COMPOSITIO MATHEMATICA

On the probabilities of local behaviors in abelian field extensions

Melanie Matchett Wood

Compositio Math. **146** (2010), 102–128.

doi:10.1112/S0010437X0900431X

FOUNDATION
COMPOSITIO
MATHEMATICA

The London
Mathematical
Society

Compositio Math. 146 (2010) 102–128
doi:10.1112/S0010437X0900431X

On the probabilities of local behaviors in abelian field extensions

Melanie Matchett Wood

Abstract

For a number field K and a finite abelian group G, we determine the probabilities of various local completions of a random G-extension of K when extensions are ordered by conductor. In particular, for a fixed prime $\wp$ of K, we determine the probability that $\wp$ splits into r primes in a random G-extension of K that is unramified at $\wp$. We find that these probabilities are nicely behaved and mostly independent. This is in analogy to Chebotarev's density theorem, which gives the probability that in a fixed extension a random prime of K splits into r primes in the extension. We also give the asymptotics for the number of G-extensions with bounded conductor. In fact, we give a class of extension invariants, including conductor, for which we obtain the same counting and probabilistic results. In contrast, we prove that neither the analogy with the Chebotarev probabilities nor the independence of probabilities holds when extensions are ordered by discriminant.

1. Introduction

Given a finite Galois extension $L/\mathbb{Q}$ with Galois group G, and a rational prime p, what is the probability that p splits completely in L? If we fix L and vary p, the Chebotarev density theorem tells us what proportion of primes have any given splitting behavior. However, we can alternatively fix p (and G), and study the probability that p splits a certain way in a random L with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$. We ask whether the probabilities of the unramified splitting types are in the proportions we expect from the Chebotarev density theorem. We also ask if the probabilities are independent at different primes p. In fact, we shall ask more refined questions and study the probabilities of various local $\mathbb{Q}_v$-algebras $L_v := L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ at a place v of $\mathbb{Q}$. These questions have recently been asked by Bhargava [Bhab, § 8.2] and have come up naturally in the work counting extensions of $\mathbb{Q}$ with a given Galois group (see [Coh02, CDO02a, Tay84, Wri89], and § 1.2). In this paper, we answer these refined questions for abelian G. For the rest of this paper, we fix a finite abelian group G.

We define a *G-extension of* a field K to be a Galois extension L/K with an isomorphism $\phi : G \to \mathrm{Gal}(L/K)$. An isomorphism of two G-extensions L and L' is given by an isomorphism $L \to L'$ of K-algebras that respects the G-action on L and L'. Let $E_G(K)$ be the set of isomorphism classes of G-extensions of K. Given a finite set S of places of $\mathbb{Q}$, and a $\mathbb{Q}_v$-algebra T_v for each $v \in S$, we use T to denote the collection of all the choices T_v. We define the *probability of* T as

Received 23 November 2008, accepted in final form 22 April 2009, published online 8 December 2009.
2000 Mathematics Subject Classification 11R20, 11R45.
Keywords: abelian extensions, density of discriminants, local-to-global, local behavior.
This work was completed while the author was supported by a National Science Foundation Graduate Fellowship and a National Defense Science and Engineering Graduate Fellowship.

follows:

$$\Pr(T) = \lim_{X\to\infty} \frac{\#\{L \in E_G(\mathbb{Q}) \mid L_v \cong T_v \text{ for all } v \in S \text{ and } \mathfrak{f}(L) < X\}}{\#\{L \in E_G(\mathbb{Q}) \mid \mathfrak{f}(L) < X\}}, \tag{1}$$

where $\mathfrak{f}(L)$ is the finite conductor of L over $\mathbb{Q}$. We can analogously define the probability of one local algebra T_v, or of a splitting type of a prime.

Given a G-extension L of $\mathbb{Q}$, every L_v is of the form $M^{\oplus r}$, where M is a field extension of $\mathbb{Q}_v$ with Galois group H, and H is a subgroup of G of index r. The first twist in this story is that some algebras $M^{\oplus r}$ of the form *never* occur as L_v. For example, when $G = \mathbb{Z}/8\mathbb{Z}$, it is never the case that $L_2/\mathbb{Q}_2$ is unramified of degree 8. This means we cannot expect unramified splitting types to occur in the proportions suggested by the Chebotarev density theorem. Wang [Wan50], in a correction to the work of Grunwald [Gru33], completely determined which local algebras occur. The only obstruction is that, for even $|G|$, some $\mathbb{Q}_2$ algebras do not occur as L_2 for any G-extension L. Call these *inviable* $\mathbb{Q}_2$-algebras (and all other $M^{\oplus r}$ of the above form *viable*) and note that the characterization implicitly depends on G. Once one knows which local algebras can occur, it is natural to ask how often they occur. We answer that question in the following theorem.

Theorem 1.1. *Let v be a place of $\mathbb{Q}$. Let M and M' be field extensions of $\mathbb{Q}_v$ with Galois groups H and H' that are subgroups of G of index r and r', respectively. Then, unless $v = 2$ and at least one of $M^{\oplus r}$, $M'^{\oplus r'}$ is inviable,*

$$\frac{\Pr(M^{\oplus r})}{\Pr(M'^{\oplus r'})} = \frac{|\mathrm{Hom}_0(H, G)|/\mathfrak{f}(M)}{|\mathrm{Hom}_0(H', G)|/\mathfrak{f}(M')},$$

where $\mathrm{Hom}_0(E, G)$ denotes the set of injective homomorphisms from E to G. The conductor $\mathfrak{f}(M)$ is viewed as an element of $\mathbb{Q}$.

We will refer to the density of primes with a given splitting type in a fixed G-extension as the *Chebotarev probability* of that splitting type. We compare Theorem 1.1 to the Chebotarev density theorem in the following corollary.

Corollary 1.2. *The probability of a fixed rational prime p (not 2 if $|G|$ is even) splitting into r primes in a random $L \in E_G(\mathbb{Q})$, given that p is unramified, is the same as the Chebotarev probability of a random rational prime p splitting into r primes in a fixed $L \in E_G(\mathbb{Q})$.*

In fact, it follows from Theorem 1.1 that when $|G|$ is even and $p = 2$ the probabilities of viable splitting types in a random G-extension occur in the same proportions as they occur in the Chebotarev density theorem for a fixed extension and random prime. Of course, one contrast to the Chebotarev probabilities is that, for a fixed p and a random G-extension L, the prime p will be ramified with positive probability. In this paper, we also determine the independence of the local probabilities calculated in Theorem 1.1, leading to the following result.

Theorem 1.3. *For any finite set S of places of $\mathbb{Q}$ and any choice of local $\mathbb{Q}_v$-algebras T_v for $v \in S$, the events T_v are independent.*

One may ask whether we obtain the same result if we count the G-extensions in other ways, for example by replacing the conductor by the discriminant, by an Artin conductor, or by the product of the ramified primes. In fact, in § 2 we prove a stronger version of Theorem 1.1 which replaces the conductor with any function satisfying a certain *fairness* hypothesis (defined in § 2), which is satisfied by the conductor, some Artin conductors, and the product of the

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

ramified primes. In § 5 we give examples of some Artin conductors that are fair. The discriminant is fair only when G has prime exponent. Much work has been done to study the asymptotics of the number of extensions with bounded discriminant and having Galois closure with a specified Galois group (see [Coh02, CDO06] for surveys). These asymptotics were determined completely for abelian Galois groups by Mäki [Mäk85]. Mäki [Mäk93] has also determined the asymptotics of the number of extensions with fixed abelian Galois group and bounded conductor. In § 3, we give the asymptotics of the number of G-extensions with bounded conductor (or any fair counting function) for a finite abelian group G. Our result is a generalization of Mäki's work [Mäk93], in that we can replace the conductor by other fair counting functions and that we give the result over an arbitrary base number field (see § 1.1). We also give the constant in the asymptotic more explicitly than it appears in [Mäk93].

For degree n extensions having Galois closure with Galois group S_n, it is known that, when counting by discriminant for $n = 2$, 3, 4, and 5, local completions L_v show up with probability proportional to $(1/|\mathrm{Aut}_{\mathbb{Q}_v} L_v|)(1/|\mathrm{Disc}\, L_v|)$ (see [DH71, Bha05, Bhaa] for the computation of the probabilities, and [Bhab] for this interpretation). We will see after Corollary 1.7 how to interpret our probabilities in closer analogy to the results in [DH71, Bha05, Bhaa]. However, it turns out that counting abelian extensions by discriminant does not lead to such nice local probabilities. This was observed by Wright [Wri89] in his work on counting abelian extensions asymptotically by discriminant. Let the *discriminant probability* be defined as in (1) but with the conductor replaced by the absolute value of the discriminant. We call two events *discriminant independent* if they are independent with the discriminant probability. Wright showed that all viable $\mathbb{Q}_v$-algebras occur with positive discriminant probability, and noted that, when G has prime exponent, the relative probabilities of local extensions are simple expressions. (Wright actually works over an arbitrary global field with characteristic not dividing $|G|$; in § 1.1 of this paper we describe our work over an arbitrary number field.) When $G = \mathbb{Z}/4\mathbb{Z}$, Wright notes that the ratio of the discriminant probability of $\mathbb{Q}_p^{\oplus 4}$ to the discriminant probability of the unramified extension of $\mathbb{Q}_p$ of degree 4 is an apparently very complicated expression. In § 4, we prove the following propositions in order to show that the discriminant probability analogs of Corollary 1.2 or Theorem 1.3 do not hold.

Proposition 1.4. *Let p, q_1, and q_2 be primes with $q_i \equiv 1 \pmod{p^2}$ for $i = 1, 2$. Then q_1 ramifying and q_2 ramifying in a random $\mathbb{Z}/p^2\mathbb{Z}$-extension are not discriminant independent.*

The Chebotarev probability that a random prime splits completely in a fixed $\mathbb{Z}/9\mathbb{Z}$-extension is 1/9. However, we have the following.

Proposition 1.5. *Let $q = 2$, 3, 5, 7, 11, or 13. Given that q is unramified, the discriminant probability that q splits completely in a random $\mathbb{Z}/9\mathbb{Z}$-extension is strictly less than* 1/9.

For comparison, in the above two cases we have that the (conductor) probabilities are independent, and the (conductor) probability is 1/9, respectively.

1.1 Other base fields

Of course, we can ask all of the same questions when $\mathbb{Q}$ is replaced by an arbitrary number field K, and we now fix a number field K. However, for arbitrary number fields there is a further twist in this story. Given G, it is possible that the K_v-algebra T_v and the $K_{v'}$-algebra $T'_{v'}$ both occur from global G-extensions, but never occur simultaneously (a forthcoming paper of the author explores the frequency of such examples). This suggests that we should not expect T_v

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

and $T'_{v'}$ to be independent events. However, given obstructions of this sort, which were completely determined in [Wan50] (or see [AT68, ch. 10]), we have the best possible behavior of the local probabilities. We shall need more precise language to clearly explain this behavior.

The local K_v-algebras coming from L have structure that we have so far ignored; namely, they have a G-action coming from the global G-action. Given a field F, a *G-structured F-algebra* is an étale F-algebra L of degree $|G|$ with an inclusion $G \hookrightarrow \mathrm{Aut}_F(L)$ of G into the F-algebra automorphisms of L, such that G acts transitively on the idempotents of L. An isomorphism of two G-structured F-algebras L and L' is an F-algebra isomorphism $L \to L'$ such that the induced map $\mathrm{Aut}_F(L) \to \mathrm{Aut}_F(L')$ restricts to the identity on G. If we have a G-extension L of K, for each place v of K, then we have a G-structured K_v-algebra $L_v = L \otimes_K K_v$, where G acts on the left factor. Given a subgroup H of G, and an H-extension M of K_v, we can form the induced G-structured K_v-algebra $\mathrm{Ind}_H^G M$ via the usual construction of an induced representation, which will have a natural structure of an étale K_v-algebra. All G-structured K_v-algebras coming from G-extensions L of K are of the form $\mathrm{Ind}_H^G M$. So we can ask an even more refined question, at all places, about the probability of a certain G-structured K_v-algebra. We let $\mathfrak{f}(L)$ be the norm from K to $\mathbb{Q}$ of the conductor of L/K (or of the conductor of L/K_v, viewed as an ideal of K). Let S be a finite set of places of K, and let Σ denote a choice Σ_v of G-structured K_v-algebra for each $v \in S$, which we refer to as a (*local*) *specification*. We can then define probabilities as in (1), replacing $E_G(\mathbb{Q})$ with $E_G(K)$.

If there exists a G-extension L/K such that $L_v \cong \Sigma_v$ for all $v \in S$, then we call Σ *viable* and otherwise we call it *inviable*. The question of which specifications are viable has been completely answered (see [AT68, ch. 10]). There is a set S_0 of places of K (depending on G, all dividing 2, and empty if $|G|$ is odd) and a finite list $\Sigma(1), \dots, \Sigma(\ell)$ of local specifications on S_0 such that a local specification Σ on S is viable if and only if either $S_0 \not\subset S$ or Σ restricts to some $\Sigma(i)$ on S_0. (We give S_0 explicitly in § 2.) In other words, whether a specification on S is viable depends only on its specifications at places in S_0, and if a specification does not include specifications at all places in S_0 then it is viable.

Now we will build a model for the expected probabilities of local specifications. Let $\Omega = \prod_{v \text{ place of } K} \{\text{isometry classes of } G\text{-structured } K_v\text{-algebras}\}$. For a local specification Σ, let $\tilde{\Sigma} = \{x \in \Omega \mid x_v \cong \Sigma_v \text{ for all } v \in S\}$. Let $A = \bigcup_{i=1}^{\ell} \tilde{\Sigma}(i)$, where $\Sigma(i)$ are as in the above paragraph in the condition for a local specification to be viable. So, for a specification Σ on S, we have that $\tilde{\Sigma} \cap A$ is non-empty if and only if Σ is viable, and in fact $\tilde{\Sigma} \cap A$ is the union of $\tilde{\Sigma}'$ for all local specifications Σ' on $S \cup S_0$ that are viable and restrict to Σ on S.

The $\tilde{\Sigma}_v$ generate an algebra of subsets of Ω. We can define a finitely additive probability measure P on this algebra by specifying that:

(i)
$$\frac{P(\tilde{\Sigma}_v)}{P(\tilde{\Sigma}'_v)} = \frac{1/\mathfrak{f}(\Sigma_v)}{1/\mathfrak{f}(\Sigma'_v)}$$
for all G-structured K_v-algebras Σ_v and Σ'_v;

(ii) $\tilde{\Sigma}_{v_1}, \dots, \tilde{\Sigma}_{v_s}$ at pairwise distinct places $v_1, \dots, v_s$, respectively, are independent.

We might at first hope that P is a model for the probabilities of local specifications in the space of G-extensions. However, once we know that some specifications never occur, including combinations of occurring specifications, the best we can hope for is the following, which we prove in § 2.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Theorem 1.6. *For a local specification Σ on a finite set of places S,*

$$\Pr(\Sigma) = P(\tilde{\Sigma}|A).$$

Corollary 1.7. *If S is a finite set of places of K either containing S_0 or disjoint from S_0, and Σ and Σ' are viable local specifications on S then*

$$\frac{\Pr(\Sigma)}{\Pr(\Sigma')} = \frac{\prod_{v \in S}(1/\mathfrak{f}(\Sigma_v))}{\prod_{v \in S}(1/\mathfrak{f}(\Sigma'_v))}.$$

All G-structured algebras have $|G|$ automorphisms (Proposition 2.7), and so, for v not in S_0, we can also say that the probability of Σ_v is proportional to $1/(|\mathrm{Aut}(\Sigma_v)|\mathfrak{f}(\Sigma_v))$.

Corollary 1.8. *The probability of a fixed prime $\wp$ of K (not in S_0) splitting into r primes in a random $L \in E_G(K)$, given that $\wp$ is unramified, is the same as the Chebotarev probability of a random prime $\wp$ of K splitting into r primes in a fixed $L \in E_G(K)$.*

Corollary 1.9. *If $S_1, \dots, S_t$ are pairwise disjoint finite sets of places of K, and each S_i either contains S_0 or is disjoint from S_0, then local specifications $\Sigma^{(i)}$ on S_i are independent.*

Theorem 1.6 says that the probabilities of local specifications of random G-extensions are exactly as in a model with simple and independent local probabilities, but restricted to a subspace corresponding to the viable specifications on S_0. As when $K = \mathbb{Q}$, we prove Theorem 1.6 and its corollaries as a special case of analogous results (see Theorem 2.1) for more general ways of counting extensions than by conductor.

1.2 History of the problem and previous work

The results mentioned above of Davenport and Heilbronn [DH71] and Bhargava [Bha05, Bhaa] are a major motivation of this work. These results show that the local behaviors of random degree n extensions of $\mathbb{Q}$, whose Galois closure has Galois group S_n, have nice discriminant probabilities and are discriminant independent, when $n = 3$, 4, or 5. The work of Datskovsky and Wright [DW86] generalizes that of Davenport and Heilbronn (the case $n = 3$) to an arbitrary base field.

Taylor [Tay84] proves the result of our Corollary 1.8 in the special case that $G = \mathbb{Z}/n\mathbb{Z}$, and assuming that if $2^g \mid n$ then K contains the 2^gth roots of unity (in which case S_0 is empty). Taylor attributes the question of the distribution of splitting types of a given prime in random G-extensions to Fröhlich, who was motivated by the work of Davenport and Heilbronn [DH71]. Wright [Wri89] proves an analog of Corollary 1.7 for discriminant probability in the case that $G = (\mathbb{Z}/p\mathbb{Z})^b$ for p prime and $|S| = 1$, and for these G the discriminant is a fixed power of the conductor, and thus discriminant probability is the same as conductor probability. Wright [Wri89] suggests that his methods for counting abelian extensions by discriminant could be combined with the methods of Taylor to count abelian extensions by conductor. In this paper, we follow this suggestion and incorporate methods of both Wright and Taylor along with some new ideas. We implicitly count abelian extensions by conductor (and give this result in § 3), but are focused on the probabilities of local behaviors.

In the work of counting extensions whose Galois closure has some fixed Galois group, it has been often suggested that it is natural to also count such extensions with fixed local behavior (for example, in the work of Cohen *et al.* [CDO06] for the group D_4, the heuristics of Malle [Mal04, Remark 1.2] for general groups, and in the general surveys [Coh02, CDO02a]). Some authors have also considered these questions when one replaces field extensions with polynomials, and counts with a natural density on the polynomials (see [DD93, DD98, DD00, van88]).

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Theorems 1.1, 1.3, and 1.6 and their corollaries are all new (except in the special cases mentioned above), but the proofs use many techniques that come from the work of Taylor and Wright. Some new techniques are required to calculate the probabilities exactly in the case of non-cyclic G and for more general ways of counting extensions. An important new ingredient is the consideration of the probabilities of G-structured K_v-algebras (and not just K_v-algebras), which not only allows us to give more refined probabilities but allows us to state Theorem 1.6. One of the central contributions of this paper is the formulation of Theorem 1.6, which makes precise the idea that the probabilities are as well-behaved as possible in light of the non-occurrence of certain local extensions (see [Wan50, AT68]). For abelian groups G, we study for the first time the probabilities when more than one local behavior is specified and the independence of these local probabilities. Our results are for all base number fields K, all finite abelian groups G, and for many ways of counting extensions (see the definition of *fair* in § 2) including by conductor.

1.3 Outline of the paper

In § 2, we define counting functions and fairness, and prove our main theorems. The proof of our main theorems involves making a Dirichlet series generating function for the extensions we are counting, relating it to L-functions whose analytic behavior is known, using standard Tauberian theorems to deduce asymptotic counting results, and using fairness to express the desired probabilities in a simple form. In § 3, we give the asymptotic number of G-extensions with a given invariant (such as conductor) bounded. We give an explicit Euler product for the constant in this asymptotic result. In § 4, we prove that, when counting by discriminant, the local probabilities do not have the same nice behavior as in the conductor case. In § 5, we give some examples of fair Artin conductors. In § 6, we discuss the further questions that this work motivates.

2. Statement and proof of the main theorem

In this section, we prove a generalization of Theorems 1.1 and 1.6 for more general ways of counting G-extensions than by conductor. First, in § 2.1, we will define the acceptable ways of counting G-extensions. Then, in § 2.2, we state Theorem 2.1 (our generalization of Theorems 1.1 and 1.6) and deduce several corollaries. In § 2.3, we relate G-structured algebras to Galois representations. In § 2.4, we define a generating function counting G-extensions satisfying a local specification Σ and express this generating function as a sum of Euler products. In § 2.5, we state three lemmas about the analytic behavior of these Euler products, and then use the standard Tauberian analysis to determine the asymptotic behavior of the coefficient sums of the generating function from the rightmost poles. From this asymptotic behavior we deduce Theorem 2.1. In § 2.6, we prove the three lemmas stated in § 2.5. The method in § 2.4 is very similar to that of Wright [Wri89] and some of the methods in § 2.6 are motivated by those of Taylor [Tay84].

2.1 Counting functions and fairness

We fix a finite abelian group G and a number field K. Let $n = |G|$. Let $c_G : G \to \mathbb{Z}_{\geqslant 0}$ be a function such that (i) $c_G(g) = 0$ if and only if $g = 1$ and (ii) if e is relatively prime to the order of $g \in G$, then $c_G(g^e) = c_G(g)$. For all places v dividing n or infinite, let

$$c_v : \{\text{isometry classes of } G\text{-structured } K_v\text{-algebras}\} \to \mathbb{Z}_{\geqslant 0}$$

be an arbitrary function. From these functions c_G and the c_v, we define

$$c : \{\text{isometry classes of } G\text{-structured } K_v\text{-algebras}\} \to \mathbb{Z}_{\geqslant 0}$$

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

by

$$c(\Sigma_v) = \begin{cases} c_G(y_v) & \text{if } v \nmid n\infty, \text{ where } \Sigma_v = \operatorname{Ind}_H^G M, \text{ and } M/K_v \text{ a field extension,} \\ & \text{and } y_v \text{ is any generator of tame inertia in } \operatorname{Gal}(M/K_v) \subset G; \\ c_v(\Sigma_v) & \text{if } v \mid n\infty. \end{cases}$$

We then define an invariant C of G-extensions by the product $C(L) = \prod_v Nv^{c(L_v)}$ over places of K, where Nv is $N_{K/\mathbb{Q}}v$ at finite places and by convention 1 at infinite places. We call such a C, determined by components c_G and the c_v, a *counting function*. Let $m = \min_{g \in G \setminus \{1\}} c_G(g)$ and let $\mathfrak{M} = c_G^{-1}(m)$. Let $G_r = \{x \in G \mid x^r = 1\}$.

A counting function is *fair* if, for all r, we have that $\mathfrak{M} \cap G_r$ generates G_r. The norms to $\mathbb{Q}$ of the conductor and of the product of ramified primes of an extension are both fair counting functions with $m = 1$ and $\mathfrak{M} = G \setminus \{1\}$. The discriminant is a counting function, but it is not fair unless G has prime exponent. For example, when $G = \mathbb{Z}/p^2\mathbb{Z}$, for the discriminant we have $\mathfrak{M} = p\mathbb{Z}/p^2\mathbb{Z}$. In § 5, we give some examples of fair Artin conductors.

2.2 Statement of the main theorem and corollaries

We define the C-probability, Pr_C, by replacing $\mathfrak{f}$ with C in (1). (Note that $C(L) < X$ implies that L is unramified at all primes larger than nX, and so there are only finitely many such extensions.) As in the definition of P in the introduction, we define P_C on the algebra of subsets of $\Omega = \prod_{v \text{ place of } K} \{\text{isometry classes of } G\text{-structured } K_v\text{-algebras}\}$ generated by the $\tilde{\Sigma}_v$ by specifying:

(i)
$$\frac{P_C(\tilde{\Sigma}_v)}{P_C(\tilde{\Sigma}'_v)} = \frac{Nv^{-c(\Sigma_v)/m}}{Nv^{-c(\Sigma'_v)/m}}$$

for all G-structured algebras Σ_v and Σ'_v; and

(ii) $\tilde{\Sigma}_{v_1}, \ldots, \tilde{\Sigma}_{v_s}$ at pairwise distinct places $v_1, \ldots, v_s$ are C-independent.

Let $\eta_i = \zeta_{2^i} + \zeta_{2^i}^{-1}$, where ζ_{2^i} is a primitive 2^ith root of unity. Let s be maximal such that $\eta_s \in K$. If 2^{s+1} does not divide the exponent of G, then let $S_0 = \emptyset$. Otherwise, let S_0 be the set of primes $\wp$ of K dividing 2 such that none of -1, $2 + \eta_s$, and $-2 - \eta_s$ are squares in $K_\wp$. Recall that there is a list $\Sigma(1), \ldots, \Sigma(\ell)$ of local specifications on S_0 such that a local specification Σ on S is viable if and only if either $S_0 \not\subset S$ or Σ restricts to some $\Sigma(i)$ on S_0 (see [AT68, ch. 10]). We have defined $A = \bigcup_{i=1}^{\ell} \tilde{\Sigma}(i)$. If S_0 is empty, then all local specifications are viable and A is the total space Ω. In this section, we prove the following theorem, of which Theorems 1.1 and 1.6 are special cases.

Theorem 2.1. *For a local specification Σ on a finite set of places S and a fair counting function C,*

$$\mathrm{Pr}_C(\Sigma) = P_C(\tilde{\Sigma}|A).$$

Now, we will prove several corollaries of Theorem 2.1. Corollaries 1.2, 1.7, 1.8, and 1.9 from the introduction are just the following corollaries when C is the norm to $\mathbb{Q}$ of the conductor. Theorem 1.3 follows from Corollary 1.9.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Corollary 2.2. *If S is a finite set of places of K either containing S_0 or disjoint from S_0, and Σ and Σ' are viable local specifications on S then*

$$\frac{\Pr_C(\Sigma)}{\Pr_C(\Sigma')} = \prod_{v \in S} \frac{Nv^{-c(\Sigma_v)/m}}{Nv^{-c(\Sigma'_v)/m}}.$$

Proof. If S is disjoint from S_0, then since A only includes specifications on S_0, we have that $\tilde{\Sigma}$ and $\tilde{\Sigma}'$ are each P_C-independent from A in Ω. Thus $\Pr_C(\Sigma) = P_C(\tilde{\Sigma}|A) = P_C(\tilde{\Sigma})$, and similarly for Σ'. If $S \supset S_0$, then since Σ is viable, $\tilde{\Sigma} \subset A$. Thus, $\Pr_C(\Sigma) = P_C(\tilde{\Sigma}|A) = P_C(\tilde{\Sigma})/P_C(A)$, and similarly for Σ'. □

Corollary 2.3. *The C-probability of a fixed prime $\wp$ of K (not in S_0) splitting into r primes in a random $L \in E_G(K)$, given that $\wp$ is unramified, is the same as the Chebotarev probability of a random prime $\wp$ of K splitting into r primes in a fixed $L \in E_G(K)$.*

Proof. The number of $\Sigma_\wp$ that give $\wp$ unramified and splitting into r primes is the number of order $|G|/r$ elements of $|G|$. (This can be seen, for example, from Lemma 2.6.) Thus

$$\frac{\Pr_C(\wp \text{ splits unramified into } r \text{ primes})}{\Pr_C(\wp \text{ splits unramified into } r' \text{ primes})} = \frac{\text{number of order } |G|/r \text{ elements of } |G|}{\text{number of order } |G|/r' \text{ elements of } |G|},$$

which agrees with the Chebotarev probabilities. □

Corollary 2.4. *Let $S_1, \dots, S_t$ be pairwise disjoint finite sets of places of K, and suppose each S_i either contains S_0 or is disjoint from S_0. (For example, if $|S_0|$ is 0 or 1, then this is always the case.) Then local specifications $\Sigma^{(i)}$ on S_i are C-independent.*

Proof. If S_0 is empty, then $A = \Omega$, and this corollary is clear. Otherwise, first suppose some S_i, say S_1, contains S_0. If $\Sigma^{(1)}$ is inviable, then $\Pr_C(\Sigma^{(1)}) = 0$ and otherwise we have $\Pr_C(\Sigma^{(1)}) = P_C(\tilde{\Sigma}^{(1)})/P_C(A)$. For $i \neq 1$ we have $\Pr_C(\Sigma^{(i)}) = P_C(\tilde{\Sigma}^{(i)})$, as in the proof of Corollary 2.2. Let Σ be the local specification that is the union of the $\Sigma^{(i)}$. If $\Sigma^{(1)}$ is inviable then $\Pr_C(\Sigma) = 0$, otherwise

$$\Pr_C(\Sigma) = P_C(\tilde{\Sigma})/P_C(A) = \frac{\prod_i P_C(\tilde{\Sigma}^{(i)})}{P_C(A)} = \prod_i \Pr_C(\Sigma^{(i)}).$$

If, on the other hand, no S_i contains S_0, then we have $\Pr_C(\Sigma^{(i)}) = P_C(\tilde{\Sigma}^{(i)})$ for all i and $\tilde{\Sigma}$ is C-independent from A. Thus $\Pr_C(\Sigma) = P_C(\tilde{\Sigma}) = \prod_i \Pr_C(\tilde{\Sigma}^{(i)}) = \prod_i \Pr_C(\Sigma^{(i)})$. □

Notation 2.5. We let $n = |G|$ and write $G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$. For the rest of § 2 we use additive notation for G. For all positive integers m, we choose compatible primitive mth roots of unity ζ_m such that if $m'|m$, then $\zeta_{m'} = \zeta_m^{m/m'}$. Let J be the group of idèles of K. For a map χ from J, we denote by χ_v the restriction of χ to $K_v^\times$. Let o_v be the ring of integers of K_v. Let J_S be the group of idèles which have components in $o_v^\times$ for all places $v \notin S$. In this paper, when we write a map from the idèles, idèle class group, or $K_v^\times$ to a finite group (e.g., $\chi : J \to G$), it will always mean a continuous homomorphism (for the discrete topology on the range).

2.3 G-structured algebras and Galois representations

Recall that G is a finite abelian group. The following two results are fairly standard, but we include them here for completeness.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Lemma 2.6. *For a field F, there is a one-to-one correspondence*

$$\left\{\begin{matrix}\text{isomorphism classes of}\\ G\text{-structured } F\text{-algebras}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{continuous homomorphisms}\\ G_F \to G\end{matrix}\right\}$$

where G_F is the Galois group of a separable closure of F over F. In this correspondence, G-extensions correspond to surjective homomorphisms.

Proof. Given a G-structured K-algebra L with $G \subset \operatorname{Aut}_K(L)$, we consider the stabilizer $\mathrm{Stab} \subset G$ of one of the fields L_0 that is a direct summand of L. We have a morphism $\mathrm{Stab} \to \mathrm{Gal}(L_0/K)$. Since G is transitive on the idempotents of L and abelian, this is an injection. Since G is transitive on the idempotents, we see that all the fields that are direct summands of L are isomorphic, and thus $|\mathrm{Stab}| = [L_0 : K]$. Therefore, $\mathrm{Stab} \to \mathrm{Gal}(L_0/K)$ is an isomorphism. Its inverse gives $G_K \to \mathrm{Gal}(L_0/K) \to \mathrm{Stab} \subset G$.

Given a continuous homomorphism $\chi : G_K \to G$, we have an $\mathrm{im}(\chi)$-extension L_0 of K corresponding to the kernel of χ via Galois theory. We let $L = \mathrm{Ind}_{\mathrm{im}(\chi)}^G L_0$. It is straightforward to check that these two constructions are inverse to each other. □

Proposition 2.7. *A G-structured algebra has exactly $|G|$-automorphisms.*

Proof. Consider a G-structured F-algebra L. Let $\bar{F}$ be the separable closure of F. There are $|G|$ non-zero morphisms $\phi_i : L \to \bar{F}$. Let $S_{|G|}$ be the permutations of these ϕ_i. We have $G \subset \operatorname{Aut}_F(L) \subset S_{|G|}$. An automorphism of L as a G-structured F-algebra is an element $\sigma \in \operatorname{Aut}_F(L)$ such that σ centralizes G. Clearly all elements of G will satisfy this condition since G is abelian. Since G acts transitively on the idempotents of L, G acts transitively in $S_{|G|}$. Thus we can relabel the ϕ_i by elements of G, and G will act by multiplication on the labels. So if $\sigma \in S_{|G|}$ centralizes G, then σ is translation by an element of G, and these are just the automorphisms that come from G. □

By class field theory, the maps $\chi : G_K \to G$ are in one-to-one correspondence with the maps $\chi : J/K^\times \to G$. Given the correspondence of Lemma 2.6, we can also apply C to the characters $\chi : J/K^\times \to G$. We now view a generator of tame inertia y_v as an element of $K_v^\times$, and define $c(\chi_v)$ to be $c_G(\chi_v(y_v))$ for v finite and not dividing n. For v infinite or dividing n, let L_v be the G-structured étale K_v-algebra corresponding to the character χ_v, and define $c(\chi_v)$ to be $c_v(L_v)$. We say that

$$C(\chi) = \prod_{v \text{ place of } K} Nv^{c(\chi_v)}.$$

Just as Σ denotes local specifications of G-structured K_v-algebras at the places $v \in S$, we let ϕ denote a collection of choices $\phi_v : K_v^\times \to G$ for all $v \in S$. We say that ϕ *corresponds to* Σ if each ϕ_v corresponds to Σ_v via Lemma 2.6.

2.4 Generating functions and Euler products

For now, we will assume that C is an arbitrary counting function, and, in Lemma 2.17, we will first see how fairness plays a role in our analysis. Also, for now we will consider one local specification Σ (not necessarily viable) on a finite set S of places of K such that S contains all infinite places, places dividing n, and so that the finite places of S generate the class group of K. In particular, if o_S is the ring of S-integers of K (elements of K with non-negative valuation at all places not in S), then o_S has class number 1.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

We define the generating functions

$$N_{C,G}(s,\Sigma)=\sum_{\substack{G\text{-extensions } L/K\\ \forall v\in S\ \ L_v\cong\Sigma_v}}\frac{1}{C(L)^s}\quad\text{and}\quad N_{C,G}(s,\phi)=\sum_{\substack{\chi:J/K^\times\to G\\ \forall v\in S\ \ \chi_v=\phi_v\\ \chi\text{ surjective}}}\frac{1}{C(\chi)^s}.$$

By Lemma 2.6, for ϕ corresponding to Σ we have $N_{C,G}(s,\Sigma)=N_{C,G}(s,\phi)$. It will be easier to work without the restriction that our characters are surjective, so we define the following generating function:

$$F_{C,G}(s,\phi)=\sum_{\substack{\chi:J/K^\times\to G\\ \forall v\in S\ \ \chi_v=\phi_v}}\frac{1}{C(\chi)^s}.$$

For a subgroup H of G, we define $C|_H$, a counting function for H. For $\chi_v:J/K^\times\to H$, we let $c|_H(\chi_v)=c(J/K^\times\overset{\chi_v}{\to}H\subset G)$. We have that

$$F_{C,G}(s,\phi)=\sum_{H\text{ subgroup of }G}N_{C|_H,H}(s,\phi).$$

We can use Möbius inversion (as in Wright's work [Wri89, § 2]) to write

$$N_{C,G}(s,\phi)=\sum_{H\text{ subgroup of }G}\mu(H,G)F_{C|_H,H}(s,\phi),$$

where $\mu(H,G)$ is a constant and $\mu(G,G)=1$. (This is just solving an upper triangular system of linear equations.) Thus, by studying the $F_{C,G}$ we can recover information about the $N_{C,G}$.

A character $\chi:J\to G$ is determined by a collection of $\chi_v:K_v^\times\to G$ for all places v of K, but not all χ factor through $J/K^\times$. However, we can use the following lemma.

Lemma 2.8. *If o_S has class number 1, then the natural map $J_S/o_S^\times\to J/K^\times$ is an isomorphism.*

Proof. Since $J_S\cap K^\times=o_S^\times$, the map is injective. Let $x\in J$. Then, since o_S has class number 1, we can find an element of K with specified valuation at all places outside S. In particular, we can find a $y\in K^\times$ such that $yx\in J_S$. □

We can then rewrite

$$F_{C,G}(s,\phi)=\sum_{\substack{\chi:J_S/o_S^\times\to G\\ \forall v\in S\ \ \chi_v=\phi_v}}\frac{1}{C(\chi)^s}.$$

We shall study characters on J_S, and then check their behavior on the finitely generated group $o_S^\times$ to see if they factor through $J_S/o_S^\times$. Let $\mathcal{A}=\prod_{i=1}^k o_S^\times/o_S^{\times n_i}$. Given a $\chi:J_S\to G$, with projection $\chi_i:J_S\to\mathbb{Z}/n_i$ (or the same from $K_v^\times$ or $o_v^\times$), and an $\epsilon=(\epsilon_1,\dots,\epsilon_k)\in\mathcal{A}$, we define $\dot\chi(\epsilon)=\prod_{i=1}^k\zeta_{n_i}^{\chi_i(\epsilon_i)}$, where we evaluate $\chi_i(\epsilon_i)$ using the natural map $o_S^\times\to J_S$ (or to $K_v^\times$ or $o_v^\times$). Note that the map χ has its image in G, the map χ_i has its image in $\mathbb{Z}/n_i$, and the map $\dot\chi$ has its image in the complex roots of unity. We define the twists

$$F_{C,G}(s,\epsilon,\phi)=\sum_{\substack{\chi:J_S\to G\\ \forall v\in S\ \ \chi_v=\phi_v}}\frac{\dot\chi(\epsilon)}{C(\chi)^s},$$

which we use with the following corollary of Lemma 2.8 (motivated by [Wri89, Equation (3.2)]).

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Corollary 2.9. *We have*

$$F_{C,G}(s,\phi)=\frac{1}{|\mathcal{A}|}\sum_{\epsilon\in\mathcal{A}}F_{C,G}(s,\epsilon,\phi).$$

Proof. We rearrange the sum to obtain

$$\sum_{\epsilon\in\mathcal{A}}F_{C,G}(s,\epsilon,\phi)=\sum_{\substack{\chi:J_S\to G\\ \forall v\in S\ \chi_v=\phi_v}}\frac{1}{C(\chi)^s}\sum_{\epsilon_1\in o_S^\times/o_S^{n_1}}\zeta_{n_1}^{\chi_1(\epsilon_1)}\cdots\sum_{\epsilon_k\in o_S^\times/o_S^{n_k}}\zeta_{n_k}^{\chi_k(\epsilon_k)}.$$

We note that $\zeta_{n_i}^{\chi_i(\epsilon_i)}$ is a complex valued character on the finite group $o_S^\times/o_S^{n_i}$ and thus the sum $\sum_{\epsilon_i\in o_S^\times/o_S^{n_i}}\zeta_{n_i}^{\chi_i(\epsilon_i)}$ is $|o_S^\times/o_S^{n_i}|$ if χ_i is trivial on $o_S^\times$ and 0 otherwise. □

The $F_{C,G}(s,\epsilon,\phi)$ are convenient to work with because they have Euler products (as in [Wri89, Equation (3.4)])

$$F_{C,G}(s,\epsilon,\phi)=\prod_{v\notin S}\bigg(\sum_{\chi_v:o_v^\times\to G}\frac{\dot{\chi_v}(\epsilon)}{Nv^{c(\chi_v)s}}\bigg)\prod_{v\in S}\frac{\dot{\phi_v}(\epsilon)}{Nv^{c(\phi_v)s}}.$$

In this paper, all products over $v\notin S$ are products over the places of K not in S.

2.5 Proof of main Theorem 2.1

We will now see how Theorem 2.1 will follow from three lemmas, all of which will be proven in § 2.6. Recall that $m=\min_{g\in G\setminus\{1\}}c_G(g)$ and $\mathfrak{M}=c_G^{-1}(m)$. We will prove the following lemma by relating $F_{C,G}(s,\epsilon,\phi)$ to L-functions whose analytic behavior we already know.

Lemma 2.10. *For any counting function C, the product $F_{C,G}(s,\epsilon,\phi)$ absolutely converges in* $\mathrm{Re}(s)>1/m$ *and has a meromorphic continuation to* $\mathrm{Re}(s)\geqslant 1/m$*, analytic away from $s=1/m$. The pole of $F_{C,G}(s,1,\phi)$ at $s=1/m$ is of order*

$$\sum_{g\in\mathfrak{M}}\frac{1}{[K(\zeta_{r_g}):K]},$$

where r_g is the order of g in G.

Thus we also obtain a meromorphic continuation to $\mathrm{Re}(s)\geqslant 1/m$ for $F_{C,G}(s,\phi)$ and $N_{C,G}(s,\phi)$. Lemma 2.10 will allow us to use a Tauberian theorem (see [Nar83, Corollary, p. 121]) to find the probabilities Pr_C. In the application of the Tauberian theorem, we will need to know which terms of $F_{C,G}(s,\phi)$ contribute to the main pole, and the following lemma will tell us just that.

Lemma 2.11. *For a counting function C, there is a subgroup $\mathcal{E}(C)$ of $\mathcal{A}$ such that if $\epsilon\in\mathcal{E}(C)$ then $F_{C,G}(s,\epsilon,\phi)$ has a pole of the same order at $s=1/m$ as $F_{C,G}(s,1,\phi)$, and if $\epsilon\notin\mathcal{E}(C)$ then $F_{C,G}(s,\epsilon,\phi)$ has a pole of smaller order (possibly equal to zero) than that of $F_{C,G}(s,1,\phi)$.*

The following lemma will allow us to simplify the probabilities we obtain into a reasonable form for fair counting functions.

Lemma 2.12. *If C is fair, $v\notin S$, and $\chi_v:o_v^\times\to G$, then for all $e\in\mathcal{E}(C)$, we have $\chi_v(e)=0$.*

Using these lemmas, we can prove Theorem 2.1.

Proof of Theorem 2.1. Assume C is fair. We have the Euler product

$$F_{C,G}(s,\epsilon,\phi)=\prod_{v\notin S}\bigg(\sum_{\chi_v:o_v^\times\to G}\frac{\dot{\chi}_v(\epsilon)}{Nv^{c(\chi_v)s}}\bigg)\prod_{v\in S}\frac{\dot{\phi}_v(\epsilon)}{Nv^{c(\chi_v)s}}.$$

If $e\in\mathcal{E}(C)$, and $\epsilon\in\mathcal{A}$, Lemma 2.12 implies that

$$F_{C,G}(s,e\epsilon,\phi)=F_{C,G}(s,\epsilon,\phi)\prod_{v\in S}\dot{\phi}_v(e). \tag{2}$$

Thus,

$$\begin{aligned}F_{C,G}(s,\phi)&=\frac{1}{|\mathcal{A}|}\sum_{\epsilon\in\mathcal{A}}F_{C,G}(s,\epsilon,\phi)\\&=\frac{1}{|\mathcal{A}|}\sum_{\epsilon\in\mathcal{A}/\mathcal{E}(C)}\sum_{e\in\mathcal{E}(C)}F_{C,G}(s,\epsilon,\phi)\prod_{v\in S}\dot{\phi}_v(e)\\&=\frac{1}{|\mathcal{A}|}\sum_{\epsilon\in\mathcal{A}/\mathcal{E}(C)}F_{C,G}(s,\epsilon,\phi)\sum_{e\in\mathcal{E}(C)}\prod_{v\in S}\dot{\phi}_v(e),\end{aligned} \tag{3}$$

where $\mathcal{A}/\mathcal{E}(C)$ denotes a set of coset representatives for the quotient of $\mathcal{A}$ by $\mathcal{E}(C)$.

For g and h meromorphic functions on $\mathrm{Re}(s)\geqslant 1/m$, analytic away from $s=1/m$, we use $g\sim_m h$ to denote that $g-h$ has a pole at $1/m$ of lesser order than the pole of g (or that at $(1/m)$ the function $g-h$ has no pole and g has a pole).

Case I: If $\prod_{v\in S}\dot{\phi}_v$ is not the trivial character on $\mathcal{E}(C)$, we have

$$\sum_{e\in\mathcal{E}(C)}\prod_{v\in S}\dot{\phi}_v(e)=0$$

and thus $F_{C,G}(s,\phi)=0$. This means that there are no $\chi:J/K^\times\to G$ that for all $v\in S$ have $\chi_v=\phi_v$, and thus ϕ is associated to an inviable Σ.

Case II: If $\prod_{v\in S}\dot{\phi}_v$ is the trivial character on $\mathcal{E}(C)$. Then,

$$\begin{aligned}F_{C,G}(s,\phi)=&\ \frac{|\mathcal{E}(C)|}{|\mathcal{A}|}\sum_{\epsilon\in\mathcal{A}/\mathcal{E}(C)}F_{C,G}(s,\epsilon,\phi)\quad\text{by (3)}\\ \sim_m&\ \frac{|\mathcal{E}(C)|}{|\mathcal{A}|}F_{C,G}(s,1,\phi)\quad\text{by Lemma 2.11.}\end{aligned}$$

In particular, $F_{C,G}(s,\phi)$ has a pole of order $\sum_{g\in\mathfrak{M}}(1/[K(\zeta_{r_g}):K])$ (from Lemma 2.10) at $s=1/m$.

Now we can analyze the pole at $1/m$ of $N_{C,G}(s,\phi)$. Recall that we can write

$$N_{C,G}(s,\phi)=\sum_{H\text{ subgroup of }G}\mu(H,G)F_{C|_H,H}(s,\phi).$$

By Lemma 2.10, we know that, for H a proper subgroup of G, the maximum order of a pole of any $F_{C|_H,H}(s,\epsilon,\phi)$ and thus of any $F_{C|_H,H}(s,\phi)$ is $\sum_{g\in\mathfrak{M}\cap H}(1/[K(\zeta_{r_g}):K])$. For fair C, this is smaller than the order of the pole of $F_{C,G}(s,\phi)$, and thus

$$N_{C,G}(s,\phi)\sim_m F_{C,G}(s,\phi)\sim_m\frac{|\mathcal{E}(C)|}{|\mathcal{A}|}F_{C,G}(s,1,\phi).$$

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

In particular, $N_{C,G}(s,\phi)$ has a pole at $s=1/m$ and thus is not identically zero. So there are surjective $\chi : J/K^\times \to G$ that for all $v \in S$ have $\chi_v = \phi_v$. So, ϕ is associated to a viable Σ.

If we write

$$T_{C,G}(s) = \prod_{v \notin S} \biggl(\sum_{\chi_v : o_v^\times \to G} \frac{1}{Nv^{c(\chi_v)s}} \biggr),$$

then

$$N_{C,G}(s,\phi) \sim_m \frac{|\mathcal{E}(C)|}{|\mathcal{A}|} T_{C,G}(s) \prod_{v \in S} \frac{1}{Nv^{c(\phi_v)s}}.$$

Note that $T_{C,G}(s)$ does not depend on ϕ and has a pole at $1/m$. Let w be the order of the pole of $N_{C,G}(s,\phi)$ (or $T_{C,G}(s)$) at $1/m$. Let Σ be associated to ϕ. Let

$$N_{C,G}(\Sigma, X) = \#\{L \in E_G(K) \mid L_v \cong \Sigma_v \text{ for all } v \in S \text{ and } C(L) < X\}.$$

Then, for viable Σ, using a Tauberian theorem (as in [Nar83, Corollary, p. 121]), we obtain a positive finite limit

$$\lim_{X\to\infty} \frac{N_{C,G}(\Sigma, X)}{X^{1/m}(\log X)^{w-1}} = \lim_{s \to 1/m} \biggl[N_{C,G}(s,\Sigma) \biggl(s - \frac{1}{m} \biggr)^w \biggr] \frac{m}{\Gamma(w)},$$

where Γ is the Gamma function. Summing over the finitely many Σ on S, we have that

$$\lim_{X\to\infty} \frac{\#\{L \in E_G(K) | C(L) < X\}}{X^{1/m}(\log X)^{p-1}}$$

is a positive finite constant. Thus for viable Σ on S, we have $\mathrm{Pr}_C(\Sigma) > 0$.

It follows that for a fair counting function C and Σ and Σ' viable local specifications on S, we have

$$\frac{\mathrm{Pr}_C(\Sigma)}{\mathrm{Pr}_C(\Sigma')} = \lim_{X\to\infty} \frac{N_{C,G}(\Sigma_1, X)}{N_{C,G}(\Sigma_2, X)} = \frac{\prod_{v\in S}(1/Nv^{c(\Sigma_v)/m})}{\prod_{v\in S}(1/Nv^{c(\Sigma'_v)/m})}.$$

We have required that S is sufficiently large to contain certain places depending on G and K and from our requirements it follows that $S_0 \subset S$. Thus, since Σ and Σ' are viable, we have $\tilde{\Sigma}, \tilde{\Sigma}' \subset A$ and

$$P_C(\tilde{\Sigma}|A) = \frac{P_C(\tilde{\Sigma})}{P_C(A)}.$$

We then conclude that

$$\frac{\mathrm{Pr}_C(\Sigma)}{\mathrm{Pr}_C(\Sigma')} = \frac{P_C(\tilde{\Sigma})}{P_C(\tilde{\Sigma}')} = \frac{P_C(\tilde{\Sigma}|A)}{P_C(\tilde{\Sigma}'|A)}.$$

This proves Theorem 2.1 in the case when S is sufficiently large.

Consider a local specification Σ' on $S' \subset S$. Then, we see that

$$\mathrm{Pr}_C(\Sigma') = \sum_{\substack{\text{viable } \Sigma \text{ on } S, \\ \text{restricting to } \Sigma' \text{ on } S'}} \mathrm{Pr}_C(\Sigma) = \sum_{\substack{\text{viable } \Sigma \text{ on } S, \\ \text{restricting to } \Sigma' \text{ on } S'}} \frac{P_C(\tilde{\Sigma})}{P_C(A)} = \frac{P_C(\tilde{\Sigma}' \cap A)}{P_C(A)},$$

which proves Theorem 2.1. □

2.6 Analytic continuation of $F_{C,G}(s,\epsilon,\phi)$

In this section we prove Lemmas 2.10, 2.11, and 2.12, the content of which we now remind the reader.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

For any counting function C, the product $F_{C,G}(s,\epsilon,\phi)$ absolutely converges in $\mathrm{Re}(s)>1/m$ *and has a meromorphic continuation to* $\mathrm{Re}(s)\geqslant 1/m$*, analytic away from* $s=1/m$*. The pole of* $F_{C,G}(s,1,\phi)$ *at* $s=1/m$ *is of order*

$$\sum_{g\in\mathfrak{M}}\frac{1}{[K(\zeta_{r_g}):K]},$$

where r_g is the order of g in G.

For a counting function C, there is a subgroup $\mathcal{E}(C)$ of $\mathcal{A}$ such that if $\epsilon\in\mathcal{E}(C)$ then $F_{C,G}(s,\epsilon,\phi)$ has a pole of the same order at $s=1/m$ as $F_{C,G}(s,1,\phi)$, and if $\epsilon\notin\mathcal{E}(C)$ then $F_{C,G}(s,\epsilon,\phi)$ has a pole of lesser (possibly zero) order than $F_{C,G}(s,1,\phi)$.

If C is fair, $v\notin S$, and $\chi_v: o_v^\times\to G$, then, for all $e\in\mathcal{E}(C)$, we have $\chi_v(e)=0$.

We see easily that $F_{C,G}(s,\epsilon,\phi)$ (as well as all other products we consider in this subsection) converges absolutely and uniformly on $\mathrm{Re}(s)>1/m$. So, we will investigate the behavior at $1/m$ by manipulating the Euler product for $F_{C,G}(s,\epsilon,\phi)$ until it resembles a product of L-functions. This strategy was motivated by the work of Taylor [Tay84, § 3], who related $F_{C,G}(s,\epsilon,\phi)$ to L-functions for C the conductor and G cyclic, although we face additional challenges both from general C and G not necessarily cyclic.

We use the following lemma to interchange sums and products, which is possible because we are only looking for behavior at $1/m$ and so higher-order terms will not contribute. For g and h analytic functions on $\mathrm{Re}(s)>1/m$, we use $g\approx_m h$ to denote that g/h has an analytic continuation to $\mathrm{Re}(s)\geqslant 1/m$.

Lemma 2.13. *Let m and M be positive reals. Let K be a number field and, for each place v of K, let $P_v(x)=1+\sum_{i=1}^{M}b_{v,i}x^{\alpha_{v,i}}$, where $m\leqslant\alpha_{v,i}$ and $b_{v,i}\in\mathbb{C}$ with $|b_{v,i}|\leqslant M$. Then for some large Y we have*

$$\prod_v P_v(Nv^{-s})\approx_m\prod_{\substack{v\\ Nv>Y}}\prod_{i=1}^{M}(1+b_{v,i}Nv^{-\alpha_{v,i}s})$$

(where the products over v are over all finite places v of K satisfying the condition).

Proof. We can bound the absolute value of each factor of $\prod_v P_v(Nv^{-s})$ by $1+M^2Nv^{-ms}$ and each factor of $\prod_v\prod_{i=1}^{M}(1+b_{v,i}Nv^{-\alpha_{v,i}s})$ by $(1+MNv^{-ms})^M$, and thus both products converge absolutely on $\mathrm{Re}(s)>1/m$. For sufficiently large v, the function $\prod_{i=1}^{M}(1+b_{v,i}Nv^{-\alpha_{v,i}s})$ has absolute value at least $1/2$ everywhere on $\mathrm{Re}(s)\geqslant 1/m$. For those v,

$$\left|\frac{P_v(Nv^{-s})}{\prod_{i=1}^{M}(1+b_{v,i}Nv^{-\alpha_{v,i}s})}\right|\leqslant 1+\frac{2^M M^M Nv^{-2ms}}{|\prod_{i=1}^{M}(1+b_{v,i}Nv^{-\alpha_{v,i}s})|}\leqslant 1+2^{M+1}M^M Nv^{-2ms}.$$

Thus we conclude the lemma. □

Now, we set our notation for the rest of the proof of Lemmas 2.10, 2.11, and 2.12.

Notation 2.14. A *division* of G is a set of all the invertible multiples of some element $x\in G$, in other words $\{y\mid y=ex \text{ and } x=fy \text{ for some } e,f\in\mathbb{Z}\}$. Let $\mathrm{Div}(G)$ be the set of non-identity divisions of G. For an element $g\in G$, let r_g be its order and for $d\in\mathrm{Div}(G)$, let r_d be the order of any element of d. Recall that any map from $o_v^\times$ to a finite group of order relatively prime to v factors through $(o_v/v)^\times$.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

We now make a specific choice, for all places $v \nmid |G|$, of a generator y_v of the tame inertia group of K_v (which is isomorphic to $(o_v/v)^\times$). Our choice is that $y_v \equiv \zeta_{Nv-1} \pmod{v}$, where ζ_{Nv-1} is the primitive $(Nv-1)$th root of unity we fixed just before § 2.3.

Since $c(\chi_v)$ only depends on the division of $\chi_v(y_v)$, for a division d we can write $c(d)$ to denote $c(\chi_v)$ for any χ_v that sends y_v to an element of d.

We now rearrange $F_{C,G}(s, \epsilon, \phi)$ as follows:

$$F_G(s, \epsilon, \phi) \approx_m \prod_{v \notin S} \bigg(\sum_{\chi_v : o_v^\times \to G} \frac{\dot{\chi_v}(\epsilon)}{Nv^{c(\chi_v)s}} \bigg)$$

$$= \prod_{v \notin S} \bigg(1 + \sum_{d \in \mathrm{Div}(G)} \sum_{g \in d} \sum_{\substack{\chi_v : o_v^\times \to G \\ \chi_v(y_v) = g}} \frac{\dot{\chi_v}(\epsilon)}{Nv^{c(d)s}} \bigg).$$

The sum over $\chi_v : o_v^\times \to G$ such that $\chi_v(y_v) = g$ has at most one term, but we keep the summation sign for notational convenience. So we have

$$F_G(s, \epsilon, \phi) \approx_m \prod_{\substack{v \notin S \\ Nv > Y}} \prod_{d \in \mathrm{Div}(G)} \prod_{g \in d} \bigg(1 + \sum_{\substack{\chi_v : o_v^\times \to G \\ \chi_v(y_v) = g}} \frac{\dot{\chi_v}(\epsilon)}{Nv^{c(d)s}} \bigg) \quad \text{by Lemma 2.13}$$

$$= \prod_{d \in \mathrm{Div}(G)} \prod_{\substack{v \notin S \\ Nv \equiv 1 \ (\mathrm{mod}\ r_d) \\ Nv > Y}} \prod_{g \in d} \bigg(1 + \frac{1}{Nv^{c(d)s}} \sum_{\substack{\chi_v : o_v^\times \to G \\ \chi_v(y_v) = g}} \dot{\chi_v}(\epsilon) \bigg).$$

Only v with $Nv \equiv 1 \pmod{r_d}$ have $\chi : o_v^\times \to G$ such that $\chi_v(y_v) \in d$.

Now we prove the following lemmas in order to evaluate the term $\dot{\chi_v}(\epsilon)$ in the above. Our strategy to evaluate $\dot{\chi_v}(\epsilon)$ is motivated by the work of Taylor [Tay84], who calculated the order of $\dot{\chi_v}(\epsilon)$ for G cyclic. For non-cyclic G, we need to take advantage of our choice of y_v.

Lemma 2.15. *We have*

$$\zeta_{Nv-1} = \frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}},$$

where the Frobenius is in the Galois group of the maximal unramified extension of K_v.

Proof. Note that K_v contains the $(Nv-1)$th roots of unity and so

$$\frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}}$$

does not depend on the choice of root of y_v. We know that both ζ_{Nv-1} and

$$\frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}}$$

are $(Nv-1)$th roots of unity, and that those roots of unity inject into $(o_v/v)^\times$. Thus we can prove the lemma modulo v. There we have

$$\frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}} \equiv y_v^{(Nv-1)/(Nv-1)} \equiv y_v \equiv \zeta_{Nv-1},$$

where the last equality is by choice of y_v. □

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Lemma 2.16. *Let $v \nmid n\infty$ and $\chi_v(y_v) = g$. Suppose the projections of g to the $\mathbb{Z}/n_i\mathbb{Z}$ are $n_i k_i/\ell_i \in \mathbb{Z}/n_i\mathbb{Z}$, where $\ell_i \mid n_i$ and $(k_i, \ell_i) = 1$. Let ϵ^g be notation for $\prod_{i=1}^k \epsilon_i^{k_i/\ell_i}$, and let w_v be a prime of $K(\zeta_{r_g})$ over v. Then*

$$\dot{\chi}_v(\epsilon) = \prod_{i=1}^{k} \frac{\mathrm{Frob}_{w_v}(\epsilon_i^{k_i/\ell_i})}{\epsilon_i^{k_i/\ell_i}} = \frac{\mathrm{Frob}_{w_v}(\epsilon^g)}{\epsilon^g},$$

where the Frobenius is in the Galois group of the maximal extension of $K(\zeta_{r_g})$ unramified outside S.

Proof. Note that $\ell_i \mid r_g$. Since χ_v factors through $(o_v/v)^\times$ and y_v has order $Nv - 1$ in $(o_v/v)^\times$, we also have that $r_g \mid Nv - 1$. In $(o_v/v)^\times$, write $\epsilon_i = y_v^{b_i}$ so that in K_v we have $\epsilon_i u_i = y_v^{b_i}$, where u_i is a unit congruent to 1 modulo v. We have that

$$\dot{\chi}_{vi}(\epsilon_i) = \zeta_{n_i}^{\chi_{vi}(\epsilon_i)} = \zeta_{n_i}^{b_i \chi_{vi}(y_v)} = \zeta_{n_i}^{n_i k_i b_i/\ell_i} = \zeta_{\ell_i}^{k_i b_i} = \zeta_{Nv-1}^{(Nv-1)k_i b_i/\ell_i}.$$

From Lemma 2.15, we have

$$\zeta_{Nv-1} = \frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}},$$

where the Frobenius is in the Galois group of the maximal unramified extension of K_v. Thus

$$\dot{\chi}_{vi}(\epsilon_i) = \left(\frac{\mathrm{Frob}_v(y_v^{1/(Nv-1)})}{y_v^{1/(Nv-1)}}\right)^{(Nv-1)k_i b_i/\ell_i} = \frac{\mathrm{Frob}_v(y_v^{k_i b_i/\ell_i})}{y_v^{k_i b_i/\ell_i}} = \frac{\mathrm{Frob}_v(\epsilon_i^{k_i/\ell_i})\,\mathrm{Frob}_v(u_i^{k_i/\ell_i})}{\epsilon_i^{k_i/\ell_i} u_i^{k_i/\ell_i}},$$

where the Frobenius is still in the Galois group of the maximal unramified extension of K_v. Since u_i is a unit congruent to 1 modulo v and $\ell_i \mid Nv - 1$, we have that all the ℓ_ith roots of u_i are in $K_v = K(\zeta_r)_w$ and that $\mathrm{Frob}_v(u_i^{k_i/\ell_i}) = u_i^{k_i/\ell_i}$. Note that $K_v = K(\zeta_{r_g})_{w_v}$ since $r_g | Nv - 1$, and thus we can replace Frob_v with the Frobenius of w_v in $K(\zeta_{r_g})_{w_v}$. We thus have

$$\dot{\chi}_{vi}(\epsilon_i) = \frac{\mathrm{Frob}_{w_v}(\epsilon_i^{k_i/\ell_i})}{\epsilon_i^{k_i/\ell_i}}.$$

Since the ℓ_ith roots of ϵ_i are in the maximal extension of $K(\zeta_{r_g})$ unramified outside S, we can interpret the Frobenius as the Frobenius of w_v in the Galois group of the maximal extension of $K(\zeta_{r_g})$ unramified outside S in the statement of the lemma. Note that $K(\zeta_{r_g})$ contains the ℓ_ith roots of unity and so $\mathrm{Frob}_v(\epsilon_i^{k_i/\ell_i})/\epsilon_i^{k_i/\ell_i}$ does not depend on the choice of root of ϵ_i. □

Using Lemma 2.16 and its definitions of ϵ^g, w_v, and Frob, we have

$$\begin{aligned} F_{C,G}(s, \epsilon, \phi) &\approx_m \prod_{d \in \mathrm{Div}(G)} \prod_{\substack{v \notin S \\ Nv \equiv 1 \ (\mathrm{mod}\ r_d) \\ Nv > Y}} \prod_{g \in d} \left(1 + \frac{1}{Nv^{c(d)s}} \sum_{\substack{\chi_v : o_v^\times \to G \\ \chi_v(y_v) = g}} \dot{\chi}_v(\epsilon)\right) \\ &= \prod_{d \in \mathrm{Div}(G)} \prod_{\substack{v \notin S \\ Nv \equiv 1 \ (\mathrm{mod}\ r_d) \\ Nv > Y}} \prod_{g \in d} \left(1 + \frac{1}{Nv^{c(d)s}} \frac{\mathrm{Frob}_{w_v}(\epsilon^g)}{\epsilon^g}\right). \end{aligned}$$

We now partition $\mathrm{Div}(G)$ into $\mathrm{Div}^0(\epsilon, G)$, the divisions whose elements g have $\epsilon^g \in K(\zeta_{r_g})$, and $\mathrm{Div}^+(\epsilon, G)$, the divisions whose elements g have $\epsilon^g \notin K(\zeta_{r_g})$. Let $t(r) := [K(\zeta_r) : K]$. We factor the last product above into two factors $A(s)$ and $B(s)$, defined below.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

We have

$$\begin{aligned} A(s) := &\prod_{d\in \mathrm{Div}^0(\epsilon,G)} \prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{g\in d}\left(1+\frac{1}{Nv^{c(d)s}}\frac{\mathrm{Frob}_{w_v}(\epsilon^g)}{\epsilon^g}\right)\\ = &\prod_{d\in \mathrm{Div}^0(\epsilon,G)} \prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{g\in d}\left(1+\frac{1}{Nv^{c(d)s}}\right)\\ = &\prod_{d\in \mathrm{Div}^0(\epsilon,G)} \prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{w\mid v}\left(1+\frac{1}{Nv^{c(d)s}}\right)^{\phi(r_d)/t(r_d)}, \end{aligned}$$

where the last product is over the primes w of $K(\zeta_{r_d})$ over v. Note that $\phi(r_d)/t(r_d)$ is an integer. By the standard argument about only degree one primes contributing to the pole, we have

$$\prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{w\mid v}\left(1+\frac{1}{Nv^{c(d)s}}\right) \approx_m \zeta_{K(\zeta_{r_d})}(c(d)s).$$

Thus

$$A(s) \approx_m \prod_{d\in \mathrm{Div}^0(\epsilon,G)} \zeta_{K(\zeta_{r_d})}(c(d)s)^{\phi(r_d)/t(r_d)}.$$

We define

$$B(s) := \prod_{d\in \mathrm{Div}^+(\epsilon,G)} \prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{g\in d}\left(1+\frac{1}{Nv^{c(d)s}}\frac{\mathrm{Frob}_{w_v}(\epsilon^g)}{\epsilon^g}\right).$$

Let N be the least common multiple of the n_i, and note that, since $r_d \mid N$, we have that $t(r_d) \mid t(N)$. We now have

$$B(s)^{t(N)} = \prod_{d\in \mathrm{Div}^+(\epsilon,G)} \prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{g\in d}\prod_{w\mid v}\left(1+\frac{1}{Nv^{c(d)s}}\frac{\mathrm{Frob}_{w}(\epsilon^g)}{\epsilon^g}\right)^{t(N)/t(r_d)},$$

where the last product is over the primes w of $K(\zeta_{r_d})$ over v. For $d \in \mathrm{Div}^+(\epsilon, G)$ we have that $K(\zeta_{r_d}, \epsilon^g)/K(\zeta_{r_d})$ is abelian and non-trivial. Thus there is a non-trivial Hecke character θ_{ϵ^g} for $K(\zeta_{r_d})$ such that $\mathrm{Frob}_w(\epsilon^g)/\epsilon^g$ is $\theta_{\epsilon^g}(w)$. Again by standard arguments we have

$$\prod_{\substack{v\notin S\\ Nv\equiv 1 \ (\mathrm{mod}\ r_d)\\ Nv>Y}} \prod_{w\mid v}\left(1+\frac{\mathrm{Frob}_{w}(\epsilon^g)}{\epsilon^g}\frac{1}{Nv^{c(d)s}}\right) \approx_m L(c(d)s, \theta_{\epsilon^g})$$

and thus we can write

$$B(s)^{t(N)} = g(s) \prod_{d\in \mathrm{Div}^+(\epsilon,G)} \prod_{g\in d} L(c(d)s, \theta_{\epsilon^g})^{t(N)/t(r_d)},$$

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

where $g(s)$ is analytic in $\operatorname{Re}(s) \geqslant 1/m$. We know that $L(c(d)s, \theta_{\epsilon^g})$ not only has an analytic continuation to $\operatorname{Re}(s) \geqslant 1/m$ but is also non-zero in that region. We can check that $g(s)$ is also non-zero in $\operatorname{Re}(s) \geqslant 1/m$. Thus $B(s)$ has an analytic continuation to $\operatorname{Re}(s) \geqslant 1/m$.

Thus, we conclude that

$$F_{C,G}(s, \epsilon, \phi) \approx_m \prod_{d \in \operatorname{Div}^0(\epsilon, G)} \zeta_{K(\zeta_{r_d})}(c(d)s)^{\phi(r)/t(r_d)}.$$

So, $F_{C,G}(s, \epsilon, \phi)$ has a meromorphic continuation to $\operatorname{Re}(s) \geqslant 1/m$ analytic away from $s = 1/m$. The pole of $F_{C,G}(s, \epsilon, \phi)$ at $1/m$ is of order

$$\sum_{\substack{d \in \operatorname{Div}^0(\epsilon,G) \\ c(d)=m}} \frac{\phi(r_d)}{t(r_d)} = \sum_{d \in \operatorname{Div}^0(\epsilon,G) \cap \mathfrak{M}} \frac{\phi(r_d)}{t(r_d)} = \sum_{d \in \operatorname{Div}^0(\epsilon,G) \cap \mathfrak{M}} \sum_{g \in d} \frac{1}{t(r_g)} = \sum_{g \in G(\epsilon) \cap \mathfrak{M}} \frac{1}{t(r_g)},$$

where $G(\epsilon)$ is the set of $g \in G$ such that $\epsilon^g \in K(\zeta_{r_g})$. Note that $G(1) = G$. This proves Lemma 2.10. The maximal order pole among terms $F_{C,G}(s, \epsilon, \phi)$ is in $F_{C,G}(s, 1, \phi)$, and any other $F_{C,G}(s, \epsilon, \phi)$ has that same order pole if and only if $\mathfrak{M} \subset G(\epsilon)$. Let $\mathcal{E}(C)$ be the elements $\epsilon \in \mathcal{A}$ such that $\mathfrak{M} \subset G(\epsilon)$. It is easy to see that $\mathcal{E}(C)$ is a subgroup, and this proves Lemma 2.11. Lemma 2.12 will follow from the next result.

Lemma 2.17. *For a fair counting function C, and $\epsilon \in \mathcal{E}(C)$, we have ${\epsilon_j}^{1/r} \in K(\zeta_r)$ for all $r \mid n_j$.*

Proof. Fix a j with $1 \leqslant j \leqslant k$ and an r dividing n_j. Let g be the element of G with jth projection n_j/r and all other projections 0. Since g is of order r and C is fair, we can write $\sum_{s=1}^{\ell} g_s = g$, where g_s are elements of $\mathfrak{M}$ and all g_s have order dividing r. Write $g_s = (g_{s,1}, \dots, g_{s,k})$ according to our chosen factorization of G. We can write $g_{s,i} = n_i h_{s,i}/\ell_{s,i}$ with $(h_{s,i}, \ell_{s,i}) = 1$. Since g_s is of order dividing r, we must have $\ell_{s,i} | r$. Thus by definition of $\mathcal{E}(C)$ we have

$$\epsilon^{g_s} = \prod_{i=1}^{k} \epsilon_i^{h_{s,i}/\ell_{s,i}} \in K(\zeta_r).$$

We then see that

$$\prod_{s=1}^{\ell} \prod_{i=1}^{k} \epsilon_i^{h_{s,i}/\ell_{s,i}} \in K(\zeta_r).$$

By the choice of the g_s, we have that $\sum_{s=1}^{\ell} n_i h_{s,i}/\ell_{s,i}$ (as a sum in $\mathbb{Z}/n_i$) is n_j/r if $i = j$ and 0 otherwise. Equivalently, $\sum_{s=1}^{\ell} (h_{s,i}/\ell_{s,i})$ (as a sum in $\mathbb{Q}/\mathbb{Z}$) is $1/r$ if $i = j$ and 0 otherwise. Thus, we conclude that $\prod_{s=1}^{\ell} \prod_{i=1}^{k} \epsilon_i^{h_{s,i}/d_{s,i}}$ is ${\epsilon_j}^{1/r}$ times an element of $K^\times$, and thus ${\epsilon_j}^{1/r} \in K(\zeta_r)$. □

Suppose C is fair, $v \notin S$, and we have a $\chi : o_v^\times \rightarrow G$ of order r, with projection to $\mathbb{Z}/n_i\mathbb{Z}$ of order ℓ_i. Then $Nv \equiv 1 \pmod{r}$, and thus for all i we have $K_v = K_v(\zeta_{\ell_i})$. So, for all $\epsilon \in \mathcal{E}(C)$, we have ${\epsilon_j}^{1/\ell_j} \in K(\zeta_{\ell_j})$, which implies that ${\epsilon_j}^{1/\ell_j} \in K_v(\zeta_{\ell_j}) = K_v$, and thus ϵ_j is an ℓ_jth power in $o_v^\times$ for all j. We conclude that $\dot{\chi}_v(\epsilon) = 0$, which proves Lemma 2.12.

Remark 2.18. By definition, $\mathcal{E}(C)$ depends on our choice of C. However, given that C is fair, by Lemma 2.17, we see that for $\epsilon \in \mathcal{E}(C)$ we have $\epsilon^g \in K(\zeta_{r_g})$ for *all* $g \in G$. If $\epsilon \in \mathcal{A}$ is such that $\epsilon^g \in K(\zeta_{r_g})$ for *all* $g \in G$, then $\epsilon \in \mathcal{E}(C)$. Thus if C is fair, we see that $\mathcal{E}(C)$ is the subgroup of ϵ such that $\epsilon^g \in K(\zeta_{r_g})$ for all $g \in G$, and thus does not depend on C.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

3. Counting by conductor

In the proof of Theorem 2.1 in § 2.5, we have implicitly found the asymptotics of

$$N_{C,G}(X) := \#\{L \in E_G(K) | C(L) < X\},$$

for any fair counting function C. We state those asymptotics here. Recall the definition of S_0 from § 2 as follows. Let $\eta_i = \zeta_{2^i} + \zeta_{2^i}^{-1}$, where ζ_{2^i} is a primitive 2^ith root of unity. Let s_K be maximal such that $\eta_{s_K} \in K$. If 2^{s_K+1} does not divide the exponent of G, then let $S_0(K) = \emptyset$. Otherwise, let $S_0(K)$ be the set of primes $\wp$ of K dividing 2 such that none of -1, $2+\eta_{s_K}$, and $-2-\eta_{s_K}$ are squares in $K_\wp$.

Theorem 3.1. *For a fair counting function C, we have*

$$\begin{aligned}
&\lim_{X\to\infty} \frac{N_{C,G}(X)}{X^{m_C}(\log X)^{w_{K,C}-1}} \\
&\quad= \frac{\mathrm{Sp}(K,G)}{m_C^{w_{K,C}-1}(w_{K,C}-1)!|G|^{|S_0(K)|}\prod_i |o_K^\times/o_K^{n_i}|} \\
&\quad\quad \times \prod_{\substack{v\notin S_0(K)\\ v \text{ finite}}} \Bigg(\bigg(\sum_{\chi_v : o_v^\times \to G} \frac{1}{Nv^{c(\chi_v)/m_C}}\bigg)\bigg(1-\frac{1}{Nv}\bigg)^{w_{K,C}}\Bigg) \\
&\quad\quad\quad \cdot \Bigg(\sum_{\substack{\Sigma \text{ viable local}\\ \text{specification of } G\text{-structured}\\ \text{algebras on } S_0(K)}} \prod_{v\in S_0(K)} \frac{1}{Nv^{c(\Sigma_v)/m_C}}\bigg(1-\frac{1}{Nv}\bigg)^{w_{K,C}}\Bigg) \prod_{v|\infty}\bigg(\sum_{G_{K_v}\to G} 1\bigg),
\end{aligned}$$

where $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, $m_C = \min_{g\in G\setminus\{0\}} c_G(g)$, $\mathfrak{M} = c_G^{-1}(m)$, r_g is the order of $g \in G$, ζ_j are the jth roots of unity,

$$w_{K,C} = \sum_{g\in\mathfrak{M}} \frac{1}{[K(\zeta_{r_g}) : K]},$$

$h_{G,K}$ is the number of i such that $2^{s_K+1}|n_i$,

$$Sp(K,G) = \begin{cases} 2^{h_{G,K}} & \text{if none of } -1,\ 2+\eta_s, \text{ and } -2-\eta_s \text{ are squares in } K, \\ 1 & \text{otherwise,} \end{cases}$$

o_K is the ring of integers in K, G_F is the absolute Galois group of F, o_v is the ring of integers of K_v, and all products are over places of K.

We can also specialize to the case that the counting function is $\mathfrak{f}$, the norm of the conductor to $\mathbb{Q}$. In this case $m_\mathfrak{f} = 1$ and $\mathfrak{M} = G \setminus \{0\}$ and so the expression in Theorem 3.1 simplifies slightly.

Proof. This result follows from the analysis of Section 2.5. We simplify the constant that one obtains using that analysis by applying

$$\lim_{s\to 1/m}\left[\zeta_K(sm)\left(s-\frac{1}{m}\right)\right] = \frac{1}{m}$$

and the following two lemmas.

Lemma 3.2. *For fair C, we have $|\mathcal{E}(C)| = Sp(K,G)$.*

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Proof. We know from Lemma 2.17 that $\epsilon \in \mathcal{E}(C)$ implies that for all $\ell_i \mid n_i$ we have $\epsilon_i^{1/\ell_i} \in K(\zeta_{\ell_i})$. If $v \notin S$, and $(Nv-1, n_i) = \ell_i$, then ϵ_i is an n_ith power in K_v if and only if it is an ℓ_ith power in K_v. Since $\ell_i \mid Nv-1$, we have $K_v(\zeta_{\ell_i}) = K_v$, and thus $\epsilon_i^{1/n_i} \in K_v$. By [AT68, ch. 10, Theorem 1], it follows that either (i) ϵ_i is an n_ith power in K or (ii) $\epsilon_i \in b_0^{n_i/2}K^{n_i}$, where $b_0 = 2 + \eta_{s_K} = (1 + \zeta_{2^{s_K}})^2$. Also, the second case only occurs when none of -1, $2 + \eta_{s_K}$, and $-2 - \eta_{s_K}$ are squares in K and when $2^{s_K+1} \mid n_i$.

Next, we will see that any ϵ such that $\epsilon_i = b_0^{n_i/2}$ and $2^{s_K+1} \mid n_i$ for some $i \in I$ and $\epsilon_j = 1$ for all $j \notin I$ is in $\mathcal{E}(C)$. First note that b_0 is a unit at all places not dividing 2, and so it will be in $o_S^\times$ as long as S contains 2 (which we have required when $|G|$ is even). We can reduce to the case that $I = \{i\}$. Then we need to conclude that $b_0^{n_i/2} \in K(\zeta_{\ell_i})^{\ell_i}$ for all $\ell_i \mid n_i$. We can easily reduce to the case that n_i is a power of 2 (e.g., by choosing the n_i to be prime powers originally). We know that $b_0^{n_i/2} \in K^{n_i/2}$. If $\ell_i = n_i$, then $K(\zeta_{\ell_i})$ contains $\zeta_{2^{s_K}}$ (because $2^{s_K} \mid n_i$) and thus $b_0^{n_i/2}$ is an ℓ_ith power in $K(\zeta_{\ell_i})$.

We see that $\mathcal{E}(C)$ is trivial when any of -1, $2 + \eta_{s_K}$, and $-2 - \eta_{s_K}$ are squares in K. Otherwise, $\mathcal{E}(C)$ contains exactly the ϵ that have $\epsilon_i = 1$ where $2^{s_K+1} \nmid n_i$ and that have $\epsilon_i = 1$ or $b_0^{n_i/2}$ at all other i. From [AT68, ch. 10, Theorem 1] we know that $b_0^{n_i/2}$ is not an n_ith power in K when none of -1, $2 + \eta_{s_K}$, and $-2 - \eta_{s_K}$ are squares in K and $2^{s_K+1} \mid n_i$. This proves the lemma. □

The next lemma follows from the fact that a local specification of G-structured algebras on S containing $S_0(K)$ is viable if and only if its restriction to S_0 is viable (see [AT68, ch. 10, Theorem 5]). Also recall Lemma 2.6, which gives the correspondence between G-structured algebras and Galois representations.

Lemma 3.3. *For S containing $S_0(K)$,*

$$\sum_{\substack{\Sigma \text{ viable local}\\ \text{specification of } G\text{-structured}\\ \text{algebras on } S}} \prod_{v\in S} \frac{1}{Nv^{c(\Sigma_v)/m_C}}$$

$$= \prod_{v\in S\setminus S_0}\left(|G| \sum_{\chi_v : o_v^\times \to G} \frac{1}{Nv^{c(\chi_v)/m_C}}\right) \sum_{\substack{\Sigma \text{ viable local}\\ \text{specification of } G\text{-structured}\\ \text{algebras on } S_0(K)}} \prod_{v\in S_0(K)} \frac{1}{Nv^{c(\Sigma_v)/m_C}}.$$

This completes the proof of Theorem 3.1. □

4. Discriminant probabilities

For this section, we work with the base field $K = \mathbb{Q}$. We show that when one replaces the conductor by the discriminant when defining probabilities in (1) (to define what we call *discriminant probabilities*), we do not in general have analogs of the nice behavior of Corollary 1.2 and Theorem 1.3. When G has prime exponent, the discriminant is a fixed power of the conductor, and so we do have analogs of Corollary 1.2 and Theorem 1.3. However, in the simplest case when G does not have prime exponent, that is $G = \mathbb{Z}/p^2\mathbb{Z}$ for p prime, we find examples of dependence of local behaviors at different places (Proposition 4.1), and examples where we do not have the Chebotarev probabilities for unramified splitting behavior (Proposition 4.4). As discussed in the introduction, Wright [Wri89] observed that for $G=\mathbb{Z}/4\mathbb{Z}$ the ratios of probabilities of local behaviors are apparently very complicated. Our propositions give concrete evidence for the suggestion of Wright that the discriminant probabilities are not well-behaved. We calculate the probabilities for the propositions below in a similar fashion to our work in § 2.

Proposition 4.1. *Let p, q_1, and q_2 be primes with $q_i \equiv 1 \pmod{p^2}$ for $i=1,2$. If $G=\mathbb{Z}/p^2\mathbb{Z}$, then q_1 ramifying and q_2 ramifying in a random G-extension are not discriminant independent.*

Proof. From Lemma 2.8 with S empty, we have $J/\mathbb{Q}^\times \cong \prod_p \mathbb{Z}_p^\times \times \mathbb{R}/\{\pm 1\}$, where the product is over finite places of $\mathbb{Q}$. We also have the following.

Lemma 4.2. *The natural map*

$$\operatorname{Hom}\biggl(\prod_p \mathbb{Z}_p^\times \times \mathbb{R}/\{\pm 1\}, G\biggr) \to \operatorname{Hom}\biggl(\prod_p \mathbb{Z}_p^\times, G\biggr),$$

sending $\chi \mapsto \chi(-,1)$, is an isomorphism.

We work as in § 2, but now we let Φ be a set of isomorphism classes of G-structured algebras at each place of S instead of just considering a single G-structured algebra. For the following computations, we let G be either $\mathbb{Z}/p^2\mathbb{Z}$ or $p\mathbb{Z}/p^2\mathbb{Z}$, and let D on $\mathbb{Z}/p^2\mathbb{Z}$ be given by $D(L)=|\operatorname{Disc}_{\mathbb{Q}} L|$, and D on $p\mathbb{Z}/p^2\mathbb{Z}$ be given by $D|_{p\mathbb{Z}/p^2\mathbb{Z}}(L)=|\operatorname{Disc}_{\mathbb{Q}} L|^p$. In both cases, $m=p(p-1)$. Let S be a finite set of finite places and let Φ specify that a character is unramified at all places in S. We consider

$$F_{D,G}(s,\Phi) := \sum_{\substack{\chi:J/\mathbb{Q}^\times \to G \\ \forall v\in S \ \chi_v \in \Phi_v}} \frac{1}{D(\chi)^s} = \prod_{\ell \notin S}\biggl(\sum_{\chi_\ell:\mathbb{Z}_\ell^\times \to G} \frac{1}{D(\chi_\ell)^s}\biggr),$$

where the product is over finite rational primes ℓ. We can express $F_{D,G}(s,\Phi)$ as this Euler product by Lemma 4.2, which allows us to count characters from $J/\mathbb{Q}^\times$ by counting characters from $\prod_\ell \mathbb{Z}_\ell^\times$. We know that D only depends on the restriction of local characters to $\mathbb{Z}_\ell^\times$. We see that $F_{D,G}(s,\Phi)$ only differs by finitely many factors from the $F_{D,G}(s,1,\phi)$ of § 2 (for any choice of ϕ), and that $F_{D,G}(s,\Phi)/F_{D,G}(s,1,\phi)$ is entire. We conclude from Lemma 2.10 that $F_{D,G}(s,\Phi)$ has a pole at $1/p(p-1)$ of order 1, but otherwise can be analytically continued to $\operatorname{Re}(s) \geqslant 1/p(p-1)$. As at the end of § 2, we can use a Tauberian theorem to calculate the coefficient sums

$$F_{D,G}(\Phi,X) = \#\{\chi : J/\mathbb{Q}^\times \to G \mid \chi_v \in \Phi_v \text{ for all } v \in S \text{ and } D(\chi) < X\}.$$

If we let $\Phi^{(q_i)}$ specify that a character is unramified at q_i, let $\Phi^{(q_1,q_2)}$ specify that a character is unramified at q_1 and q_2, and let $\Phi^{(0)}$ make no specification at all, we find that

$$\lim_{X\to\infty} \frac{F_{D,G}(\Phi^{(q_i)},X)}{F_{D,G}(\Phi^{(0)},X)} = \frac{1}{\sum_{\chi:\mathbb{Z}_{q_i}^\times \to G}(1/D(\chi)^s)},$$

$$\lim_{X\to\infty} \frac{F_{D,G}(\Phi^{(q_1,q_2)},X)}{F_{D,G}(\Phi^{(0)},X)} = \frac{1}{(\sum_{\chi:\mathbb{Z}_{q_1}^\times \to G}(1/D(\chi)^s))(\sum_{\chi:\mathbb{Z}_{q_2}^\times \to G}(1/D(\chi)^s))},$$

and

$$\lim_{X\to\infty} \frac{F_{D|_{p\mathbb{Z}/p^2\mathbb{Z}},p\mathbb{Z}/p^2\mathbb{Z}}(\Phi^{(0)},X)}{F_{D,\mathbb{Z}/p^2\mathbb{Z}}(\Phi^{(0)},X)} = \lim_{s\to 1/(p(p-1))} \frac{F_{D|_{p\mathbb{Z}/p^2\mathbb{Z}},p\mathbb{Z}/p^2\mathbb{Z}}(s,\Phi^{(0)})}{F_{D,\mathbb{Z}/p^2\mathbb{Z}}(s,\Phi^{(0)})} \neq 0, 1.$$

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

We can define D-probabilities of local specifications for random characters $J/\mathbb{Q}^\times \to \mathbb{Z}/p^2\mathbb{Z}$ as in (1), essentially replacing the set of surjective characters $J/\mathbb{Q}^\times \to G$ by the set of all characters $J/\mathbb{Q}^\times \to G$. Then the above tells us that q_1 ramifying and q_2 ramifying are D-independent events for random characters to $\mathbb{Z}/p^2\mathbb{Z}$. We see that q_1 ramifying and q_2 ramifying are D-independent events for random characters with image in $p\mathbb{Z}/p^2\mathbb{Z}$. Also, the probability that a random character to $\mathbb{Z}/p^2\mathbb{Z}$ has image in $p\mathbb{Z}/p^2\mathbb{Z}$ is not 0 or 1. Since we have $q_i \equiv 1 \pmod{p^2}$, there are more maps from $\mathbb{Z}_{q_i}^\times$ to $\mathbb{Z}/p^2\mathbb{Z}$ than to $p\mathbb{Z}/p^2\mathbb{Z}$. Thus the probabilities of q_i ramifying in a random character to $\mathbb{Z}/p^2\mathbb{Z}$ and in a random character with image in $p\mathbb{Z}/p^2\mathbb{Z}$ are different. We have the following simple fact from probability theory.

Lemma 4.3. *Let A be an event with positive probability not equal to 1. If E_1 and E_2 are independent, independent given A, and for $i=1,2$ we have that the $\Pr(E_i|A) \neq \Pr(E_i)$, then E_1 and E_2 are not independent given not-A.*

So we can conclude that the probabilities of q_1 and q_2 ramifying in a random surjective character to $\mathbb{Z}/p^2\mathbb{Z}$, or equivalently in a $\mathbb{Z}/p^2\mathbb{Z}$-extension of $\mathbb{Q}$, are not independent. □

Proposition 4.4. *Let $q = 2, 3, 5, 7, 11,$ or 13. Given that q is unramified, the discriminant probability that q splits completely in a $\mathbb{Z}/9\mathbb{Z}$-extension is less than $1/9$.*

Proof. From Wright [Wri89, Theorem I.4], we know that q is unramified with non-zero discriminant probability in a random $\mathbb{Z}/9\mathbb{Z}$-extension, and thus is makes sense to formulate the proposition. First, we let $G = \mathbb{Z}/p^2\mathbb{Z}$ for an arbitrary odd prime p. We let $S = \{q\}$ for some prime q, and define ϕ on S with ϕ_q the trivial character. We will use the isomorphisms

$$\operatorname{Hom}(J/\mathbb{Q}^\times, G) \cong \operatorname{Hom}\bigg(\prod_{\ell} \mathbb{Z}_\ell^\times, G\bigg) \cong \operatorname{Hom}\bigg(\bigg(\prod_{\ell\neq q} \mathbb{Z}_\ell^\times \times \mathbb{Q}_q^\times\bigg)\bigg/\langle q\rangle, G\bigg).$$

As in § 2.4, for $\epsilon \in \mathcal{A} = \langle q\rangle/\langle q^{p^2}\rangle$ we define

$$F_{D,G}(s,\phi) := \sum_{\substack{\chi: J/\mathbb{Q}^\times \to G\\ \forall v\in S, \chi_v = \phi_v}} \frac{1}{D(\chi)^s} \quad \text{and} \quad F'_{D,G}(s,\epsilon,\phi) := \sum_{\substack{\chi:\prod_{\ell\neq q}\mathbb{Z}_\ell^\times\times\mathbb{Q}_q^\times \to G\\ \forall v\in S, \chi_v=\phi_v}} \frac{\zeta_{p^2}^{\chi(\epsilon)}}{D(\chi)^s},$$

and have $F_{D,G}(s,\phi) = (1/|\mathcal{A}|)\sum_{\epsilon\in\mathcal{A}} F'_{D,G}(s,\epsilon,\phi)$. Therefore, we have the usual Euler product

$$F'_{D,G}(s,\epsilon,\phi) = \prod_{\ell\neq q} \sum_{\chi_\ell:\mathbb{Z}_l^\times\to G} \frac{\zeta_{p^2}^{\chi_\ell(\epsilon)}}{D(\chi_\ell)^s},$$

which has no factor at q because ϕ_q is the trivial character. We see that $F'_{D,G}(s,\epsilon,\phi)$ only differs from $F_{D,G}(s,\epsilon,\phi')$ (for any choice of ϕ' on $S' \ni q$) of § 2 by a finite number of factors. We also see that $F'_{D,G}(s,\epsilon,\phi)/F_{D,G}(s,\epsilon,\phi')$ is entire and non-zero at $1/p(p-1)$, and thus we conclude from Lemma 2.10 that $F'_{D,G}(s,\epsilon,\phi)$ can be analytically continued to $\operatorname{Re}(s) \geqslant 1/p(p-1)$ except for a possible pole of order at most one at $1/p(p-1)$. From Lemma 2.11 we have that $F'_{D,G}(s,\epsilon,\phi)$ has a pole at $1/p(p-1)$ exactly when $\epsilon^{1/p} \in \mathbb{Q}(\zeta_p)$, i.e. when $\epsilon \in \langle q^p\rangle$.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

For $\ell \neq q$ and $p \nmid i$,

$$\begin{aligned}
&\sum_{\chi_\ell : \mathbb{Z}_\ell^\times \to G} \frac{\zeta_{p^2}^{\chi_\ell(q^{pi})}}{D(\chi_\ell)^s} \\
&= \begin{cases}
1, & \ell \not\equiv 1 \pmod{p}; \\
1 + (p-1)\ell^{-(p^2-p)s}, & \ell \equiv 1 \pmod{p} \text{ and } \ell \not\equiv 1 \pmod{p^2}; \\
1 + (p-1)\ell^{-(p^2-p)s} - p\ell^{-(p^2-1)s}, & \ell \equiv 1 \text{ or } p \pmod{p^2} \text{ and } q \text{ not a } p\text{th} \\
& \quad \text{power in } \mathbb{Q}_\ell; \\
1 + (p-1)\ell^{-(p^2-p)s} + (p^2-p)\ell^{-(p^2-1)s}, & \ell \equiv 1 \text{ or } p \pmod{p^2} \text{ and } q \text{ a } p\text{th} \\
& \quad \text{power in } \mathbb{Q}_\ell.
\end{cases}
\end{aligned}$$

Also,

$$\begin{aligned}
&\sum_{\chi_\ell : \mathbb{Z}_\ell^\times \to G} \frac{1}{D(\chi_\ell)^s} \\
&= \begin{cases}
1, & \ell \not\equiv 1 \pmod{p}; \\
1 + (p-1)\ell^{-(p^2-p)s}, & \ell \equiv 1 \pmod{p} \text{ and } \ell \not\equiv 1 \pmod{p^2}; \\
1 + (p-1)\ell^{-(p^2-p)s} + (p^2-p)\ell^{-(p^2-1)s}, & \ell \equiv 1 \text{ or } p \pmod{p^2}.
\end{cases}
\end{aligned}$$

To find the discriminant probability that a random character to $\mathbb{Z}/p^2\mathbb{Z}$ splits completely at q, given that it is unramified at q, we compare $F_{D,G}(s, \phi)$ to $F_{D,G}(s, \Phi^{(q)})$ (from the proof of Proposition 4.1), which counts all characters to $\mathbb{Z}/p^2\mathbb{Z}$, unramified at q. We have

$$F_{D,G}(s, \Phi^{(q)}) = \prod_{\ell \neq q} \biggl(\sum_{\chi_\ell : \mathbb{Z}_\ell^\times \to G} \frac{1}{D(\chi_\ell)^s} \biggr).$$

Both $F_{D,G}(s, \phi)$ and $F_{D,G}(s, \Phi^{(q)})$ can be meromorphically continued to $\mathrm{Re}(s) \geqslant 1/p(p-1)$, analytic away from $1/p(p-1)$ and with a pole of order 1 at $1/p(p-1)$. Thus we can use a Tauberian theorem, as at the end of § 2, to find that the discriminant probability of a random character $\chi : J/\mathbb{Q}^\times \to \mathbb{Z}/p^2\mathbb{Z}$ being trivial at q, given that it is unramified, is

$$\begin{aligned}
s &= \lim_{s \to 1/(p(p-1))} \frac{(1/|\mathcal{A}|) \sum_{\epsilon \in \mathcal{A}} F'_{D,G}(s, \epsilon, \phi)}{F_{D,G}(s, \Phi^{(q)})} \\
&= \frac{1}{p^2} \biggl(1 + (p-1) \prod_{\substack{\ell \equiv 1 \text{ or } p \pmod{p^2} \\ q \text{ not a } p\text{th power in } \mathbb{Q}_\ell \\ \ell \neq q}} \frac{(1 + (p-1)\ell^{-1} - p\ell^{-(p+1)/p})}{(1 + (p-1)\ell^{-1} + (p^2-p)\ell^{-(p+1)/p})} \biggr).
\end{aligned}$$

Remark 4.5. Note that $s > 1/p^2$ because we know that both $F'_{D,G}(s, q^{pi}, \phi)$ and $F_{D,G}(s, \Phi^{(q)})$ do have a pole at $1/p(p-1)$. Thus we cannot 'resolve' this proposition by simply considering all characters $\chi : J/\mathbb{Q}^\times \to \mathbb{Z}/p^2\mathbb{Z}$ instead of just $\mathbb{Z}/p^2\mathbb{Z}$-extensions.

We have shown that the discriminant probability of q splitting completely in a random character $\chi : J/\mathbb{Q}^\times \to p\mathbb{Z}/p^2\mathbb{Z}$, given that it is unramified at q, is $1/p$, because $D|_{p\mathbb{Z}/p^2\mathbb{Z}}$ is fair and so we can use Corollary 1.2. By the method in the proof of Proposition 4.1, we can calculate that the discriminant probability that a random character $\chi : J/\mathbb{Q}^\times \to \mathbb{Z}/p^2\mathbb{Z}$, unramified at q, has image in $p\mathbb{Z}/p^2\mathbb{Z}$ is

$$r = \prod_{\ell \neq q} \frac{\sum_{\chi:\mathbb{Z}_\ell^\times \to p\mathbb{Z}/p^2\mathbb{Z}} (1/D(\chi)^{1/(p^2-p)})}{\sum_{\chi:\mathbb{Z}_\ell^\times \to \mathbb{Z}/p^2\mathbb{Z}} (1/D(\chi)^{1/(p^2-p)})} = \prod_{\substack{\ell \equiv 1 \text{ or } p \pmod{p^2} \\ \ell \neq q}} \frac{(1+(p-1)\ell^{-1})}{(1+(p-1)\ell^{-1}+(p^2-p)\ell^{-(p+1)/p})}.$$

Thus if s_1 is the probability that a random surjective character to $\mathbb{Z}/p^2\mathbb{Z}$ is trivial at q, given that it is unramified at q, we have

$$s_1 = \frac{s-(r/p)}{1-r}$$

and thus $s_1 > 1/p^2$ if and only if $(p^2 s - 1/(p-1)r) > 1$. In other words, $s_1 > 1$ if and only if the product

$$\prod_{\substack{\ell \equiv 1 \text{ or } p \pmod{p^2} \\ q \notin \mathbb{Q}_\ell^p \\ \ell \neq q}} \frac{(1+(p-1)\ell^{-1} - p\ell^{-(p+1)/p})}{(1+(p-1)\ell^{-1})} \prod_{\substack{\ell \equiv 1 \text{ or } p \pmod{p^2} \\ q \in \mathbb{Q}_\ell^p \\ \ell \neq q}} \frac{(1+(p-1)\ell^{-1}+(p^2-p)\ell^{-(p+1)/p})}{(1+(p-1)\ell^{-1})}$$

is greater than 1. We can calculate truncations of the above product in PARI/GP [PAR06] for $p=3$, $q=2,3,5,7,11,13$, and $\ell \leqslant N$, where $N=10^5$ (except for when $q=3$ where we use $N=10^8$). We can estimate that the remainder, the product of the terms with $l > N$, is at most

$$\begin{aligned}\prod_{\ell > N} (1+(p^2-p)\ell^{-(p+1)/p}) &\leqslant \prod_{\ell > N} (1+\ell^{-(p+1)/p})^{p^2-p} \\ &\leqslant \left(1+\sum_{n>N} n^{-(p+1)/p}\right)^{p^2-p} \\ &\leqslant (1+pN^{-1/p})^{p^2-p},\end{aligned}$$

where the sum is over integers n. We can then prove that $s_1 \leqslant 0.97$ in all of these cases. In conclusion, the probability that a random $\mathbb{Z}/9\mathbb{Z}$-extension of $\mathbb{Q}$ splits completely at q, given that it is unramified at q, is less than 1/9 for $q=2,3,5,7,11$, or 13. □

5. Fair Artin conductors

For any faithful finite-dimensional complex representation R of G and G-extension L, we have the Artin conductor $C^R(L)$, which is a counting function (as defined in the beginning of § 2). If R is not faithful, then the Artin conductor is not a counting function because it will have $c_G^R(g)=0$ for non-trivial g. We have seen that for fair counting functions the probabilities of local behaviors are nice, but in § 4 we saw that for an example of an unfair counting function the probabilities are not so well-behaved. In this section, we give two simple examples of Artin conductors which give fair counting functions.

For a general definition of Artin conductors, see [Neu99, ch. VII.11]. The discriminant is given by the Artin conductor of the regular representation. Since we are only concerned with G abelian, any representation R breaks up as a sum of one-dimensional representations, each of which is determined by the kernel of the action of G on that one-dimensional representation. Suppose R is given by kernels $H_1, \ldots, H_s$. Then for $g \in G$, we have $c_G^R(g) = s - \#\{i | g \in H_i\}$. This can serve as a definition of the Artin conductor at all tame places, which is all that concerns fairness. In other words, for a character $\chi : K_v^\times \to G$ for $v \nmid |G|$, we have $c^R(\chi) = c_G^R(\chi(y_v))$, where y_v is

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

a generator of tame inertia. Recall that m_R is the minimum value, other than 0, taken by c_G^R, and $\mathfrak{M} = \mathfrak{M}_R = (c_G^R)^{-1}(m)$. The counting function is fair if $\mathfrak{M} \cap \{g \in G \mid g^r = 1\}$ generates the subgroup $\{g \in G \mid g^r = 1\}$ for all r.

We write $G = \prod_i \mathbb{Z}/n_i\mathbb{Z}$, and let $f_i : G \to \mathbb{Z}/n_i\mathbb{Z} \hookrightarrow \mathbb{C}^*$ be the projection of G to a factor composed with an injection to $\mathbb{C}^*$. Then $\bigoplus_i f_i$ gives a fair Artin conductor. Since the representation is faithful, the Artin conductor of $\bigoplus_i f_i$ is a counting function. Also, the elements of $\mathfrak{M}$ are exactly the elements of G that are in all but one $\ker f_i$, and these are the elements with non-zero coordinates in exactly one factor of G. These elements of $\mathfrak{M}$ generate G in every exponent, and thus the Artin conductor is fair.

Also, $\bigotimes_i f_i \oplus \bigoplus_i f_i$ has a fair Artin conductor. We have $\bigcap_i \ker f_i = \{1\}$ and $\ker(\bigotimes_i f_i) \cap \bigcap_{i \neq j} \ker f_i = \{1\}$, and so the elements of $\mathfrak{M}$ are exactly the elements of G that are in all but two of the $\ker f_i$ and $\ker(\bigotimes_i f_i)$. The elements of G with non-zero coordinates in exactly one factor are in $\mathfrak{M}$, and they generate G in every exponent, and thus in this case the Artin conductor is fair. We can apply these two examples of fair Artin conductors to other factorizations of G into cyclic groups to obtain more examples of fair Artin conductors.

6. Further questions

One may ask whether counting abelian extensions by conductor or by discriminant is more natural. In this paper, we have seen that the probabilities of local behaviors are very nice when counting by conductor and not so well behaved when counting by discriminant. While in both cases we can obtain asymptotic counting results for the total number of extensions (see § 3 and [Wri89]), in the case of conductor we can express the constant in the asymptotic count as an Euler product (see Theorem 3.1). No Euler product is known for the constant counting abelian extensions by discriminant for a general group G and base field K. So it seems for abelian groups G, counting by conductor gives more natural answers.

The other main examples where this global asymptotic counting and computation of local probabilities can be done are for degree n extensions with Galois closure with group S_n for $n = 3, 4, 5$ (see [DH71, Bha05, Bhaa]). In these cases the counting is done by discriminant, and in fact it is not clear what we might mean by *conductor* in these cases. Perhaps one should define the conductor to be the greatest common divisor of all Artin conductors. In [BW08] the present author and Bhargava count these S_3 extensions another way; equivalently, we count Galois degree six extensions with Galois group S_3 by their discriminant. In this case, we obtain an asymptotic for the overall count with an Euler product constant and nice local behaviors (simple ratios of probabilities at a given place, and independence at any finite set of places). In [BW08] it is remarked that one can obtain all these nice behaviors for a range of counting functions.

For quartic extensions of $\mathbb{Q}$ having Galois closure with Galois group D_4 the overall asymptotic counting by discriminant has been completed (see [CDO02b]), but the constant has not been found to have a simple form, and no results for local probabilities analogous to those in this paper have been found. We wonder if counting these D_4 extensions another way would yield nicer results. In particular, see [Woo08, § 5] for a specific counting function one might investigate.

Ellenberg and Venkatesh [EV05, § 4.2] suggest that we can try to count extensions of global fields by general counting functions (our terminology). The larger question that is motivated by this paper is which of these counting functions are better than others. For which counting functions can we obtain an asymptotic total count? For which counting functions is the constant

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

in the asymptotic total count an Euler product? And for which counting functions are the local probabilities simple and independent at finite sets of places? These questions are exactly in line with the questions of Bhargava in [Bhab, § 8.2], except he asks these questions mainly for counting by discriminant and here we emphasize that the answers will depend on the choice of counting function.

Acknowledgements

I would like to thank Manjul Bhargava for suggesting the original questions of this paper to me, for many helpful conversations over the course of the work, and for his thorough suggestions on an earlier draft of this paper. I would also like to thank Bisi Agboola for very detailed comments and suggestions on an earlier draft.

References

AT68 E. Artin and J. Tate, *Class field theory* (W. A. Benjamin Inc., New York, 1968).

BW08 M. Bhargava and M. M. Wood, *The density of discriminants of S_3-sextic number fields*, Proc. Amer. Math. Soc. **136** (2008), 1581–1587.

Bha05 M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063.

Bhaa M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math., to appear.

Bhab M. Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*, Int. Math. Res. Not. (2007), Art. ID rnm052, 20 pp.

Coh02 H. Cohen, *Constructing and counting number fields*, in *Proceedings of the International congress of mathematicians,* Beijing, 2002, vol. II (Higher Ed. Press, Beijing, 2002), 129–138.

CDO06 H. Cohen, F. Diaz y diaz and M. Olivier, *Counting discriminants of number fields*, J. Théor. Nombres Bordeaux **18** (2006), 573–593.

CDO02a H. Cohen, F. Diaz y Diaz and M. Olivier, *A survey of discriminant counting*, in *Algorithmic number theory,* Sydney, 2002, Lecture Notes in Computer Science, vol. 2369 (Springer, Berlin, 2002), 80–94.

CDO02b H. Cohen, F. Diaz y Diaz and M. Olivier, *Enumerating quartic dihedral extensions of $\mathbb{Q}$*, Compositio Math. **133** (2002), 65–93.

DW86 B. Datskovsky and D. J. Wright, *The adelic zeta function associated to the space of binary cubic forms. II. Local theory*, J. Reine Angew. Math. **367** (1986), 27–75.

DH71 H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.

DD93 I. Del Corso and R. Dvornicich, *A converse of Artin's density theorem: the case of cubic fields*, J. Number Theory **45** (1993), 28–44.

DD98 I. Del Corso and R. Dvornicich, *Uniformity over primes of unramified splittings*, Mathematika **45** (1998), 177–189.

DD00 I. Del Corso and R. Dvornicich, *Uniformity over primes of tamely ramified splittings*, Manuscripta Math. **101** (2000), 239–266.

EV05 J. S. Ellenberg and A. Venkatesh, *Counting extensions of function fields with bounded discriminant and specified Galois group*, in *Geometric methods in algebra and number theory*, Progress in Mathematics, vol. 235 (Birkhäuser, Boston, MA, 2005), 151–168.

Gru33 W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, J. Reine Angew. Math. **169** (1933), 103–107.

Mäk85 S. Mäki, *On the density of abelian number fields*, Ann. Acad. Sci. Fenn. Ser. A I Math. Diss. **54** (1985), 104.

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press

Mäk93 S. Mäki, *The conductor density of abelian number fields*, J. London Math. Soc. (2) **47** (1993), 18–30.

Mal04 G. Malle, *On the distribution of Galois groups. II*, Experiment. Math. **13** (2004), 129–135.

Nar83 W. Narkiewicz, *Number theory* (World Scientific, Singapore, 1983). (Translated by S. Kanemitsu.)

Neu99 J. Neukirch, *Algebraic number theory* (Springer, Berlin, 1999). (Translated from the 1992 German original and with a note by Norbert Schappacher.)

PAR06 PARI/GP, version `2.3.2`, Bordeaux, 2006, http://pari.math.u-bordeaux.fr/.

Tay84 M. J. Taylor, *On the equidistribution of Frobenius in cyclic extensions of a number field*, J. London Math. Soc. (2) **29** (1984), 211–223.

van88 C. E. van der Ploeg, *On a converse to the Tschebotarev density theorem*, J. Aust. Math. Soc. Ser. A **44** (1988), 287–293.

Wan50 S. Wang, *On Grunwald's theorem*, Ann. of Math. (2) **51** (1950), 471–484.

Woo08 M. M. Wood, *Mass formulas for local Galois representations to wreath products and cross products*, Algebra Number Theory **2** (2008), 391–405.

Wri89 D. J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), 17–50.

Melanie Matchett Wood melanie.wood@math.princeton.edu
Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA

https://doi.org/10.1112/S0010437X0900431X Published online by Cambridge University Press