2 d_3)$ is even, it follows from Lemma 3.1 that either 0 or 2 of the $c_i$ are equal to $2e_K + 1$, and the rest are even integers with $2 \leq c_i \leq 2e_K$. The result follows.

**Lemma 3.3.** *[Tun78, Lemma 4.7] Let $m$ be a positive even integer with $2 \leq m \leq 6e_K + 2$. Then*

$$\#\Sigma_m^{V_4} = 2(q-1)q^{\frac{m-4}{2}}\left(q^{-\lfloor \frac{m}{6}\rfloor}(1 + \mathbb{1}_{3|m}\cdot\frac{q-2}{3}) - \mathbb{1}_{m\leq 4e_K+2}\cdot q^{-\lfloor \frac{m-2}{4}\rfloor}\right)$$

**Proof** *(Proof of Theorem 1.3).* The result follows immediately from Lemmas 3.2 and 3.3.

**Proof** *(Proof of Corollary 1.8).* By Lemmas 3.2 and 3.3, we have

$$\widetilde{m}(\Sigma^{V_4}) = \frac{1}{2}(q-1) \times \left(\sum_{\substack{4\leq m\leq 6e_K+2\\ m \text{ even}}} q^{-\frac{m+4}{2}-\lfloor \frac{m}{6}\rfloor}(1 + \mathbb{1}_{3|m}\cdot\frac{q-2}{3}) - \sum_{\substack{4\leq m\leq 4e_K+2\\ m \text{ even}}} q^{-\frac{m+4}{2}-\lfloor \frac{m-2}{4}\rfloor}\right),$$

and it is straightforward to rearrange this expression into the desired form.

## 4. The case $G = C_4$

### 4.1. Sketch of our approach

Let $L/K$ be a $C_4$-extension and let $E$ be its unique nontrivial intermediate field.

For a 2-adic field $F$, write $\mathrm{Ext}_{2/F}$ for the set of isomorphism classes of quadratic extensions of $F$. For any real number $m$, write $\mathrm{Ext}_{2/F,m}$ (respectively $\mathrm{Ext}_{2/F,\leq m}$) for the set of $E \in \mathrm{Ext}_{2/F}$ with $v_F(d_{E/F}) = m$ (respectively $v_F(d_{E/F}) \leq m$). For quadratic extensions $E/K$ and $G \in \{D_4, V_4, C_4\}$, write $\mathrm{Ext}_{2/E}^{G/K}$ for the set of $L \in \mathrm{Ext}_{2/E}$ such that $L/K$ has Galois closure group isomorphic to $G$. Finally, for any real number $m_2$, write $\mathrm{Ext}_{2/E,m_2}^{G/K}$ (respectively $\mathrm{Ext}_{2/E,\leq m_2}^{G/K}$) for the intersection $\mathrm{Ext}_{2/E}^{G/K} \cap \mathrm{Ext}_{2/E,m_2}$ (respectively $\mathrm{Ext}_{2/E}^{G/K} \cap \mathrm{Ext}_{2/E,\leq m_2}$).

Call a quadratic extension $E/K$ *$C_4$-extendable* if there is some quadratic extension $L/E$ such that $L/K$ is a $C_4$-extension. For any real number $m_1$, write $\mathrm{Ext}_{2/K,m_1}^{\uparrow C_4}$ (respectively $\mathrm{Ext}_{2/K,\leq m_1}^{\uparrow C_4}$) for the set of $C_4$-extendable extensions $E/K$ such that $v_K(d_{E/K}) = m_1$ (respectively $v_K(d_{E/K}) \leq m_1$).

Recall that we write $d_{(-1)} = v_K(d_{K(\sqrt{-1})/K})$. In the current subsection, we state the main results, whose proofs are postponed to the later subsections.

**Definition 4.1.** For even integers $m_1$ with $2 \leq m_1 \leq 2e_K$, define

$$N_{\mathrm{ext}}(m_1) := (1 + \mathbb{1}_{m_1 \leq 2e_K - d_{(-1)}}) q^{\frac{m_1}{2}-1}(q - 1 - \mathbb{1}_{m_1 = 2e_K - d_{(-1)}+2}).$$

For $m_1 = 2e_K + 1$, define

$$N_{\mathrm{ext}}(2e_K+1) = \begin{cases} 2q^{e_K} & \text{if } -1 \in K^{\times 2}, \\ q^{e_K} & \text{if } K(\sqrt{-1})/K \text{ is quadratic and totally ramified}, \\ 0 & \text{if } K(\sqrt{-1})/K \text{ is quadratic and unramified.} \end{cases}$$

And set $N_{\mathrm{ext}}(m_1) = 0$ for all other real numbers $m_1$.

**Lemma 4.2.** *If $E/K$ is a totally ramified $C_4$-extendable extension, then $2 \leq v_K(d_{E/K}) \leq 2e_K + 1$ and $v_K(d_{E/K})$ is either even or equal to $2e_K + 1$. For such $m_1$, we have*

$$\#\mathrm{Ext}_{2/K,m_1}^{\uparrow C_4} = N_{\mathrm{ext}}(m_1).$$

**Definition 4.3.** Let $m_1$ be an even integer with $2 \leq m_1 \leq e_K$. For each integer $m_2$, define

$$N^{C_4}(m_1, m_2) = \begin{cases} q^{m_1 - 1} & \text{if } m_2 = 3m_1 - 2, \\ q^{\lfloor \frac{m_1+m_2}{4} \rfloor} - q^{\lfloor \frac{m_1+m_2-2}{4} \rfloor} & \text{if } 3m_1 \leq m_2 \leq 4e_K - m_1 \text{ and } m_2 \text{ is even}, \\ q^{e_K} & \text{if } m_2 = 4e_K - m_1 + 2, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $m_1 = 2e_K + 1$ or $m_1$ is even with $e_K < m_1 \leq 2e_K$. Then define

$$N^{C_4}(m_1, m_2) = \begin{cases} 2q^{e_K} & \text{if } m_2 = m_1 + 2e_K, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, define $N^{C_4}(m_1, m_2) = 0$ for all other real numbers $m_1$ and $m_2$.

**Lemma 4.4.** *Let $E$ be a totally ramified $C_4$-extendable extension and let $m_1 = v_K(d_{E/K})$. For all $m_2$, we have*

$$\#\mathrm{Ext}^{C_4/K}_{2/E,m_2} = N^{C_4}(m_1, m_2).$$

**Corollary 4.5.** *If $\Sigma_m^{C_4}$ is nonempty, then either $m = 8e_K + 3$ or $m$ is an even integer with $8 \leq m \leq 8e_K$. For any even integer $m$, the number $\#\Sigma_m^{C_4}$ is the sum of the following four quantities:*

1. $\mathbb{1}_{8 \leq m \leq 5e_K - 2} \cdot q^{\frac{m-3}{5}} N_{\mathrm{ext}}(\frac{m+2}{5})$.
2. $$\sum_{\substack{\max\{2, m-4e_K\} \leq m_1 \leq \min\{\frac{m}{5}, e_K\} \\ m_1 \equiv m \pmod 4}} q^{\frac{m-m_1}{4} - 1}(q-1) N_{\mathrm{ext}}(m_1).$$
3. $\mathbb{1}_{4e_K + 4 \leq m \leq 5e_K + 2} \cdot q^{e_K} N_{\mathrm{ext}}(m - 4e_K - 2)$.
4. $\mathbb{1}_{5e_K + 3 \leq m \leq 8e_K} \cdot 2q^{e_K} N_{\mathrm{ext}}(\frac{m - 2e_K}{3})$.

*Moreover,*

$$\#\Sigma^{C_4}_{8e_K+3} = \begin{cases} 4q^{2e_K} & \text{if } -1 \in K^{\times 2}, \\ 2q^{2e_K} & \text{if } K(\sqrt{-1})/K \text{ is quadratic and totally ramified,} \\ 0 & \text{if } K(\sqrt{-1})/K \text{ is quadratic and unramified.} \end{cases}$$

### *4.2. Counting $C_4$-extendable extensions*

The aim of this subsection is to prove Lemma 4.2. The paper [CDO05] gives conditions on $d \in K^\times$ for the extension $K(\sqrt{d})/K$ to be $C_4$-extendable. We use these conditions and adapt the methods of [CDO05] to parametrise and count $C_4$-extendable extensions.

**Lemma 4.6** *(Hecke's Theorem). Let $E$ be a 2-adic field, let $\alpha \in E^\times \setminus E^{\times 2}$, and let $L = E(\sqrt{\alpha})$. If $v_E(\alpha)$ is odd, then $v_E(d_{L/E}) = 2v_E(2) + 1$. If $v_E(\alpha)$ is even, then $L/E$ is totally ramified if and only if $\alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^{2v_E(2)}}$ has no solution $x \in E$. In that case, we have*

$$v_E(d_{L/E}) = 2v_E(2) + 1 - \kappa_{E,\alpha},$$

*where*

$$\kappa_{E,\alpha} = \max\{0 \leq l < 2v_E(2) : \alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^l} \text{ has a solution in } E\}.$$

**Proof.** This is the special case $p = 2$ of [Dab01, Theorem 2.4].

**Corollary 4.7.** *Let $E, \alpha$, and $L$ be as in Lemma 4.6, and assume that $v_E(\alpha)$ is even. Let $t$ be an integer with $0 \leq t \leq v_E(2)$. Then $v_E(d_{L/E})$ is an even integer and*

$$v_E(d_{L/E}) \leq 2v_E(2) - 2t$$

*if and only if there is some $x \in E^\times$ with $\alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^{2t}}$.*

**Proof.** This follows from Lemma 4.6, along with the fact[3] that for $0 \leq t < v_E(2)$ and $u \in \mathcal{O}_E^\times$, if $u$ is square modulo $\mathfrak{p}_E^{2t}$ then it is also square modulo $\mathfrak{p}_E^{2t+1}$.

**Lemma 4.8.** *Let $E = K(\sqrt{d})$ for $d \in K^\times \setminus K^{\times 2}$ and let $L = E(\sqrt{\alpha})$ for $\alpha \in E^\times \setminus E^{\times 2}$. The Galois closure group of $L/K$ is*

$$\begin{cases} V_4 & \text{if } N_{E/K}(\alpha) \in K^{\times 2}, \\ C_4 & \text{if } N_{E/K}(\alpha) \in dK^{\times 2}, \\ D_4 & \text{otherwise.} \end{cases}$$

**Proof.** Write $\alpha = a + b\sqrt{d}$ for $a, b \in K$ and let $\theta = \sqrt{\alpha}$. Let $m(X)$ be the minimal polynomial of $\theta$ over $K$. Let $N$ be a splitting field of $m(X)$ over $L$. The polynomial $m(X)$ has roots $\pm\theta, \pm\varphi$ for some element $\varphi \in N$.

We claim that $L/K$ is a $V_4$-extension if and only if $\theta\varphi \in K$. Suppose that $L/K$ is a $V_4$-extension. Since $L/K$ is the splitting field of $m(X)$, there are $\sigma, \tau \in \mathrm{Gal}(L/K)$ with $\sigma(\theta) = \varphi$ and $\tau(\theta) = -\theta$. These have order 2, so $\sigma(\theta\varphi) = \tau(\theta\varphi) = \theta\varphi$, and therefore $\theta\varphi \in K$. Suppose conversely that $\theta\varphi \in K$. Then $K(\theta) = K(\varphi)$, so $L$ is the splitting field of $m(X)$ over $K$, and therefore there are $\sigma, \tau \in \mathrm{Gal}(L/K)$ with $\sigma(\theta) = \varphi$ and $\tau(\theta) = -\theta$. Since $\theta\varphi \in K$, it is fixed by $\sigma$, so

$$\theta\varphi = \varphi\sigma(\varphi),$$

and therefore $\theta = \sigma(\varphi)$, so $\sigma$ has order 2. Clearly $\tau$ has order 2, so $\mathrm{Gal}(L/K) \cong V_4$.

Let $\lambda := \frac{\theta}{\varphi} - \frac{\varphi}{\theta}$. We claim that $L/K$ is a $C_4$-extension if and only if $\lambda \in K$. Suppose that $L/K$ is a $C_4$-extension. Then $\theta, \varphi \in L$, so there is a generator $\sigma \in \mathrm{Gal}(L/K)$ such

[3] If $u \equiv x^2 \pmod{\mathfrak{p}_E^{2t}}$, then $u/x^2 = 1 + \pi_E^{2t} y$ for some $y \in \mathcal{O}_E$. Taking $z \in \mathcal{O}_E$ with $y \equiv z^2 \pmod{\mathfrak{p}_E}$, we obtain $u/x^2 \equiv (1 + \pi_E^t z)^2 \pmod{\mathfrak{p}_E^{2t+1}}$.

that $\sigma(\theta) = \varphi$. It follows that $\sigma(\lambda) = \lambda$, so $\lambda \in K$. Suppose conversely that $\lambda \in K$. There is some element $\sigma \in \mathrm{Gal}(N/K)$ such that $\sigma(\theta) = \varphi$. It is easy to see that $\sigma^2(\theta) = \varepsilon\theta$ for some $\varepsilon \in \{\pm 1\}$. Since $\lambda \in K$, we have $\varepsilon = -1$, so $\sigma$ has order 4. Clearly $\theta^2 + \varphi^2 = 2a$, so

$$\lambda = \frac{2\theta^2 - 2a}{\theta\varphi},$$

which means that

$$\varphi = \frac{2\theta^2 - 2a}{\theta\lambda} \in L,$$

so $L/K$ is Galois and hence $C_4$ with Galois group $\langle\sigma\rangle$. Finally,

$$\lambda^2 = \frac{4b^2 d}{N_{E/K}(\alpha)},$$

and the result follows.

**Corollary 4.9.** *For $d \in K^\times \setminus K^{\times 2}$, the following are equivalent:*

1. *The extension $K(\sqrt{d})/K$ is $C_4$-extendable.*
2. *The element $d$ is a sum of two squares in $K$.*
3. *The element $d$ is in the norm group of the extension $K(\sqrt{-1})/K$.*

**Proof.** The equivalence of (1) and (2) follows from Lemma 4.8. If $-1 \in K^{\times 2}$, then (2) and (3) are equivalent because every element of $K$ can be written as a sum of two squares, due to the identity

$$d = \left(\frac{d+1}{2}\right)^2 + \left(\frac{d-1}{2\sqrt{-1}}\right)^2.$$

If $-1 \notin K^{\times 2}$, then the equivalence of (2) and (3) is trivial.

By symmetry of the quadratic Hilbert symbol, it follows from Corollary 4.9 that we need to count extensions $K(\sqrt{d})$ such that $-1 \in \mathrm{Nm}\, K(\sqrt{d})$. Our technique for doing this applies much more generally, to counting $K(\sqrt{d})$ such that $\mathcal{A} \subseteq \mathrm{Nm}\, K(\sqrt{d})$, where $\mathcal{A}$ is any subgroup of $K^\times/K^{\times 2}$. Since it does not require much additional theory, we opt to work at this more natural level of generality.

Let $F/K$ be an extension of 2-adic fields. For $1 \le t \le v_F(2)$, write

$$\begin{aligned} S_{F/K,t} &= (U_F^{(2t)} F^{\times 2} \cap K^\times)/K^{\times 2} \\ &= \{u \in K^\times/K^{\times 2} : u/x^2 \equiv 1 \pmod{\mathfrak{p}_F^{2t}} \text{ for some } x \in F^\times\}, \end{aligned}$$

and define

$$S_{F/K,0} = \{u \in K^\times/K^{\times 2} : v_F(u) \text{ is even}\}.$$

For a subgroup $\mathcal{A} \subseteq K^\times/K^{\times 2}$, let $K(\sqrt{\mathcal{A}})$ be the extension

$$K(\{\sqrt{\alpha} : [\alpha] \in \mathcal{A}\})$$

of $K$, write $\operatorname{Nm} K(\sqrt{\mathcal{A}})$ for its norm group, and define

$$\mathcal{O}_K^{\mathcal{A}} = \mathcal{O}_K^\times \cap \operatorname{Nm} K(\sqrt{\mathcal{A}}).$$

For $0 \leq t \leq e_K$, define the subgroup

$$S_{K/K,t}^{\mathcal{A}} = S_{K/K,t} \cap \left(\operatorname{Nm} K(\sqrt{\mathcal{A}})/K^{\times 2}\right).$$

For each $m_1$, let $\operatorname{Ext}_{2/K,\leq m_1}^{\mathcal{A}}$ be the set of $E \in \operatorname{Ext}_{2/K,\leq m_1}$ with $\mathcal{A} \subseteq \operatorname{Nm} E$.

**Lemma 4.10.** *Let $0 \leq t \leq e_K$ and let $\mathcal{A} \subseteq K^\times/K^{\times 2}$ be any subgroup. We have a bijection*

$$S_{K/K,t}^{\mathcal{A}} \to \operatorname{Ext}_{2/K,\leq 2e_K-2t}^{\mathcal{A}} \cup \{K\}, \quad u \mapsto K(\sqrt{u}).$$

**Proof.** By Corollary 4.7, the map $u \mapsto K(\sqrt{u})$ gives a well-defined bijection

$$\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2} \to \operatorname{Ext}_{2/K,\leq 2e_K} \cup \{K\}.$$

For $u \in \mathcal{O}_K^\times \setminus \mathcal{O}_K^{\times 2}$, we claim that the following two statements are true:

1. $K(\sqrt{u}) \in \operatorname{Ext}_{2/K,\leq 2e_K}^{\mathcal{A}}$ if and only if $u \in S_{K/K,0}^{\mathcal{A}}$.
2. $K(\sqrt{u}) \in \operatorname{Ext}_{2/K,\leq 2e_K-2t}$ if and only if $u \in S_{K/K,t}$.

The first statement follows from symmetry of the quadratic Hilbert symbol, and the second follows from Corollary 4.7. The result then follows, since

$$S_{K/K,t}^{\mathcal{A}} = S_{K/K,0}^{\mathcal{A}} \cap S_{K/K,t}.$$

For each $0 \leq t \leq e_K$, define the subgroup

$$(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}} \subseteq (\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times$$

to be the image of the map

$$\mathcal{O}_K^{\mathcal{A}} \to (\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times.$$

**Lemma 4.11.** *Let $0 \leq t \leq e_K$ and let $\mathcal{A} \subseteq K^\times/K^{\times 2}$ be any subgroup. There is a short exact sequence*

$$1 \to S^{\mathcal{A}}_{K/K,t} \to S^{\mathcal{A}}_{K/K,0} \to \frac{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}}{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\times 2}} \to 1.$$

**Proof.** This is immediate from the definitions.

**Lemma 4.12.** *For any subgroup $\mathcal{A} \subseteq K^\times/K^{\times 2}$, we have*

$$[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}}] = \frac{\#\mathcal{A}}{f(K(\sqrt{\mathcal{A}})/K)}.$$

**Proof.** Let $[\alpha_1], \dots, [\alpha_r] \in K^\times/K^{\times 2}$ be a minimal set of generators for $\mathcal{A}$, so that

$$K(\sqrt{\mathcal{A}}) = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r}).$$

By class field theory, we have

$$[K^\times : \operatorname{Nm} K(\sqrt{\mathcal{A}})] = 2^r = \#\mathcal{A}.$$

It follows that

$$[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}}] = \begin{cases} \#\mathcal{A} & \text{if there exists } x \in \operatorname{Nm}(K(\sqrt{\mathcal{A}})) \text{ with } v_K(x) = 1, \\ \frac{1}{2} \cdot \#\mathcal{A} & \text{otherwise,} \end{cases}$$

so we need to show that there exists $x \in \operatorname{Nm}(K(\sqrt{\mathcal{A}}))$ with $v_K(x) = 1$ if and only if $K(\sqrt{\mathcal{A}})/K$ is totally ramified. This follows from class field theory, since $K(\sqrt{\mathcal{A}})$ contains the unramified quadratic extension $E^{\mathrm{ur}}/K$ if and only if

$$\operatorname{Nm} K(\sqrt{\mathcal{A}}) \subseteq \operatorname{Nm} E^{\mathrm{ur}} = \{x \in K^\times : 2 \mid v_K(x)\}.$$

For each $0 \leq t \leq e_K$, let

$$\mathcal{A}_t = \mathcal{A} \cap \left(U_K^{(2t)} K^{\times 2}/K^{\times 2}\right).$$

**Lemma 4.13.** *Let $0 \leq t \leq e_K$ and let $\mathcal{A} \subseteq K^\times/K^{\times 2}$ be any subgroup. The extension $K(\sqrt{\mathcal{A}})/K$ is totally ramified if and only if $K(\sqrt{\mathcal{A}_t})/K$ is totally ramified.*

**Proof.** Suppose that $K(\sqrt{\mathcal{A}})/K$ is not totally ramified. Then we have $[u] \in \mathcal{A}$, where $[u] \in K^\times/K^{\times 2}$ is the unique element such that $K(\sqrt{u})/K$ is unramified. In that case, Corollary 4.7 tells us that $u \in \mathcal{A}_t$, so $K(\sqrt{\mathcal{A}_t})/K$ is not totally ramified.

Suppose conversely that $K(\sqrt{\mathcal{A}_t})/K$ is not totally ramified. Since $\mathcal{A}_t \subseteq \mathcal{A}$, we have $K(\sqrt{\mathcal{A}_t}) \subseteq K(\sqrt{\mathcal{A}})$, so $K(\sqrt{\mathcal{A}})$ is not totally ramified.

**Lemma 4.14.** *Let $0 \leq t \leq e_K$ and let $\mathcal{A} \subseteq K^\times/K^{\times 2}$ be any subgroup. We have*

$$\mathcal{O}_K^{\mathcal{A}_t} = \mathcal{O}_K^{\mathcal{A}} U_K^{(2e_K-2t)}.$$

**Proof.** First we claim that

$$\operatorname{Nm} K(\sqrt{\mathcal{A}_t}) = U_K^{(2e_K-2t)} \operatorname{Nm} K(\sqrt{\mathcal{A}}).$$

For $[\alpha] \in \mathcal{A}_t$, Corollary 4.7 tells us that $v_K(d_{K(\sqrt{\alpha})/K}) \leq 2e_K - 2t$, so we have the inclusion $U_K^{(2e_K-2t)} \subseteq \operatorname{Nm} K(\sqrt{\alpha})$, and therefore

$$U_K^{(2e_K-2t)} \subseteq \operatorname{Nm} K(\sqrt{\mathcal{A}_t}).$$

Since $\mathcal{A}_t \subseteq \mathcal{A}$, class field theory tells us that

$$\operatorname{Nm} K(\sqrt{\mathcal{A}}) \subseteq \operatorname{Nm} K(\sqrt{\mathcal{A}_t}),$$

and therefore

$$U_K^{(2e_K-2t)} \operatorname{Nm} K(\sqrt{\mathcal{A}}) \subseteq \operatorname{Nm} K(\sqrt{\mathcal{A}_t}).$$

Suppose that

$$U_K^{(2e_K-2t)} \operatorname{Nm} K(\sqrt{\mathcal{A}}) \subseteq G \subseteq \operatorname{Nm} K(\sqrt{\mathcal{A}_t}),$$

for a subgroup $G$ of $K^\times$. By class field theory, there is a unique abelian extension $L/K$ such that $\operatorname{Nm} L = G$. We have

$$K(\sqrt{\mathcal{A}_t}) \subseteq L \subseteq K(\sqrt{\mathcal{A}}),$$

so

$$L = K(\sqrt{\mathcal{B}})$$

for some subgroup $\mathcal{B} \leq \mathcal{A}$. Let $[\beta] \in \mathcal{B}$. Since $U_K^{(2e_K-2t)} \subseteq \operatorname{Nm} L \subseteq \operatorname{Nm} K(\sqrt{\beta})$, we have $v_K(d_{K(\sqrt{\beta})/K}) \leq 2e_K - 2t$, so Corollary 4.7 tells us that $\beta \in U_K^{(2t)} K^{\times 2}$, and therefore $[\beta] \in \mathcal{A}_t$. It follows that $\mathcal{B} \subseteq \mathcal{A}_t$, and therefore $L \subseteq K(\sqrt{\mathcal{A}_t})$, so $G = \operatorname{Nm} K(\sqrt{\mathcal{A}_t})$. Therefore, as claimed, we have

$$\operatorname{Nm} K(\sqrt{\mathcal{A}_t}) = U_K^{(2e_K-2t)} \operatorname{Nm} K(\sqrt{\mathcal{A}}).$$

It follows that

$$\mathcal{O}_K^{\mathcal{A}_t} = \left(U_K^{(2e_K-2t)} \operatorname{Nm} K(\sqrt{\mathcal{A}})\right) \cap \mathcal{O}_K^\times,$$

so we need to show that

$$\left(U_K^{(2e_K-2t)}\operatorname{Nm} K(\sqrt{\mathcal{A}})\right)\cap\mathcal{O}_K^\times = U_K^{(2e_K-2t)}\left(\operatorname{Nm} K(\sqrt{\mathcal{A}})\cap\mathcal{O}_K^\times\right),$$

which is an easy exercise in definitions.

**Lemma 4.15.** *Let $1\le t\le e_K$ and let $\mathcal{A}\subseteq K^\times/K^{\times 2}$ be any subgroup. There is a short exact sequence*

$$1\to\mathcal{O}_K^{\mathcal{A}_{e_K-t}}\to\mathcal{O}_K^\times\to\frac{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times}{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}}\to 1.$$

**Proof.** Clearly the map $\varphi:\mathcal{O}_K^\times\to\frac{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times}{(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}}$ is well-defined and surjective. It follows from the definitions that

$$\ker\varphi=\mathcal{O}_K^{\mathcal{A}}U_K^{(2t)},$$

so the result follows from Lemma 4.14.

**Lemma 4.16.** *For any subgroup $\mathcal{A}\subseteq K^\times/K^{\times 2}$, we have*

$$\#\mathcal{A}_{e_K}=f(K(\sqrt{\mathcal{A}})/K).$$

**Proof.** Lemma 4.6 tells us that $U_K^{(2e_K)}K^{\times 2}/K^{\times 2}=\{1,[u]\}$, where $K(\sqrt{u})/K$ is the unique unramified quadratic extension. It follows that

$$\mathcal{A}_{e_K}=\begin{cases}\{[1],[u]\} & \text{if } K(\sqrt{u})\subseteq K(\sqrt{\mathcal{A}}),\\ \{[1]\} & \text{otherwise,}\end{cases}$$

and the result follows.

**Lemma 4.17.** *Let $0\le t\le e_K$ and let $\mathcal{A}\subseteq K^\times/K^{\times 2}$ be any subgroup. We have*

$$\#S_{K/K,t}^{\mathcal{A}}=2q^{e_K-t}\cdot\frac{\#\mathcal{A}_{e_K-t}}{\#\mathcal{A}}.$$

**Proof.** It follows from Lemma 4.11 that

$$\#S_{K/K,t}^{\mathcal{A}}=\frac{\#S_{K/K,0}^{\mathcal{A}}\#(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\times 2}}{\#(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}}.$$

By [Neu13, Proposition 3.7], we have $[\mathcal{O}_K^\times:\mathcal{O}_K^{\times 2}]=2q^{e_K}$, so the definition of $S_{K/K,0}^{\mathcal{A}}$ gives

$$\#S^{\mathcal{A}}_{K/K,0} = \frac{2q^{e_K}}{[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}}]}.$$

The result for $t = 0$ then follows from Lemmas 4.12 and 4.16. Now assume that $t \geq 1$. Lemma 4.15 tells us that

$$\frac{1}{\#(\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\mathcal{A}}} = \frac{[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}_{e_K-t}}]}{\#(\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times}.$$

It follows that

$$\#S^{\mathcal{A}}_{K/K,t} = \frac{2q^{e_K}}{[(\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times : (\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\times 2}]} \cdot \frac{[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}_{e_K-t}}]}{[\mathcal{O}_K^\times : \mathcal{O}_K^{\mathcal{A}}]}.$$

The short exact sequence

$$1 \to U_K^{(t)}/U_K^{(2t)} \xrightarrow{[u]\mapsto[u]} (\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times \xrightarrow{[u]\mapsto[u^2]} (\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\times 2} \to 1$$

tells us that $[(\mathcal{O}_K/\mathfrak{p}_K^{2t})^\times : (\mathcal{O}_K/\mathfrak{p}_K^{2t})^{\times 2}] = q^t$. Finally, the result follows from Lemmas 4.12 and 4.13.

**Corollary 4.18.** *Let $0 \leq m_1 \leq 2e_K$ be an even integer and let $\mathcal{A} \subseteq K^\times/K^{\times 2}$ be any subgroup. Then*

$$\#\mathrm{Ext}^{\mathcal{A}}_{2/K,\leq m_1} = 2q^{m_1/2} \cdot \frac{\#\mathcal{A}_{m_1/2}}{\#\mathcal{A}} - 1.$$

**Proof.** This is immediate from Lemmas 4.10 and 4.17.

**Corollary 4.19.** *Let $m_1$ be an even integer with $2 \leq m_1 \leq 2e_K$. We have*

$$\#\mathrm{Ext}^{\uparrow C_4}_{2/K,\leq m_1} = (1 + \mathbb{1}_{m_1 \leq 2e_K - d_{(-1)}}) \cdot q^{m_1/2} - 1.$$

**Proof.** Let $\mathcal{A} = \langle [-1] \rangle \subseteq K^\times/K^{\times 2}$. Corollary 4.9 tells us that

$$\mathrm{Ext}^{\uparrow C_4}_{2/K,\leq m_1} = \mathrm{Ext}^{\mathcal{A}}_{2/K,\leq m_1},$$

and it follows by Corollary 4.18 that

$$\mathrm{Ext}^{\uparrow C_4}_{2/K,\leq m_1} = 2q^{m_1/2} \cdot \frac{\#\mathcal{A}_{m_1/2}}{\#\mathcal{A}} - 1.$$

Suppose first that $-1 \in K^{\times 2}$. Then $[-1] = [1]$, so $\#\mathcal{A} = \#\mathcal{A}_{m_1/2} = 1$, and the result follows since $d_{(-1)} = 0$.

Suppose instead that $-1 \notin K^{\times 2}$. Then

$$\#\mathcal{A} = 2,$$

and (by Corollary 4.7)

$$\#\mathcal{A}_{m_1/2} = 1 + \mathbb{1}_{d_{(-1)} \leq 2e_K - m_1},$$

and the result follows.

**Proof** *(Proof of Lemma 4.2).* The first claim follows from the classification of quadratic extensions in [Tun78, Lemma 4.3]. The result for $2 \leq m_1 \leq 2e_K$ follows from Corollary 4.19. By Lemma 4.6, for any quadratic extension $E/K$, we have $v_K(d_{E/K}) = 2e_K + 1$ if and only if $E = K(\sqrt{\alpha})$ for some $\alpha \in K^\times$ with $v_K(\alpha) = 1$. Assume that this is the case. Then Corollary 4.9 tells us that $E/K$ is $C_4$-extendable if and only if $\alpha$ is in the norm group of $K(\sqrt{-1})/K$, and the result follows by basic class field theory.

**Lemma 4.20.** *The constant $d_{(-1)}$ is an even integer with*

$$d_{(-1)} \leq 2\left\lceil \frac{e_K}{2} \right\rceil.$$

**Proof.** This follows from Corollary 4.7, along with the trivial fact that

$$-1 \equiv 1 \pmod{\mathfrak{p}_K^{e_K}}.$$

*4.3. Counting $C_4$-extensions with a given intermediate field*

**Lemma 4.21.** *Let $E = K(\sqrt{d})$ be a totally ramified $C_4$-extendable extension of $K$ with $m_1 = v_K(d_{E/K})$, and let $0 \leq m_2 \leq 4e_K$ be an even integer. The following are equivalent:*

1. *The set $\mathrm{Ext}^{C_4/K}_{2/E,\leq m_2}$ is nonempty.*
2. *There is some $\beta \in \mathcal{O}_E^\times$ such that $\beta \equiv 1 \pmod{\mathfrak{p}_E^{4e_K - m_2}}$ and $N_{E/K}(\beta) \in dK^{\times 2}$.*
3. *We have $m_2 \geq \min\{m_1 + 2e_K, 3m_1 - 2\}$.*

**Proof.** The first two points are equivalent by Corollary 4.7 and Lemma 4.8. The equivalence of (2) and (3) is essentially [CDO05, Proposition 3.15]. At the start of the proof, the authors state that their "condition $(*)$" is equivalent to (2), and the statement of their proposition is equivalent to (3), where $t = 2e_K - \frac{m_2}{2}$. Their result is stated for prime ideals of number fields lying over 2, but it is trivial to check that the proof works for 2-adic fields.

**Lemma 4.22.** *Let $E/K$ be a totally ramified $C_4$-extendable extension, and suppose that $0 \leq m_2 \leq 4e_K$ is an even integer such that $\mathrm{Ext}_{2/E,\leq m_2}^{C_4/K}$ is nonempty. Let $\omega \in E$ such that $E(\sqrt{\omega}) \in \mathrm{Ext}_{2/E,\leq m_2}^{C_4/K}$. Then the map*

$$K^\times/K^{\times 2} \to \mathrm{Ext}_{2/E}^{C_4/K}, \quad u \mapsto E(\sqrt{u\omega})$$

*is surjective and 2-to-1. Moreover, this map restricts to a surjective 2-to-1 map*

$$S_{E/K,2e_K-\frac{m_2}{2}} \to \mathrm{Ext}_{2/E,\leq m_2}^{C_4/K}.$$

**Proof.** The first claim is [CDO05, Proposition 1.2], and the second claim follows from Corollary 4.7.

Fix a totally ramified quadratic extension $E/K$ with $m_1 = v_K(d_{E/K})$, and assume that $m_1$ is even. For $0 \leq t \leq 2e_K - \frac{m_1}{2}$, define $\mathcal{Z}_{E,t}$ by the short exact sequence

$$1 \to S_{E/K,t} \to K^\times/K^{\times 2} \to \mathcal{Z}_{E,t} \to 1.$$

**Lemma 4.23.** *Let $E$ be a totally ramified quadratic extension of $K$ with even discriminant exponent $m_1 = v_K(d_{E/K})$. Let $m_2$ be an even integer with $m_1 \leq m_2 \leq 4e_K$. Then we have:*

1.
$$\#\mathcal{Z}_{E,2e_K-\frac{m_2}{2}} = \begin{cases} 2q^{\lceil e_K - \frac{m_1+m_2}{4} \rceil} & \text{if } m_2 \leq 4e_K - m_1, \\ 1 & \text{if } m_2 > 4e_K - m_1. \end{cases}$$

2.
$$\#S_{E/K,2e_K-\frac{m_2}{2}} = \begin{cases} 2q^{\lfloor \frac{m_1+m_2}{4} \rfloor} & \text{if } m_2 \leq 4e_K - m_1, \\ 4q^{e_K} & \text{if } m_2 > 4e_K - m_1. \end{cases}$$

**Proof.**

1. For $m_2 = 4e_K$, we have $\mathcal{Z}_{E,2e_K-\frac{m_2}{2}} = 1$, so we can assume that $m_1 \leq m_2 \leq 4e_K - 2$. The claim is then essentially [CDO05, Corollary 3.13]. Under our notation, $\mathcal{Z}_{E,t}$ corresponds[4] to Cohen, Diaz y Diaz, and Olivier's $\mathcal{Z}_{\mathfrak{P}^{2t}}$, defined in [CDO05, Page 486]. As with Lemma 4.21, the statement in [CDO05] is for prime ideals of number fields, but the modifications to the proof are trivial.
2. The second claim follows from the first, together with the definition of $\mathcal{Z}_{E,t}$, and [Neu13, Proposition 3.7].

[4] In [CDO05], here are the locations of the relevant definitions: $\mathcal{Z}_{\mathfrak{C}^2}$ is defined on Page 486; $Q_K(\mathfrak{C}^2)$ is defined on Page 479; $\mathfrak{C}$ is defined on Page 478; $T$ is defined on Page 478; the angle brackets $\langle T \rangle$ denote the monoid of ideals generated by $T$ - this can be inferred from the proof of Lemma 1.6.

**Corollary 4.24.** *Let $E/K$ be a totally ramified $C_4$-extendable extension such that the discriminant valuation $m_1 = v_K(d_{E/K})$ is even. Let $m_2 \leq 4e_K$ be an even integer and write $n_0 := \min\{m_1 + 2e_K, 3m_1 - 2\}$. Then we have*

$$\#\mathrm{Ext}^{C_4/K}_{2/E,\leq m_2} = \begin{cases} 0 & \text{if } m_2 < n_0, \\ q^{\lfloor \frac{m_1+m_2}{4} \rfloor} & \text{if } n_0 \leq m_2 \leq 4e_K - m_1, \\ 2q^{e_K} & \text{if } m_2 \geq \max\{4e_K - m_1 + 2, n_0\}. \end{cases}$$

**Proof.** Lemma 4.21 deals with the case $m_2 < n_0$. Let $n_0 \leq m_2 \leq 4e_K$. By Lemma 4.21, the set $\mathrm{Ext}^{C_4/K}_{2/E,\leq m_2}$ is nonempty, so Lemma 4.22 tells us that

$$\#\mathrm{Ext}^{C_4/K}_{2/E,\leq m_2} = \frac{1}{2}\#S_{E/K,2e_K-\frac{m_2}{2}},$$

and the result follows from Lemma 4.23.

**Proof** *(Proof of Lemma 4.4).* By [Tun78, Lemma 4.3], either $m_1 = 2e_K + 1$ or $m_1$ is even with $2 \leq m_1 \leq 2e_K$. The case where $m_1$ is even follows easily from Corollary 4.24. For the case with $m_1$ odd, suppose that $m_1 = 2e_K + 1$. Then by Lemma 4.6 we have $E = K(\sqrt{d})$ for $d \in K^\times$ with $v_K(d) = 1$. By Lemma 4.8, each $C_4$-extension $L/K$ extending $E$ has $L = E(\sqrt{\alpha})$ for some $\alpha \in E^\times$ with $v_K(N_{E/K}(\alpha))$ odd. It follows that $v_E(\alpha)$ is odd, so $v_E(d_{L/E}) = 4e_K + 1$ by Lemma 4.6. Therefore,

$$\mathrm{Ext}^{C_4/K}_{2/E} = \mathrm{Ext}^{C_4/K}_{2/E,4e_K+1},$$

so the result follows from Lemma 4.22.

**Proof** *(Proof of Corollary 4.5).* Suppose that $L/K$ is a $C_4$-extension with intermediate quadratic field $E$. By the tower law for discriminant, we have

$$v_K(d_{L/K}) = 2v_K(d_{E/K}) + f(E/K) \cdot v_E(d_{L/E}).$$

So if $L \in \Sigma_m^{C_4}$ with $m_1 = v_K(d_{E/K})$ and $m_2 = v_E(d_{L/E})$, then $m = 2m_1 + m_2$, and Lemmas 4.2 and 4.4 tell us that either $(m_1, m_2) = (2e_K + 1, 4e_K + 1)$ or $m_1$ and $m_2$ are both even with $2 \leq m_1 \leq 2e_K$ and $4 \leq m_2 \leq 4e_K$. It follows that either $m$ is even with $8 \leq m \leq 8e_K$ or $m = 8e_K + 3$. If $m = 8e_K + 3$, then the result follows from Lemmas 4.2 and 4.4.

Now consider the case where $8 \leq m \leq 8e_K$ and $m$ is even. For positive integers $m_1$ and $m_2$, write $\Sigma^{C_4}_{m_1,m_2}$ for the set of totally ramified $C_4$-extensions $L/K$ such that $v_K(d_{E/K}) = m_1$ and $v_E(d_{L/E}) = m_2$. By the discussion above, we have

$$\#\Sigma_m^{C_4} = \sum_{\substack{2\leq m_1\leq 2e_K \\ m_1 \text{ even}}} \#\Sigma^{C_4}_{m_1,m-2m_1}.$$

Let $2 \leq m_1 \leq 2e_K$ be even. By Lemmas 4.2 and 4.4, whenever $N_{\text{ext}}(m_1) \neq 0$ we have

$$\frac{\#\Sigma^{C_4}_{m_1,m-2m_1}}{N_{\text{ext}}(m_1)} = \begin{cases} q^{m_1-1} & \text{if } m_1 = \frac{m+2}{5} \text{ and } m_1 \leq e_K, \\ q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} & \text{if } m - 4e_K \leq m_1 \leq \min\{\frac{m}{5}, e_K\}, \\ q^{e_K} & \text{if } m_1 = m - 4e_K - 2 \text{ and } m_1 \leq e_K, \\ 2q^{e_K} & \text{if } e_K < m_1 \leq 2e_K \text{ and } m_1 = \frac{m-2e_K}{3}, \\ 0 & \text{otherwise.} \end{cases}$$

$$= \begin{cases} q^{\frac{m-3}{5}} & \text{if } m_1 = \frac{m+2}{5} \text{ and } 8 \leq m \leq 5e_K - 2, \\ q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} & \text{if } m - 4e_K \leq m_1 \leq \min\{\frac{m}{5}, e_K\}, \\ q^{e_K} & \text{if } m_1 = m - 4e_K - 2 \text{ and } 4e_K + 4 \leq m \leq 5e_K + 2, \\ 2q^{e_K} & \text{if } m_1 = \frac{m-2e_K}{3} \text{ and } 5e_K < m \leq 8e_K, \\ 0 & \text{otherwise.} \end{cases}$$

To finish the proof, we just need to observe that

$$q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} = \begin{cases} q^{\frac{m-m_1}{4}-1}(q-1) & \text{if } m_1 \equiv m \pmod 4, \\ 0 & \text{if } m_1 \not\equiv m \pmod 4. \end{cases}$$

**Proof** *(Proof of Theorem 1.4).* The possible values of $m$ come from Corollary 4.5. The result for $m = 8e_K + 3$ is immediate from Corollary 4.5. Now consider the case where $m$ is even and $8 \leq m \leq 8e_K$. The first, third, and fourth items of Corollary 4.5 respectively are equal to

1. $\mathbb{1}_{8\leq m\leq 5e_K-2} \cdot \mathbb{1}_{m\equiv 3 \pmod 5} \cdot q^{\frac{3m-14}{10}}(1+\mathbb{1}_{m\leq 10e_K-5d_{(-1)}-2})(q-1-\mathbb{1}_{m=10e_K-5d_{(-1)}+8})$.
2. $\mathbb{1}_{4e_K+4\leq m\leq 5e_K+2} \cdot q^{\frac{m}{2}-e_K-2}(1+\mathbb{1}_{m\leq 6e_K-d_{(-1)}+2})(q-1-\mathbb{1}_{m=6e_K-d_{(-1)}+4})$.
3. $\mathbb{1}_{5e_K+3\leq m\leq 8e_K} \cdot \mathbb{1}_{m\equiv 2e_K \pmod 3} \cdot 2q^{\frac{m+4e_K}{6}-1}(1+\mathbb{1}_{m\leq 8e_K-3d_{(-1)}})(q-1-\mathbb{1}_{m=8e_K-3d_{(-1)}+6})$.

Lemma 4.20 turns these into the first three points of Theorem 1.4. It remains to compute the value of

$$\sum_{\substack{\max\{2,m-4e_K\}\leq m_1\leq \min\{\frac{m}{5},e_K\} \\ m_1\equiv m \pmod 4}} q^{\frac{m-m_1}{4}-1}(q-1)N_{\text{ext}}(m_1).$$

For such $m_1$, we have

$$N_{\text{ext}}(m_1) = \begin{cases} 2q^{\frac{m_1}{2}-1}(q-1) & \text{if } m_1 \leq 2e_K - d_{(-1)}, \\ q^{\frac{m_1}{2}-1}(q-2) & \text{if } m_1 = 2e_K - d_{(-1)} + 2, \\ q^{\frac{m_1}{2}-1}(q-1) & \text{if } m_1 \geq 2e_K - d_{(-1)} + 4. \end{cases}$$

Lemma 4.20 tells us that $2e_K - d_{(-1)} + 2 > e_K$, so the sum is actually

$$\sum_{\substack{\max\{2,m-4e_K\}\leq m_1\leq \min\{\frac{m}{5},e_K\}\\ m_1\equiv m \pmod 4}} 2q^{\frac{m+m_1}{4}-2}(q-1)^2.$$

For integers $l$ and $u$, the substitution $m_1 = -m + 4k$ makes it easy to see that

$$\sum_{\substack{l\leq m_1\leq u\\ m_1\equiv m \pmod 4}} q^{\frac{m+m_1}{4}} = \mathbb{1}_{l\leq u}\cdot \frac{q^{b+1}-q^a}{q-1},$$

where $a = \lceil \frac{m+l}{4} \rceil$ and $b = \lfloor \frac{m+u}{4} \rfloor$. In this case, we have $l = \max\{2, m-4e_K\}$ and $u = \min\{e_K, \frac{m}{5}\}$, which gives

$$a = \lceil \max\{\frac{m+2}{4}, \frac{m}{2} - e_K\}\rceil, \quad b = \lfloor \min\{\frac{m+e_K}{4}, \frac{3m}{10}\}\rfloor.$$

Finally, it is easy to see that $l \leq u$ if and only if $10 \leq m \leq 5e_K$. In that case, we have $b = \lfloor \frac{3m}{10} \rfloor$, so

$$\sum_{\substack{\max\{2,m-4e_K\}\leq m_1\leq \min\{e_K,\frac{m}{5}\}\\ m_1\equiv m \pmod 4}} q^{\frac{m+m_1}{4}} = \mathbb{1}_{10\leq m\leq 5e_K}\cdot \frac{q^{\lfloor \frac{3m}{10}\rfloor+1} - q^{\lceil \max\{\frac{m+2}{4}, \frac{m}{2}-e_K\}\rceil}}{q-1},$$

and the result follows.

**Proof** *(Proof of Corollary 1.9).* Theorem 1.4 and Lemma 4.20 tell us that the mass is the sum of the following quantities:

1. $$\frac{1}{2}\cdot \sum_{\substack{8\leq m\leq 5e_K-2\\ m\equiv 8 \pmod{10}}} q^{-\frac{7m+14}{10}}(q-1).$$

2. $$\frac{1}{2}\cdot \sum_{\substack{4e_K+4\leq m\leq 5e_K+2\\ m \text{ even}}} q^{-\frac{m}{2}-e_K-2}(q-1).$$

3. (a) $$\sum_{\substack{5e_K+3\leq m\leq 8e_K-3d_{(-1)}\\ m\equiv 2e_K \pmod 6}} q^{\frac{4e_K-5m}{6}-1}(q-1).$$

   (b) $$\mathbb{1}_{d_{(-1)}\geq 2}\cdot \frac{1}{2}\cdot q^{-6e_K+\frac{5}{2}d_{(-1)}-6}(q-2).$$

   (c) $$\frac{1}{2}\cdot \sum_{\substack{8e_K-3d_{(-1)}+12\leq m\leq 8e_K\\ m\equiv 2e_K \pmod 6}} q^{\frac{4e_K-5m}{6}-1}(q-1).$$

4. (a)
$$\frac{1}{2}(q-1)q^{-1}\sum_{\substack{10\le m\le 5e_K\\ m \text{ even}}} q^{\lfloor -\frac{7m}{10}\rfloor}.$$

(b)
$$-\frac{1}{2}(q-1)q^{-2}\sum_{\substack{10\le m\le 5e_K\\ m \text{ even}}} q^{\max\{\lceil\frac{-3m+2}{4}\rceil,-\frac{m}{2}-e_K\}}.$$

5.
$$\begin{cases} q^{-6e_K-3} & \text{if } -1\in K^{\times 2},\\ \frac{1}{2}q^{-6e_K-3} & \text{if } K(\sqrt{-1})/K \text{ is quadratic and totally ramified},\\ 0 & \text{otherwise.}\end{cases}$$

We address these one by one.

1. Making the substitution $m=10k+8$, we have
$$\sum_{\substack{8\le m\le 5e_K-2\\ m\equiv 8 \pmod{10}}} q^{-\frac{7m+14}{10}} = \mathbb{1}_{e_K\ge 2}\cdot\frac{1-q^{-7\lfloor\frac{e_K}{2}\rfloor}}{q^7-1},$$
so the contribution to the mass is
$$\frac{1}{2}\cdot\mathbb{1}_{e_K\ge 2}\cdot\frac{(q-1)(1-q^{-7\lfloor\frac{e_K}{2}\rfloor})}{q^7-1},$$
and we can omit the indicator function since $e_K=1$ gives $1-q^{-7\lfloor\frac{e_K}{2}\rfloor}=0$.
2. Making the substitution $m=2k$, it is easy to see that
$$\sum_{\substack{4e_K+4\le m\le 5e_K+2\\ m \text{ even}}} q^{-\frac{m}{2}} = \mathbb{1}_{e_K\ge 2}\cdot\frac{q^{-2e_K-1}-q^{-\lfloor\frac{5e_K+2}{2}\rfloor}}{q-1},$$
so the contribution is
$$\frac{1}{2}\cdot(q^{-3e_K-3}-q^{-\lfloor\frac{7e_K+6}{2}\rfloor}) = \frac{1}{2}\cdot q^{-3e_K-3}(1-q^{-\lfloor\frac{e_K}{2}\rfloor}),$$
where we omit the indicator function since $e_K=1$ gives $q^{-2e_K-1}-q^{-\lfloor\frac{5e_K+2}{2}\rfloor}=0$.
3. (a) The substitution $m=2e_K+6k$ gives
$$\sum_{\substack{5e_K+3\le m\le 8e_K-3d_{(-1)}\\ m\equiv 2e_K \pmod 6}} q^{\frac{4e_K-5m}{6}} = \mathbb{1}_{d_{(-1)}<e_K}\frac{q^{-5\lfloor\frac{e_K}{2}\rfloor-e_K}-q^{\frac{5}{2}d_{(-1)}-6e_K}}{q^5-1},$$
so the contribution is

$$\mathbb{1}_{d_{(-1)}<e_K} \cdot \frac{(q-1)(q^{-5\lfloor \frac{e_K}{2} \rfloor - e_K - 1} - q^{\frac{5}{2}d_{(-1)} - 6e_K - 1})}{q^5 - 1}.$$

(b) This is already in closed form.

(c) The substitution $m = 2e_K + 6k$ gives

$$\sum_{\substack{8e_K - 3d_{(-1)} + 12 \leq m \leq 8e_K \\ m \equiv 2e_K \pmod 6}} q^{\frac{4e_K - 5m}{6}} = \mathbb{1}_{d_{(-1)} \geq 4} \cdot \frac{q^{\frac{5}{2}d_{(-1)} - 6e_K - 5} - q^{-6e_K}}{q^5 - 1}.$$

Therefore, the contribution is

$$\frac{1}{2} \cdot \mathbb{1}_{d_{(-1)} \geq 4} \cdot \frac{(q-1)(q^{\frac{5}{2}d_{(-1)} - 6e_K - 6} - q^{-6e_K - 1})}{q^5 - 1}.$$

4. (a) We need to compute

$$\sum_{\substack{10 \leq m \leq 5e_K \\ m \text{ even}}} q^{\lfloor \frac{-7m}{10} \rfloor} = \sum_{k=5}^{\lfloor \frac{5e_K}{2} \rfloor} q^{-\lceil \frac{7k}{5} \rceil}.$$

For an integer $b \geq 1$, it is easy to see that

$$\sum_{k=5}^{5b} q^{-\lceil \frac{7k}{5} \rceil} = \frac{(q^{-6} - q^{1-7b})(q^6 + q^4 + q^3 + q + 1)}{q^7 - 1} + q^{-7b}.$$

If $e_K$ is even, then we have

$$\begin{aligned} \sum_{k=5}^{\lfloor \frac{5e_K}{2} \rfloor} q^{-\lceil \frac{7k}{5} \rceil} &= \sum_{k=5}^{5 \cdot \frac{e_K}{2}} q^{-\lceil \frac{7k}{5} \rceil} \\ &= \mathbb{1}_{e_K \geq 2} \cdot \Big( \frac{(q^{-6} - q^{1 - \frac{7e_K}{2}})(q^6 + q^4 + q^3 + q + 1)}{q^7 - 1} + q^{-\frac{7e_K}{2}} \Big). \end{aligned}$$

If $e_K$ is odd, then we have

$$\begin{aligned} \sum_{k=5}^{\lfloor \frac{5e_K}{2} \rfloor} q^{-\lceil \frac{7k}{5} \rceil} &= \Big( \sum_{k=5}^{5 \cdot \frac{e_K - 1}{2}} q^{-\lceil \frac{7k}{5} \rceil} \Big) + q^{-\lceil \frac{7}{5} \cdot \frac{5e_K - 3}{2} \rceil} + q^{-\lceil \frac{7}{5} \cdot \frac{5e_K - 1}{2} \rceil} \\ &= \mathbb{1}_{e_K \geq 2} \cdot \Big( \frac{(q^{-6} - q^{1 - 7 \cdot \frac{e_K - 1}{2}})(q^6 + q^4 + q^3 + q + 1)}{q^7 - 1} + q^{-7 \cdot \frac{e_K - 1}{2}} \\ &\qquad + q^{-7 \cdot \frac{e_K - 1}{2} - 2} + q^{-7 \cdot \frac{e_K - 1}{2} - 3} \Big). \end{aligned}$$

In other words, the sum $\sum_{k=5}^{\lfloor \frac{5e_K}{2} \rfloor} q^{-\lceil \frac{7k}{5} \rceil}$ is equal to

$$\mathbb{1}_{e_K\geq 2}\cdot\Big(\frac{(q^{-6}-q^{1-7\lfloor\frac{e_K}{2}\rfloor})(q^6+q^4+q^3+q+1)}{q^7-1}+q^{-7\lfloor\frac{e_K}{2}\rfloor}(1+\mathbb{1}_{2\nmid e_K}(q^{-2}+q^{-3}))\Big),$$

and therefore we have a contribution of

$$\mathbb{1}_{e_K\geq 2}\cdot\frac{1}{2}(q-1)\Big(\frac{(q^{-7}-q^{-7\lfloor\frac{e_K}{2}\rfloor})(q^6+q^4+q^3+q+1)}{q^7-1}$$
$$+q^{-7\lfloor\frac{e_K}{2}\rfloor-1}(1+\mathbb{1}_{2\nmid e_K}(q^{-2}+q^{-3}))\Big).$$

(b) We need to evaluate

$$\sum_{k=5}^{\lfloor\frac{5e_K}{2}\rfloor}q^{\max\{\lceil\frac{-3k+1}{2}\rceil,-k-e_K\}}=\sum_{k=5}^{2e_K}q^{\lceil\frac{-3k+1}{2}\rceil}+\sum_{k=2e_K+1}^{\lfloor\frac{5e_K}{2}\rfloor}q^{-k-e_K}.$$

We have

$$\sum_{k=5}^{2e_K}q^{\lceil\frac{-3k+1}{2}\rceil}=\mathbb{1}_{e_K\geq 3}\cdot\frac{(q^2+q)(q^{-6}-q^{-3e_K})}{q^3-1},$$

so the first half of the sum gives a contribution of

$$-\mathbb{1}_{e_K\geq 2}\cdot\frac{1}{2}\cdot\frac{(q-1)(q+1)(q^{-7}-q^{-3e_K-1})}{q^3-1}.$$

We also have

$$\sum_{k=2e_K+1}^{\lfloor\frac{5e_K}{2}\rfloor}q^{-k-e_K}=\mathbb{1}_{e_K\geq 2}\cdot\frac{q^{-3e_K}-q^{-\lfloor\frac{5e_K}{2}\rfloor-e_K}}{q-1},$$

so we also get a contribution of

$$-\frac{1}{2}(q^{-3e_K-2}-q^{-\lfloor\frac{7e_K}{2}\rfloor-2}).$$

## 5. The case $G=D_4$

For $G\in\{V_4,C_4,D_4\}$ and $L\in\Sigma^G$, let

$$\mathrm{Ext}_{2/K}^{\hookrightarrow L}:=\{E\in\mathrm{Ext}_{2/K}:\exists K\text{-morphism } E\hookrightarrow L\}.$$

Let $L\in\Sigma^G$ and $E\in\mathrm{Ext}_{2/K}^{\hookrightarrow L}$. There is a unique embedding $E\hookrightarrow L$, so we may naturally view $L$ as an extension of $E$. We define a *$K$-twist of $L/E$* to be an element of the set

$$\mathrm{Twist}_K(L/E)=\{L'\in\mathrm{Ext}_{2/E}:\exists K\text{-isomorphism } L'\cong L\}.$$

**Lemma 5.1.** *Let $G \in \{V_4, C_4, D_4\}$. The following two statements are true:*

1. *For $L \in \Sigma^G$, we have*

$$\#\mathrm{Ext}_{2/K}^{\hookrightarrow L} = \begin{cases} 1 & \text{if } G \in \{C_4, D_4\}, \\ 3 & \text{if } G = V_4. \end{cases}$$

2. *For $L \in \Sigma^G$ and $E \in \mathrm{Ext}_{2/K}^{\hookrightarrow L}$, we have*

$$\#\,\mathrm{Twist}_K(L/E) = \begin{cases} 1 & \text{if } G \in \{C_4, V_4\}, \\ 2 & \text{if } G = D_4. \end{cases}$$

**Proof.** Claim (1) is obvious. For Claim (2), write $E = K(\sqrt{d})$ and $L = E(\sqrt{\alpha})$, where $d \in K$ and $\alpha \in E$. Let $L' \in \mathrm{Twist}_K(L/E)$. Then there exists some $K$-isomorphism $\varphi : E(\sqrt{\alpha}) \to L'$. We will view $E$ as a subset of both extensions $L$ and $L'$, even though $L$ and $L'$ are not necessarily inside the same algebraic closure of $E$.

The element $\varphi(\sqrt{\alpha}) \in L'$ has the same minimal polynomial over $K$ as $\sqrt{\alpha} \in L$, so either $L' \cong E(\sqrt{\alpha})$ or $L' \cong E(\sqrt{\overline{\alpha}})$, where $\overline{\alpha}$ is the conjugate of $\alpha$ over $K$. It is easy to see that both these choices for $L'$ are in $\mathrm{Twist}_K(L/E)$, so

$$\mathrm{Twist}_K(L/E) = \{E(\sqrt{\alpha}), E(\sqrt{\overline{\alpha}})\}.$$

By elementary Galois theory, we have $E(\sqrt{\alpha}) \ncong E(\sqrt{\overline{\alpha}})$ over $E$ if and only if $G = D_4$.

For an integer $m$, define an *$m$-tower* to be a pair $(E, L)$, where $E \in \mathrm{Ext}_{2/K}$ and $L \in \mathrm{Ext}_{2/E}$, such that $L/K$ is a totally ramified extension with $v_K(d_{L/K}) = m$. Write $\mathrm{Tow}_m$ for the set of $m$-towers. There is a natural surjection

$$\Phi_m : \mathrm{Tow}_m \to \Sigma_m^{C_4} \cup \Sigma_m^{V_4} \cup \Sigma_m^{D_4}, \quad (E, L) \mapsto L.$$

**Lemma 5.2.** *Let $G \in \{C_4, V_4, D_4\}$, let $m$ be an integer, and let $L_0 \in \Sigma_m^G$. The fibre $\Phi_m^{-1}(L_0)$ has size*

$$\begin{cases} 1 & \text{if } G = C_4, \\ 2 & \text{if } G = D_4, \\ 3 & \text{if } G = V_4. \end{cases}$$

**Proof.** It is easy to see that

$$\Phi_m^{-1}(L_0) = \{(E, L) : E \in \mathrm{Ext}_{2/K}^{\hookrightarrow L_0}, L \in \mathrm{Twist}_K(L_0/E)\},$$

and the result follows from Lemma 5.1.

**Corollary 5.3.** *For every integer $m$, we have*

$$\#\Sigma_m^{C_4} + 2 \cdot \#\Sigma_m^{D_4} + 3 \cdot \#\Sigma_m^{V_4} = \#\mathrm{Tow}_m.$$

**Proof.** This is immediate from Lemma 5.2.

**Lemma 5.4.** *If $\mathrm{Tow}_m$ is nonempty, then one of the following three statements is true:*

1. *$m$ is an even integer with $6 \leq m \leq 8e_K + 2$.*
2. *$m \equiv 1 \pmod 4$ and $4e_K + 5 \leq m \leq 8e_K + 1$.*
3. *$m = 8e_K + 3$.*

*For even $m$ with $6 \leq m \leq 8e_K + 2$, we have*

$$\#\mathrm{Tow}_m = 4(q-1)q^{\frac{m}{2}-2} \times \left(\mathbb{1}_{m \geq 4e_K+4} \cdot q^{-e_K} + \mathbb{1}_{m \leq 8e_K} \cdot \left(q^{\min\{0, e_K+1-\lceil \frac{m}{4} \rceil\}} - q^{-\min\{\lfloor \frac{m-2}{4} \rfloor, e_K\}}\right)\right).$$

*For $m \equiv 1 \pmod 4$ with $4e_K + 5 \leq m \leq 8e_K + 1$, we have*

$$\#\mathrm{Tow}_m = 4(q-1)q^{e_K + \frac{m-1}{4} - 1}.$$

*We also have*

$$\#\mathrm{Tow}_{8e_K+3} = 4q^{3e_K}.$$

**Proof.** Let $m$ be an integer such that $\mathrm{Tow}_m$ is nonempty. Let $(E, L) \in \mathrm{Tow}_m$, and let $m_1 = v_K(d_{E/K})$ and $m_2 = v_E(d_{L/E})$, so that $m = 2m_1 + m_2$ by the tower law for discriminant. By [Tun78, Lemma 4.3], either $m_1$ is even with $2 \leq m_1 \leq 2e_K$, or $m_1 = 2e_K + 1$. Similarly, either $m_2$ is even with $2 \leq m_2 \leq 4e_K$, or $m_2 = 4e_K + 1$. If $m_2$ is even, then $m$ is even and $6 \leq m \leq 8e_K + 2$. If $m_2 = 4e_K + 1$ and $m_1$ is even, then $m \equiv 1 \pmod 4$ and $4e_K + 5 \leq m \leq 8e_K + 1$. Finally, if $m_1$ and $m_2$ are both odd, then $m = 8e_K + 3$. Now that we have identified the possibilities, we can enumerate $\mathrm{Tow}_m$ in each case.

Suppose first that $m$ is even with $6 \leq m \leq 8e_K + 2$. Then each $(E, L) \in \mathrm{Tow}_m$ has $m_2$ even, so $\#\mathrm{Tow}_m$ is the sum of the following two quantities:

1.
$$\sum_{\substack{\max\{2, \frac{m}{2}-2e_K\} \leq m_1 \leq \min\{\frac{m}{2}-1, 2e_K\} \\ m_1 \text{ even}}} \sum_{E \in \mathrm{Ext}_{2/K, m_1}} \#\mathrm{Ext}_{2/E, m-2m_1}.$$

2.
$$\mathbb{1}_{m \geq 4e_K+4} \cdot \sum_{E \in \mathrm{Ext}_{2/K, 2e_K+1}} \#\mathrm{Ext}_{2/E, m-4e_K-2}.$$

By [Tun78, Lemma 4.3], the first of these quantities is equal to

$$\begin{aligned}\#\mathrm{Ext}_{2/E,m-2m_1} &= \sum_{\substack{\max\{2,\frac{m}{2}-2e_K\}\leq m_1\leq \min\{\frac{m}{2}-1,2e_K\}\\ m_1 \text{ even}}} 4(q-1)^2 q^{\frac{m-m_1}{2}-2} \\ &= 4(q-1)^2 q^{\frac{m}{2}-2}\sum_{k=a}^{b} q^{-k} \\ &= 4(q-1)^2 q^{\frac{m}{2}-2}\cdot \mathbb{1}_{a\leq b}\cdot \frac{q^{1-a}-q^{-b}}{q-1} \\ &= \mathbb{1}_{6\leq m\leq 8e_K}\cdot 4(q-1)q^{\frac{m}{2}-2}(q^{1-a}-q^{-b}),\end{aligned}$$

where

$$a := \max\{1, \lceil \frac{m}{4}\rceil - e_K\}, \quad b := \min\{\lfloor \frac{m-2}{4}\rfloor, e_K\}.$$

For $m = 2, 4$ we have $q^{1-a} - q^{-b} = 0$, so we may drop the "$6 \leq m$" from the indicator function, giving

$$\#\mathrm{Ext}_{2/E,m-2m_1} = \mathbb{1}_{m\leq 8e_K}\cdot 4(q-1)q^{\frac{m}{2}-2}(q^{1-a}-q^{-b}).$$

Similarly, the second quantity is equal to

$$\mathbb{1}_{m\geq 4e_K+4}\cdot 4(q-1)q^{\frac{m}{2}-e_K-2},$$

and we obtain the desired expression for $\#\mathrm{Tow}_m$. Now suppose that $m \equiv 1 \pmod 4$ and $4e_K + 5 \leq m \leq 8e_K + 1$. Then each $(E, L) \in \mathrm{Tow}_m$ has $m_2 = 4e_K + 1$ and $m_1 = \frac{m-1}{2} - 2e_K$, so [Tun78, Lemma 4.3] gives us

$$\begin{aligned}\#\mathrm{Tow}_m &= \sum_{E\in \mathrm{Ext}_{2/K,\frac{m-1}{2}-2e_K}} \#\mathrm{Ext}_{2/E,4e_K+1} \\ &= 4(q-1)q^{e_K+\frac{m-1}{4}-1}.\end{aligned}$$

Finally, if $m = 8e_K + 3$, then each $(E, L) \in \mathrm{Tow}_m$ has $m_1 = 2e_K + 1$ and $m_2 = 4e_K + 1$, so

$$\begin{aligned}\#\mathrm{Tow}_m &= \sum_{E\in \mathrm{Ext}_{2/K,2e_K+1}} \#\mathrm{Ext}_{2/E,4e_K+1} \\ &= 4q^{3e_K},\end{aligned}$$

by [Tun78, Lemma 4.3].

**Proof** *(Proof of Theorem 1.5).* This is immediate from Corollary 5.3 and Lemma 5.4.

**Lemma 5.5.** *We have*

$$\frac{1}{4}\sum_m q^{-m}\#\mathrm{Tow}_m = \frac{1}{q^2+q+1}(q^{-3e_K-3}+q^{-3e_K-1}+q^{-2}).$$

**Proof.** Lemma 5.4 tells us that $\frac{1}{4}\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following four quantities:

1. $\sum_{\substack{4e_K+4\le m\le 8e_K+2\\ m \text{ even}}}(q-1)q^{-\frac{m}{2}-e_K-2}$.
2. $\sum_{\substack{6\le m\le 8e_K\\ m \text{ even}}}(q-1)q^{\min\{0,e_K+1-\lceil\frac{m}{4}\rceil\}-\frac{m}{2}-2}$.
3. $-\sum_{\substack{6\le m\le 8e_K\\ m \text{ even}}}(q-1)q^{-\frac{m}{2}-2-\min\{\lfloor\frac{m-2}{4}\rfloor,e_K\}}$.
4. $\sum_{\substack{4e_K+5\le m\le 8e_K+1\\ m\equiv 1 \pmod 4}}(q-1)q^{e_K+\frac{-3m-1}{4}-1}$.
5. $q^{-5e_K-3}$.

We can simplify this as the sum of the following quantities:

1. $(q-1)q^{-e_K-2}\cdot\sum_{k=2e_K+2}^{4e_K+1}q^{-k}$.
2. (a) $(q-1)q^{-2}\cdot\sum_{k=3}^{2e_K+2}q^{-k}$.
   (b) $(q-1)q^{e_K-1}\cdot\sum_{k=2e_K+3}^{4e_K}q^{-\lceil\frac{3k}{2}\rceil}$.
3. (a) $-(q-1)q^{-e_K-2}\cdot\sum_{k=2e_K+1}^{4e_K}q^{-k}$.
   (b) $-(q-1)q^{-2}\cdot\sum_{k=3}^{2e_K}q^{-\lfloor\frac{3k-1}{2}\rfloor}$.
4. $(q-1)q^{e_K-2}\cdot\sum_{k=e_K+1}^{2e_K}q^{-3k}$.
5. $q^{-5e_K-3}$.

We put the pieces together to obtain the contributions to the final sum:

- (1) and (3)(a) cancel to give a contribution of

$$(q-1)(q^{-5e_K-3}-q^{-3e_K-3}).$$

- (2)(a) simplifies to a contribution of

$$q^{-4}-q^{-2e_K-4}.$$

- We have

$$\sum_{k=2e_K+3}^{4e_K}q^{-\lceil\frac{3k}{2}\rceil}=\frac{q+1}{q^3-1}(q^{-3e_K-3}-q^{-6e_K}),$$

  so (2)(b) gives a contribution of

$$\frac{q+1}{q^2+q+1}(q^{-2e_K-4}-q^{-5e_K-1}).$$

- We have

$$\sum_{k=3}^{2e_K} q^{-\lfloor \frac{3k-1}{2} \rfloor} = \frac{q+1}{q^3-1}(q^{-2} - q^{1-3e_K}),$$

so (3)$(b)$ gives a contribution of

$$-\frac{q+1}{q^2+q+1}(q^{-4} - q^{-1-3e_K}).$$

- We have

$$\sum_{k=e_K+1}^{2e_K} q^{-3k} = \frac{q^{-3e_K} - q^{-6e_K}}{q^3-1},$$

so (4) gives a contribution of

$$\frac{1}{q^2+q+1}(q^{-2e_K-2} - q^{-5e_K-2}).$$

- Finally, (5) obviously gives a contribution of

$$q^{-5e_K-3}.$$

So far, we have shown that $\frac{1}{4}\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following six quantities:

(A) $(q-1)(q^{-5e_K-3} - q^{-3e_K-3})$.
(B) $q^{-4} - q^{-2e_K-4}$.
(C) $\frac{q+1}{q^2+q+1}(q^{-2e_K-4} - q^{-5e_K-1})$.
(D) $-\frac{q+1}{q^2+q+1}(q^{-4} - q^{-3e_K-1})$.
(E) $\frac{1}{q^2+q+1}(q^{-2e_K-2} - q^{-5e_K-2})$.
(F) $q^{-5e_K-3}$.

The sum of $(C), (D)$ and $(E)$ is

$$q^{-2e_K-4} - q^{-5e_K-2} + \frac{q+1}{q^2+q+1}(q^{-3e_K-1} - q^{-4}),$$

so we have shown that $\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following four quantities:

1. $(q-1)(q^{-5e_K-3} - q^{-3e_K-3})$.
2. $q^{-4} - q^{-2e_K-4}$.
3. $q^{-2e_K-4} - q^{-5e_K-2} + \frac{q+1}{q^2+q+1}(q^{-3e_K-1} - q^{-4})$.
4. $q^{-5e_K-3}$.

It is easy to check that this sum simplifies to

$$\frac{1}{q^2+q+1}(q^{-3e_K-3}+q^{-3e_K-1}+q^{-2}),$$

so we are done.

**Proof** *(Proof of Corollary 1.10).* This follows easily from Corollary 5.3, Lemma 5.5, and the definition of mass.

## Data availability

No data was used for the research described in the article.

## References


[Alb23] Brandon Alberts, A random group with local data realizing heuristics for number field counting, arXiv preprint, arXiv:2304.01323 [math.NT], 2023.

[BCP97] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. (ISSN 0747-7171) 24 (3–4) (1997) 235–265, https://doi.org/10.1006/jsco.1996.0125.

[Bha07] Manjul Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, Int. Math. Res. Not. (ISSN 1073-7928) 2007 (Jan. 2007), https://doi.org/10.1093/imrn/rnm052, https://academic.oup.com/imrn/article-pdf/doi/10.1093/imrn/rnm052/19150310/rnm052.pdf.

[BSW15] Manjul Bhargava, Arul Shankar, Xiaoheng Wang, Geometry-of-numbers methods over global fields I: prehomogeneous vector spaces, arXiv preprint, https://doi.org/10.48550/ARXIV.1512.03035, https://arxiv.org/abs/1512.03035, 2015.

[CDO05] Henri Cohen, Francisco Diaz y Diaz, Michel Olivier, Counting cyclic quartic extensions of a number field, J. Théor. Nr. Bordx. 17 (2) (2005) 475–510, issn: 12467405, 21188572, http://www.jstor.org/stable/43974348 (visited on 02/21/2023).

[Dab01] Mario Daberkow, On computations in Kummer extensions, J. Symb. Comput. (ISSN 0747-7171) 31 (1) (2001) 113–131, https://doi.org/10.1006/jsco.2000.1013, https://www.sciencedirect.com/science/article/pii/S0747717100910137.

[Keu23] Frans Keune, Number Fields, Radboud University Press, 2023, http://www.jstor.org/stable/jj.1666828 (visited on 12/28/2023).

[Kra66] Marc Krasner, Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique, Tend. Géom. Algèbr. Théor. Nr. (1966) 143–169.

[Lbe09] Akram Lbekkouri, On the construction of normal wildly ramified extensions over $\mathbb{Q}_2$, Arch. Math. 93 (Oct. 2009) 235–243, https://doi.org/10.1007/s00013-009-0024-5.

[LMFDB] The LMFDB Collaboration, The L-functions and modular forms database, 2023. Online; accessed 29 May 2023.

[Mon22] Sebastian Monnet, $S_4$-quartics with prescribed norms, arXiv preprint, https://doi.org/10.48550/ARXIV.2210.06992, https://arxiv.org/abs/2210.06992, 2022.

[Neu13] Jürgen Neukirch, Class field theory, edited and with a foreword by Alexander Schmidt, translated from the 1967 German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon, in: The Bonn Lectures, Springer, Heidelberg, ISBN 978-3-642-35436-6, 2013, xii+184.

[PS15] Sebastian Pauli, Brian Sinclair, Enumerating extensions of $(\pi)$-adic fields with given invariants, arXiv preprint, https://doi.org/10.48550/ARXIV.1504.06671, https://arxiv.org/abs/1504.06671, 2015.

[Ser78] Jean-Pierre Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, C. R. Acad. Sci. Paris Sér. A-B (ISSN 0151-0509) 286 (22) (1978) A1031–A1036.

[Ser95] J.P. Serre, Local Fields, Graduate Texts in Mathematics, Springer, New York, ISBN 9780387904245, 1995, https://books.google.co.uk/books?id=DAxlMdw%5C_QloC.
[Sin15] Brian Sinclair, Counting extensions of $\mathfrak{p}$-adic fields with given invariants, arXiv preprint, https://doi.org/10.48550/ARXIV.1512.06946, https://arxiv.org/abs/1512.06946, 2015.
[Tun78] Jerrold B. Tunnell, On the local Langlands conjecture for $GL(2)$, Invent. Math. (ISSN 0020-9910) 46 (2) (1978) 179–200, https://doi.org/10.1007/BF01393255.
[WJ07] Da-Sheng Wei, Chun-Gang Ji, On the number of certain Galois extensions of local fields, Proc. Am. Math. Soc. 135 (10) (2007) 3041–3047, issn: 00029939, 10886826, http://www.jstor.org/stable/20534923 (visited on 05/19/2023).