

ON COUNTING RINGS OF INTEGERS AS GALOIS MODULES

A. AGBOOLA

ABSTRACT. Let K be a number field and G a finite abelian group. We study the asymptotic behaviour of the number of tamely ramified G -extensions of K with ring of integers of fixed realisable class as a Galois module.

1. INTRODUCTION

Suppose that K is a number field with ring of integers O_K , and let G be a fixed, finite group. If K_h/K is a tamely ramified Galois algebra with Galois group G , then a classical theorem of E. Noether implies that the ring of integers O_h of K_h is a locally free $O_K G$ -module. It therefore determines a class (O_h) in the locally free class group $\text{Cl}(O_K G)$ of $O_K G$. We say that a class $c \in \text{Cl}(O_K G)$ is *realisable* if $c = (O_h)$ for some tamely ramified G -algebra K_h/K , and we write $\mathcal{R}(O_K G)$ for the set of realisable classes in $\text{Cl}(O_K G)$. These classes are natural objects of study, and they arise, for instance, in the context of obtaining explicit analogues of known Adams-Riemann-Roch theorems for locally free class groups (see e.g. [1, §4] and the references cited there; see also the work of B. Köck ([4], [5]) on this and related topics). We also remark that the problem of describing $\mathcal{R}(O_K G)$ for arbitrary finite groups G may be viewed as being a Galois module theoretic analogue of the inverse Galois problem for finite groups.

When G is abelian, Leon McCulloh has obtained a complete description of $\mathcal{R}(O_K G)$ in terms of certain Stickelberger homomorphisms on classgroups (see [7]). In particular, he has shown that $\mathcal{R}(O_K G)$ is in fact a group. Suppose now that $c \in \mathcal{R}(O_K G)$, and write $N_{\text{disc}}(c, X)$ for the number of tame G -extensions K_h/K for which $(O_h) = c$ and $\text{disc}(K_h/\mathbf{Q}) \leq X$, where $\text{disc}(K_h/\mathbf{Q})$ denotes the absolute value of the discriminant of K_h/\mathbf{Q} . The following very natural counting problem appears to have received surprisingly little attention.

Question 1.1. *What can be said about $N_{\text{disc}}(c, X)$ as $X \rightarrow \infty$? For example, if $M_{\text{disc}}(X)$ denotes the number of tame G -extensions K_h/K for which $\text{disc}(K_h/\mathbf{Q}) \leq X$, is*

$$\lim_{X \rightarrow \infty} \frac{N_{\text{disc}}(c, X)}{M_{\text{disc}}(X)}$$

Date: Preliminary Version of November 25, 2008.

Partially supported by NSF and NSA grants.

independent of the realisable class c ?

The only previous results concerning this question of which the author is aware are those contained in the unpublished University of Illinois Ph.D. thesis of Kurt Foster (see [3]). Foster considers the case in which G is an elementary abelian l -group for some prime l . Using earlier work of McCulloh on realisable classes for elementary abelian groups (see [6]), he proves the following result.

Theorem A. (*K. Foster*) *Suppose that G is an elementary abelian l -group. Then*

$$N_{\text{disc}}(c, X) \sim \beta \cdot Y \cdot (\log Y)^{r-1}$$

as $X \rightarrow \infty$, where

- $Y^{\phi(|G|)}(\text{disc}(K/\mathbf{Q}))^{|G|} = X$ (here ϕ denotes the Euler ϕ -function);
- β is a positive constant that depends upon K and G , but not on c ;
- r is a positive integer that depends only upon K and G .

Hence, when G is an elementary abelian group, then asymptotically $N_{\text{disc}}(c, X)$ is independent of c , and so we see that the tame G -extensions of K are equidistributed amongst the realisable classes as $X \rightarrow \infty$.

Let us say a few words about the main ideas involved in the proof of Theorem A. One begins by considering the series

$$\sum_{\substack{K_h/K \text{ tame,} \\ \text{Gal}(K_h/K) \simeq G \\ (O_h)=c}} \text{disc}(K_h/\mathbf{Q})^{-s}, \quad s \in \mathbf{C}. \quad (1.1)$$

Of course it is not a priori clear that this series converges anywhere; one establishes convergence in some right-hand half-plane by showing that it may be written as an Euler product over rational primes. The series may therefore be written in the form $\sum_{n=1}^{\infty} a_n n^{-s}$. One deduces from this that in general, the series will have finitely many poles (whose locations may be determined), and that the number $N_{\text{disc}}(c, X)$ is equal to $\sum_{n \leq X} a_n$. This last quantity may then be estimated by using a suitable version of the D elange-Ikehara Tauberian theorem.

Our goal in this paper is to investigate similar counting problems when G is an arbitrary finite abelian group. We shall do this by combining Foster's approach with later work of McCulloh (see [7]) on realisable classes for arbitrary finite abelian groups.

A special case of our main result (see Theorem 8.1) may be described as follows. Let G be an arbitrary finite abelian group. For any tame G -extension K_h/K , let $\mathcal{D}(K_h/K)$ denote the absolute norm of the product of the primes of K that ramify in K_h/K . If $c \in \mathcal{R}(O_K G)$,

then we write $N_{\mathcal{D}}(c, X)$ for the number of tame G -extensions K_h/K such that $(O_h) = c$, $\mathcal{D}(K_h/K) \leq X$, and K_h/K is unramified at all places dividing $|G|$. The following result shows that asymptotically, $N_{\mathcal{D}}(c, X)$ is independent of c .

Theorem B. *With notation and hypotheses as above, we have*

$$N_{\mathcal{D}}(c, X) \sim \beta_1 \cdot X \cdot (\log X)^{r-1},$$

as $X \rightarrow \infty$. Here β_1 is a constant depending only upon K and G , but not upon c , and r is the same positive integer that occurs in the statement of Theorem A.

For arbitrary finite abelian G , our results concerning $N_{\text{disc}}(c, X)$ are unfortunately not as precise (see (3.6) and Remark 8.4). The results that we obtain indicate that it is very unlikely that the analogue of Foster's equidistribution result holds in general, although at present we are unable to prove this. This fact, namely that when tame G -extensions of K are counted by discriminant, then in general, they are probably not equidistributed amongst the realisable classes, was rather surprising to us. It is interesting to compare the results of this paper with recent work of Melanie Wood on a quite different type of counting problem (see [9]). Wood studies the probabilities of various local completions of a random G -extension of K . She proves that these probabilities are well-behaved and are—for the most part—independent when G -extensions of K are counted by conductor; as she points out, this is in close analogy with Chebotarev's density theorem. When G extensions of K are counted by discriminant however, she proves that these probabilities are poorly behaved and in general are not independent. It would be interesting to obtain a better understanding of the relationship, if any, between the results described in the present paper and those of [9].

An outline of the contents of this paper is as follows. In Section 2 we review McCulloh's theory of realisable classes. In Section 3, we use the methods of [3] to set up a counting problem that will enable us to analyse the distribution of tame G -extensions of K amongst realisable classes. In Sections 4 and 5 we study analogues of the series (1.1) in our setting. We show that they are Euler products, and we apply a Tauberian theorem in order to state a result concerning their asymptotic behaviour. In Section 6 we introduce certain Dirichlet L -series; these are then used in Section 7 to determine the location of the poles of the series introduced in Section 4. Finally, in Section 8, we state our main result and explain how it may be used to recover Theorem A and to prove Theorem B. We also explain why our results indicate that the analogue of Foster's equidistribution result probably does not hold in general.

Acknowledgements. It will be clear to the reader that this paper owes a great deal to the work of L. McCulloh and K. Foster. I am very grateful to Leon McCulloh for sending me

a copy of Foster's thesis. I would also like to thank Jordan Ellenberg for his interest, and Melanie Wood for sending me a copy of her paper [9].

Notation and conventions. If L is a number field, we write O_L for its ring of integers. We set $\Omega_L := \text{Gal}(L^c/L)$, where L^c denotes an algebraic closure of L , and we write $I(O_L)$ for the group of fractional ideals of L .

The symbol G will always denote a finite, abelian group. If H is any group, we write \widehat{H} for the group of characters of H , and $\mathbf{1}_H$ (or simply $\mathbf{1}$ if there is no danger of confusion) for the trivial character in \widehat{H} .

We identify G -Galois algebras of K with elements of $H^1(K, G) \simeq \text{Hom}(\Omega_K, G)$ (see 2.2 below). If $h \in H^1(K, G)$, then we write K_h/K for the corresponding G -extension of K , and O_h for the integral closure of O_K in O_h . We write $H_{tr}^1(K, G)$ for the subgroup of $H^1(K, G)$ consisting of those $h \in H^1(K, G)$ for which K_h/K is tamely ramified.

If L/K is any finite extension, then $N_{L/K}$ denotes the norm map from L to K .

2. REVIEW OF McCULLOH'S THEORY OF REALISABLE CLASSES

In this section we shall briefly describe McCulloh's theory of realisable classes of tame extensions. The reader is strongly encouraged to consult McCulloh's paper [7] for full details.

2.1. Locally free class groups. In this subsection we shall recall some basic facts concerning the Picard group $\text{Cl}(O_K G)$ of $O_K G$.

Let $J(KG)$ denote the group of finite ideles of KG , i.e. the restricted direct product of the groups $(K_v G)^\times$ with respect to the subgroups $(O_{K,v} G)^\times$. Then there is a natural isomorphism

$$\text{Cl}(O_K G) \simeq \frac{J(KG)}{(\prod_v (O_{K,v} G)^\times) (KG)^\times}. \quad (2.1)$$

Suppose that K_h/K is a tamely ramified Galois algebra with $\text{Gal}(K_h/K) \simeq G$. Then by Noether's theorem, the ring of integers O_h of K_h is a locally free $O_K G$ -module of rank one. Let $b \in K_h$ be a KG -generator of K_h , and, for each finite place v of K , choose an $O_{K,v} G$ -generator a_v of $O_{h,v}$. We refer to b as a *normal basis generator* and to a_v as a *normal integral basis generator*. Then there exists $c_v \in (K_v G)^\times$ such that $a_v = c_v b$. It may be shown that $c = (c_v)_v \in J(KG)$. The idele c is a representative of $(O_h) \in \text{Cl}(O_K G)$.

Now let

$$j : J(KG) \rightarrow \text{Cl}(O_K G)$$

denote the surjective homomorphism afforded by the isomorphism (2.1), and suppose that c is any idele in $J(KG)$. How can we tell whether or not the class $j(c)$ is realisable? In

order to describe the answer to this question, we need to introduce some further ideas and notation.

2.2. Resolvends. If $h : \Omega_K \rightarrow G$ is any continuous homomorphism, then we may define an associated G -Galois K -algebra K_h by

$$K_h := \text{Map}_{\Omega_K}({}^hG, K^c),$$

where hG denotes the set G endowed with an action of Ω_K via the homomorphism h , and K_h is the algebra of K^c -valued functions on G that are fixed under the action of Ω_K . The group G acts on K_h via the rule

$$a^s(t) = a(ts)$$

for all $s, t \in G$. It may be shown that every G -Galois K -algebra is isomorphic to an algebra of the form K_h for some h . Every G -Galois K -algebra may therefore be viewed as lying in the K^c -algebra $\text{Map}(G, K^c)$. It is therefore natural to consider the Fourier transforms of elements of $\text{Map}(G, K^c)$. These arise via the *resolvend* map

$$\mathbf{r}_G : \text{Map}(G, K^c) \rightarrow K^cG; \quad a \mapsto \sum_{s \in G} a(s)s^{-1}.$$

The map \mathbf{r}_G is an isomorphism of left K^cG -modules, but not of algebras, because it does not preserve multiplication. It is not hard to show that for any $a \in \text{Map}(G, K^c)$, we have that $a \in K_h$ if and only if $\mathbf{r}_G(a)^\omega = \mathbf{r}_G(a)h(\omega)$ for all $\omega \in \Omega_K$ (where here Ω_K acts on K^cG via its action on the coefficients). It may also be shown that an element $a \in K_h$ generates K_h as a KG -module if and only if $\mathbf{r}_G(a) \in (K^cG)^\times$. Two elements $a_1, a_2 \in \text{Map}(G, K^c)$ with $\mathbf{r}_G(a_1), \mathbf{r}_G(a_2) \in (K^cG)^\times$ generate the same G -Galois K -algebra as a KG -module if and only if $\mathbf{r}_G(a_1) = g \cdot \mathbf{r}_G(a_2)$ for some $g \in G$.

We define

$$\begin{aligned} H(KG) &:= \{ \alpha \in (K^cG)^\times : \alpha^\omega / \alpha \in G \quad \forall \omega \in \Omega_K \}; \\ \mathcal{H}(KG) &:= H(KG)/G. \end{aligned}$$

The group $H(KG)$ consists precisely of resolvends of normal basis generators of G -Galois K -algebras lying in $\text{Map}(G, K^c)$. The group $\mathcal{H}(KG)$ may be naturally identified with the set of all G -Galois K -algebras lying in $\text{Map}(G, K^c)$.

For each finite place v of K , we define $\mathcal{H}(K_vG)$ and $\mathcal{H}(O_{K,v}G)$ analogously. We write $\mathcal{H}(\mathbf{A}(KG))$ for the restricted direct product of the groups $\mathcal{H}(K_vG)$ with respect to the groups $\mathcal{H}(O_{K,v}G)$. Then the natural maps

$$(K_vG)^\times \rightarrow \mathcal{H}(K_vG)$$

induce a homomorphism

$$\text{rag} : J(KG) \rightarrow \mathcal{H}(\mathbf{A}(KG)).$$

McCulloh shows that if $c \in J(KG)$, then $j(c) \in \text{Cl}(O_K G)$ is realisable if and only if $\text{rag}(c)$ admits a certain local decomposition. This local decomposition involves certain Stickelberger maps that we shall now describe.

2.3. Stickelberger maps. Let \widehat{G} denote the group of complex-valued characters of G , and write $G(-1)$ for the group G endowed with a Ω_K -action via the inverse cyclotomic character. There is a natural pairing

$$\langle , \rangle : \mathbf{Q}\widehat{G} \times \mathbf{Q}G \rightarrow \mathbf{Q}$$

defined by

$$\chi(g) = \exp(2\pi i \langle \chi, g \rangle), \quad 0 \leq \langle \chi, g \rangle < 1$$

for $\chi \in \widehat{G}$ and $g \in G$. This pairing may in turn be used to define a *Stickelberger map*

$$\Theta : \mathbf{Q}\widehat{G} \rightarrow \mathbf{Q}G; \quad \alpha \mapsto \sum_{g \in G} \langle \alpha, g \rangle g.$$

Let $A_{\widehat{G}}$ denote the kernel of the determinant map

$$\det : \mathbf{Z}\widehat{G} \rightarrow \widehat{G}; \quad \sum_{\chi \in \widehat{G}} a_{\chi} \chi \mapsto \prod_{\chi \in \widehat{G}} \chi^{a_{\chi}}.$$

Then the standard isomorphism

$$(K^c G)^{\times} \simeq \text{Hom}(\mathbf{Z}\widehat{G}, (K^c)^{\times})$$

induces an isomorphism

$$(K^c G)^{\times} / G \simeq \text{Hom}(A_{\widehat{G}}, (K^c)^{\times}).$$

Proposition 2.1. (*McCulloh*) *If $\alpha \in \mathbf{Z}\widehat{G}$, then $\Theta(\alpha) \in \mathbf{Z}G$ if and only if $\alpha \in A_{\widehat{G}}$.*

Proof. See [7, Proposition 4.3]. □

Proposition 2.1 implies that, via restriction, Θ defines a homomorphism (which we denote by the same symbol)

$$\Theta : A_{\widehat{G}} \rightarrow \mathbf{Z}G.$$

Dualising this homomorphism, and twisting by the inverse cyclotomic character yields a Ω_K -equivariant *transpose Stickelberger homomorphism*

$$\Theta^t : \text{Hom}(\mathbf{Z}G(-1), (K^c)^{\times}) \rightarrow \text{Hom}(A_{\widehat{G}}, (K^c)^{\times}) \simeq (K^c G)^{\times} / G.$$

Now set

$$\begin{aligned}\Lambda &:= \text{Hom}_{\Omega_K}(\mathbf{Z}G(-1), O_{K^c}) = \text{Map}_{\Omega_K}(G(-1), O_{K^c}); \\ K\Lambda &:= \text{Hom}_{\Omega_K}(\mathbf{Z}G(-1), K^c) = \text{Map}_{\Omega_K}(G(-1), K^c).\end{aligned}$$

Then Θ^t above induces a homomorphism

$$\Theta^t : (K\Lambda)^\times \rightarrow [(K^c G)^\times / G]^{\Omega_K} = \mathcal{H}(KG).$$

For each finite place v of K , we can apply the discussion above with K replaced by K_v to obtain a local version

$$\Theta_v^t : (K_v\Lambda_v)^\times \rightarrow \mathcal{H}(K_v G) \quad (2.2)$$

of the map Θ^t . The homomorphism Θ^t commutes with local completion.

For all places v of K not dividing the order of G , it may be shown that $\Theta^t(\Lambda_v) \subseteq \mathcal{H}(O_{K,v}G)$. Hence if we write $J(K\Lambda)$ for the restricted direct product of the groups $(K_v\Lambda_v)^\times$ with respect to the groups Λ_v^\times , then the homomorphisms Θ_v^t combine to yield an idelic transpose Stickelberger homomorphism

$$\Theta^t : J(K\Lambda) \rightarrow \mathcal{H}(\mathbf{A}(KG)). \quad (2.3)$$

2.4. Prime F -elements. Let v be a finite place of K , and write q_v for the order of the residue field at v . Fix a local uniformiser π_v of K at v . Write $G_{(q_v-1)}$ for the subgroup of G consisting of all elements in G of order dividing $q_v - 1$.

For each element $s \in G_{(q_v-1)}$, define $f_{v,s} \in (K_v\Lambda_v)^\times = \text{Map}(G(-1), (K_v^c)^\times)^{\Omega_K}$ by

$$f_{v,s}(t) = \begin{cases} \pi_v, & \text{if } t = s \neq 1; \\ 1, & \text{otherwise.} \end{cases} \quad (2.4)$$

Note in particular that $f_{v,1} = 1$.

Write

$$\mathbf{F}_v := \{f_{v,s} \mid s \in G_{(q_v-1)}\}.$$

The non-trivial elements of \mathbf{F}_v are called *the prime F -elements lying above v* . We define $\mathbf{F} \subset J(F\Lambda)$ by

$$f \in \mathbf{F} \iff f \in J(F\Lambda) \text{ and } f_v \in \mathbf{F}_v \text{ for all } v.$$

In other words, each non-trivial element of \mathbf{F} is a finite product of prime F -elements lying over distinct places v of K .

We can now state two results of McCulloh. The first result (see [7, Theorem 6.7]) characterises tame G -extensions of K in terms of resolvents of normal basis generators. The

second (see [7, Theorem 6.17]) gives a precise characterisation of those ideles $c \in J(KG)$ for which $j(c) \in \text{Cl}(O_K G)$ is realisable.

Theorem 2.2. (*McCulloh*) *Suppose that $c \in J(KG)$. Then $j(c) = (O_h)$ for some tamely ramified G -Galois algebra extension K_h/K (i.e. $j(c)$ is realisable) if and only if there exist $b \in \mathcal{H}(KG)$, $f \in \mathbf{F}$ and $u \in \prod_v \mathcal{H}(O_{K,v}G)$ such that*

$$\text{rag}(c) = b^{-1} \cdot \Theta^t(f) \cdot u \in \mathcal{H}(\mathbf{A}(KG)).$$

The G -Galois algebra K_h and the element $f \in \mathbf{F}$ are uniquely determined by c . Furthermore, K_h/K is ramified at precisely those places v of K for which $f_v \neq 1$.

Theorem 2.3. (*McCulloh*) *Suppose that $c \in J(KG)$. Then $j(c) \in \text{Cl}(O_K G)$ is realisable if and only if $\text{rag}(c) \in \mathcal{H}(KG) \cdot \mathcal{H}(\mathbf{A}(O_K G)) \cdot \Theta^t(J(K\Lambda))$.*

3. A COUNTING PROBLEM

In this section we shall explain how to set up a counting problem that will enable us to study the distribution of tame G -extensions of K amongst realisable classes. We apply a modified version of a method described in [3, Chapters II and III].

Set

$$\mathcal{C}(O_K G) := \frac{\mathcal{H}(\mathbf{A}(KG))}{[(KG)^\times/G] \cdot \mathcal{H}(\mathbf{A}(O_K G))}. \quad (3.1)$$

Definition 3.1. We define a homomorphism

$$\psi : H^1(K, G) \rightarrow \mathcal{C}(O_K G) \quad (3.2)$$

as follows. Let K_h/K be the Galois G -extension of K corresponding to $h \in H^1(K, G)$, and let $b \in K_h$ be any normal basis generator. We define $\psi(h)$ to be the image of h under the composition of maps

$$H^1(K, G) \rightarrow \frac{H(KG)}{(KG)^\times} \rightarrow \mathcal{C}(O_K G),$$

where the first arrow is given by $h \mapsto [r_G(b)]$, and the second arrow is induced by the diagonal embedding

$$H(KG) \rightarrow \prod_v H(K_v G).$$

It is not hard to check that $\psi(h)$ is independent of the choice of b , and that ψ is a homomorphism.

Definition 3.2. We define

$$\rho : \text{Cl}(O_K G) \simeq \frac{J(KG)}{(KG)^\times \cdot \prod_v (O_{K,v}G)^\times} \rightarrow \mathcal{C}(O_K G)$$

to be the homomorphism induced by the composition of maps

$$J(KG) \rightarrow H(\mathbf{A}(KG)) \rightarrow \mathcal{H}(\mathbf{A}(KG)).$$

Here the first arrow is the diagonal embedding, and the second map is the obvious quotient homomorphism.

Definition 3.3. We define

$$\theta : J(K\Lambda) \rightarrow \mathcal{C}(O_K G)$$

to be the composition

$$J(K\Lambda) \xrightarrow{\Theta^t} \mathcal{H}(\mathbf{A}(KG)) \rightarrow \mathcal{C}(O_K G),$$

where the second arrow denotes the natural quotient map.

Proposition 3.4. (a) *We have that $h \in \text{Ker}(\psi)$ if and only if K_h/K is unramified at all finite places of K and O_h is $O_K G$ -free. In particular, $\text{Ker}(\psi)$ is finite.*

(b) *The homomorphism ρ is injective.*

(c) *The map $\theta|_{\mathbf{F}}$ is injective.*

Proof. (a) Suppose that $h \in \text{Ker}(\psi)$, with $K_h = KG \cdot b$. Then

$$r_G(b) \in (KG)^\times \cdot H(\mathbf{A}(O_K G)),$$

and this happens if and only if K_h/K is unramified and O_h is $O_K G$ -free (see [7, (2.12), (2.13)]).

(b) This follows directly from the fact that

$$J(KG) \cap H(\mathbf{A}(O_K G)) = \prod_v (O_{K,v} G)^\times.$$

(c) The proof of [7, Proposition 5.4] shows that for each finite place v of K , and $s_1, s_2 \in G_{q_v-1}$, we have $\Theta^t(f_{v,s_1}) = \Theta^t(f_{v,s_2})$ if and only if $s_1 = s_2$. This in turn implies that the restriction of θ to \mathbf{F} is injective, as claimed. \square

Remark 3.5. (1) Suppose that $h \in H_{tr}^1(K, G)$. Then Theorem 2.2 implies that there exists a unique $c \in \text{Cl}(O_K G)$ (namely, (O_h)) and a unique $f \in \mathbf{F}$ such that

$$\rho(c) = \psi(h)^{-1} \theta(f). \quad (3.3)$$

For fixed $c \in \mathcal{R}(O_K G)$ and fixed f , Proposition 3.4(1) implies that there are exactly $|\text{Ker}(\psi)|$ elements $h \in H_{tr}^1(K, G)$ satisfying (3.3).

(2) Theorem 2.3 implies that we have

$$\rho(\mathcal{R}(O_K G)) = \text{Im}(\rho) \cap [\text{Im}(\theta) \cdot \text{Im}(\psi)].$$

\square

Definition 3.6. We define

$$\mathcal{P}_\theta := \{x \in J(K\Lambda) \mid \theta(x) \in \text{Im}(\psi)\}.$$

Proposition 3.7. *Suppose that $c \in \text{Cl}(O_K G)$ with*

$$\rho(c) = \psi(h)^{-1}\theta(\lambda)$$

for some $h \in H_{tr}^1(K, G)$ and $\lambda \in J(K\Lambda)$. Then, for any $\mu \in J(K\Lambda)$, there exists $h_\mu \in H_{tr}^1(K, G)$ such that

$$\rho(c) = \psi(h_\mu)^{-1}\theta(\mu)$$

if and only if $\mu \in \lambda\mathcal{P}_\theta$.

In particular, for any coset $x\mathcal{P}_\theta$ of \mathcal{P}_θ in $J(K\Lambda)$, it follows that $\theta(x\mathcal{P}_\theta)$ is either a subset of, or is distinct from $\text{Im}(\psi) \cdot \text{Im}(\rho)$.

Proof. Suppose that

$$\rho(c) = \psi(h)^{-1}\theta(\lambda) = \psi(h_\mu)^{-1}\theta(\mu).$$

Then we have

$$\theta(\lambda)\theta(\mu)^{-1} = \psi(h)\psi(h_\mu)^{-1},$$

and so $\lambda\mu^{-1} \in \mathcal{P}_\theta$, as claimed.

Conversely, if

$$\rho(c) = \psi(h)^{-1}\theta(\lambda)$$

and $\lambda = \mu\nu$ for some $\nu \in \mathcal{P}_\theta$, then we have

$$\begin{aligned} \rho(c) &= \psi(h)^{-1}\theta(\lambda) \\ &= \psi(h)^{-1}\theta(\mu)\theta(\nu) \\ &= [\psi(h)\psi(h_\nu)]^{-1}\theta(\mu) \end{aligned}$$

for some $h_\nu \in H_{tr}^1(K, G)$, since $\nu \in \mathcal{P}_\theta$.

This establishes the result. □

We can see from Remark 3.5(1) and Proposition 3.7 that counting tame Galois G -extensions of K with a given realisable class is essentially equivalent to counting elements in $\mathbf{F} \cap \lambda\mathcal{P}_\theta$ for a fixed coset $\lambda\mathcal{P}_\theta$ of \mathcal{P}_θ in $J(K\Lambda)$. We therefore now focus our attention on obtaining a good description of $\mathbf{F} \cap \lambda\mathcal{P}_\theta$.

Fix a set of representatives T of $\Omega_K \backslash G(-1)$, and for each $t \in T$, let $K(t)$ be the smallest extension of K such that $\Omega_{K(t)}$ fixes t . Then the Wedderburn decomposition of $K\Lambda$ is given by

$$K\Lambda = \text{Map}_{\Omega_K}(G(-1), K^c) \simeq \prod_{t \in T} K(t), \quad (3.4)$$

where the isomorphism is induced by evaluation on the elements of T .

Definition 3.8. (see [7, §6]) Let \mathcal{M} be an integral ideal of O_K . For each finite place v of K we set $U_{\mathcal{M}}(O_{K,v}^c) = (1 + \mathcal{M}O_{K,v}^c) \cap (O_{K,v}^c)^\times$. We define

$$U'_{\mathcal{M}}(\Lambda_v) \subseteq (K_v\Lambda)^\times = \text{Map}_{\Omega_v}(G(-1), (K_v^c)^\times)$$

by

$$U'_{\mathcal{M}}(\Lambda_v) := \{g_v \in (K_v\Lambda)^\times \mid g_v(s) \in U_{\mathcal{M}}(O_{K,v}^c) \quad \forall s \neq 1\}$$

(with $g_v(1)$ allowed to be arbitrary).

Set

$$U'_{\mathcal{M}}(\Lambda) := \left(\prod_v U'_{\mathcal{M}}(\Lambda_v) \right) \cap J(K\Lambda).$$

The *modified ray class group modulo \mathcal{M}* of Λ is defined by

$$\text{Cl}'_{\mathcal{M}}(\Lambda) := \frac{J(K\Lambda)}{(K\Lambda)^\times \cdot U'_{\mathcal{M}}(\Lambda)}.$$

The group $\text{Cl}'_{\mathcal{M}}(\Lambda)$ is finite, and is isomorphic to the product of the ray class groups modulo \mathcal{M} of the Wedderburn components $K(t)$ (see (3.4)) of $K\Lambda$. \square

The following result shows that each coset $\lambda\mathcal{P}_\theta$ of \mathcal{P}_θ in $J(K\Lambda)$ is a disjoint union of cosets of $U_{\mathcal{M}}(\Lambda) \cdot K\Lambda$ in $J(K\Lambda)$ for a suitably chosen ideal \mathcal{M} of O_K .

Proposition 3.9. *Let \mathcal{M} be an integral ideal of O_K that is divisible by both $|G|$ and $\exp(G)^2$ (where $\exp(G)$ denotes the exponent of G). Then there is a natural quotient homomorphism*

$$f_{\mathcal{M}} : \text{Cl}'_{\mathcal{M}}(\Lambda) \rightarrow \frac{J(K\Lambda)}{\mathcal{P}_\theta}.$$

In particular, the group $J(K\Lambda)/\mathcal{P}_\theta$ is finite.

Proof. Set

$$\mathcal{P}_{\mathcal{M}} := (K\Lambda)^\times \cdot U'_{\mathcal{M}}(\Lambda) \subseteq J(K\Lambda)$$

McCulloh has shown (see [7, Theorem 2.14(ii)]) that if \mathcal{M} is divisible by both $|G|$ and $\exp(G)^2$, then

$$\Theta^t(\mathcal{P}_{\mathcal{M}}) \subseteq \mathcal{H}(\mathbf{A}(O_K G)),$$

whence it follows from the definition of θ that $\theta(\mathcal{P}_{\mathcal{M}}) = 0$. This implies that

$$\mathcal{P}_{\mathcal{M}} \subseteq \mathcal{P}_\theta \subseteq J(K\Lambda),$$

and so there is a natural quotient homomorphism $f_{\mathcal{M}}$, as asserted. Since $\text{Cl}'_{\mathcal{M}}(\Lambda)$ is finite, it follows that the same is true of $J(K\Lambda)/\mathcal{P}_\theta$. \square

Let $I(\Lambda)$ denote the group of fractional ideals of Λ . Via the Wedderburn decomposition (3.4) of λ , each ideal \mathfrak{A} of in $I(\Lambda)$ may be written $\mathfrak{A} = (\mathfrak{A}_t)_{t \in T}$, where each \mathfrak{A}_t is a fractional ideal of $O_{K(t)}$.

For any idele $\lambda \in J(K\Lambda)$, we write $\text{co}(\lambda) \in I(\Lambda)$ for the ideal obtained by taking the idele content of λ . The following proposition describes exactly which ideals in $I(\Lambda)$ arise via taking the idele content of elements in $\mathbf{F} \subseteq J(K\Lambda)$.

Proposition 3.10. *Let \mathfrak{F} be the subset of $I(\Lambda)$ defined by*

$$\mathfrak{F} = \{\text{co}(f) \mid f \in \mathbf{F}\}.$$

The \mathfrak{F} consists precisely of those ideals $\mathfrak{f} = (\mathfrak{f}_t)_{t \in T}$ such that

- $\mathfrak{f}_1 = O_K$;
- $N_{K(\Lambda)/K}(\mathfrak{f}) := \prod_{t \in T} N_{K(t)/K}(\mathfrak{f}_t)$ is a squarefree O_K -ideal;
- \mathfrak{f}_t is coprime to the order $|t|$ of t .

In particular, if we view \mathbf{F}_v as being a subset of \mathbf{F} via the obvious embedding $(K_v\Lambda)^\times \subseteq J(K\Lambda)$, then

$$\mathfrak{F}_v : \{\text{co}(f_v) \mid f_v \in \mathbf{F}_v\}$$

consists precisely of the invertible prime ideals of Λ arising via (3.4) from the invertible prime ideals of relative degree one over v in those Wedderburn components $K(t)$ of Λ for which $t \neq 1$ and $v(|t|) = 0$.

Proof. See [7, pages 288-289]. □

Example 3.11. Suppose that $h \in H_{tr}^1(K, G)$. Recall (see Remark 3.5) that there exist unique $c \in \mathcal{R}(O_K G)$ and $f \in \mathbf{F}$ such that $\rho(c) = \psi(h)^{-1}\theta(f)$. Let

$$\text{co}(f) = \mathfrak{f} = (\mathfrak{f}_t)_{t \in T}.$$

Then each ideal \mathfrak{f}_t of $O_{K(t)}$ may be written as a product

$$\mathfrak{f}_t = \mathcal{P}_{t,1} \cdots \mathcal{P}_{t,i_t}$$

of primes of relative degree one in $K(t)/K$. Each finite place v of K that ramifies in K_h/K lies beneath exactly one ideal $\mathcal{P}_{t,j}$, and in this case the ramification index of v in K_h/K is equal to $|t|$ (see [7, Proposition 5.4]). It therefore follows from the standard formula for tame discriminants that

$$\text{disc}(K_h/K) = \prod_{t \in T} N_{K(t)/K}(\mathfrak{f}_t)^{(|t|-1)|G|/|t|}.$$

Hence the absolute norm $\mathcal{D}(K_h/K)$ of $\text{disc}(K_h/K)$ is given by

$$\mathcal{D}(K_h/K) = \left[O_K : \prod_{t \in T} N_{K(t)/K}(\mathfrak{f}_t)^{(|t|-1)|G|/|t|} \right].$$

Let $d(\mathfrak{f}) = (d(\mathfrak{f}_t))_{t \in T}$ denote the ideal in $I(\Lambda)$ defined by $d(\mathfrak{f})_1 = O_K$ and

$$d(\mathfrak{f})_t = \mathfrak{f}_t^{(|t|-1)|G|/|t|}$$

for $t \neq 1$. Then since

$$[O_{K(t)} : \mathfrak{f}_t] = [O_K : N_{K(t)/K}(\mathfrak{f}_t)],$$

for each $t \neq 1$, it follows that we have

$$\mathcal{D}(K_h/K) = [\Lambda : d(\mathfrak{f})].$$

□

Example 3.11 motivates the following definitions.

Definition 3.12. We say that a function

$$\mathcal{W} : T \rightarrow \mathbf{Z}_{\geq 0}$$

is a *weight function on T* (or just a *weight* for short) if $\mathcal{W}(1) = 0$ and $\mathcal{W}(t) \neq 0$ for all $t \neq 1$.

For any weight \mathcal{W} , we set

$$\alpha_{\mathcal{W}} = \min\{\mathcal{W}(t) : t \neq 1\}.$$

□

Definition 3.13. Suppose that \mathcal{W} is a weight and $\mathfrak{A} = (\mathfrak{A}_t)_{t \in T}$ is an ideal in $I(\Lambda)$. We write $d_{\mathcal{W}}(\mathfrak{A}) = (d_{\mathcal{W}}(\mathfrak{A})_t)_{t \in T}$ for the ideal in $I(\Lambda)$ defined by $d_{\mathcal{W}}(\mathfrak{A})_t = \mathfrak{A}_t^{\mathcal{W}(t)}$. □

Definition 3.14. Suppose that $h \in H_{tr}^1(K, G)$ with $\rho(c) = \psi(h)^{-1}\theta(f)$. For any weight function \mathcal{W} on T , we set

$$D_{\mathcal{W}}(K_h/K) := [\Lambda : d_{\mathcal{W}}(\text{co}(f))]. \quad (3.5)$$

Example 3.15. Let K_h/K be any tamely ramified Galois G -extension of K .

(1) Define a weight function $\mathcal{W}_{\text{disc}}$ on T by $\mathcal{W}_{\text{disc}}(t) = (|t| - 1)|G|/|t|$ for $t \neq 1$. Then we see from Example 3.11 that $D_{\mathcal{W}_{\text{disc}}}(K_h/K)$ is equal to the absolute norm of the relative discriminant of K_h/K .

(2) Define a weight function \mathcal{W}_{ram} on T by $\mathcal{W}_{\text{ram}}(t) = 1$ for $t \neq 1$. Then $D_{\mathcal{W}_{\text{ram}}}(K_h/K)$ is equal to the absolute norm of the product of the primes of K that are ramified in K_h/K . □

We now fix once and for all an integral ideal \mathcal{M} of O_K that is divisible by both $|G|$ and $\exp(G)^2$, and weight function \mathcal{W} on T .

Definition 3.16. For each $c \in \mathcal{R}(O_K G)$ and each real number $X > 0$, we write $N_{\mathcal{W}}(c, X; \mathcal{M})$ for the number of tame Galois G -extensions K_h/K for which $(O_h) = c$, $D_{\mathcal{W}}(K_h/K)$ is coprime to \mathcal{M} , and $D_{\mathcal{W}}(K_h/K) \leq X$.

Let $M_{\mathcal{W}}(X; \mathcal{M})$ denote the number of tame Galois G -extensions K_h/K for which $D_{\mathcal{W}}(K_h/K) \leq X$ and $D_{\mathcal{W}}(K_h/K)$ is coprime to \mathcal{M} .

Question 3.17. *What can be said about the behaviour of $N_{\mathcal{W}}(c, X; \mathcal{M})$ as $X \rightarrow \infty$? For example, is*

$$Z_{\mathcal{W}}(c; \mathcal{M}) := \lim_{X \rightarrow \infty} \frac{N_{\mathcal{W}}(c, X; \mathcal{M})}{M_{\mathcal{W}}(X; \mathcal{M})}$$

independent of c ? □

For each coset \mathfrak{c} of $\mathcal{P}_{\mathcal{M}}$ in $J(K\Lambda)$, set

$$\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M}) = \{f \in \mathbf{F} \cap \mathfrak{c} \mid (\text{co}(f), \mathcal{M}) = 1 \text{ and } [\Lambda : d_{\mathcal{W}}(\text{co}(f))] \leq X\}$$

Then it follows from Remark 3.5(1) and Proposition 3.7 that there is a unique coset $\lambda_c \mathcal{P}_{\theta}$ of \mathcal{P}_{θ} in $J(K\Lambda)$ such that

$$\begin{aligned} N_{\mathcal{W}}(c, X; \mathcal{M}) &= |\text{Ker}(\psi)| \cdot |\{f \in F \cap \lambda_c \mathcal{P}_{\theta} \mid (\text{co}(f), \mathcal{M}) = 1 \text{ and } [\Lambda : d_{\mathcal{W}}(\text{co}(f))] \leq X\}| \\ &= |\text{Ker}(\psi)| \cdot \sum_{\mathfrak{c} \in f_{\mathcal{M}}^{-1}(c)} \kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M}). \end{aligned} \quad (3.6)$$

We therefore see that the behaviour of $N_{\mathcal{W}}(c, X; \mathcal{M})$ as $X \rightarrow \infty$ is governed by that of the $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$. For example, if $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$ is asymptotically independent of \mathfrak{c} (see Definition 5.3 below), then it follows that asymptotically, $N_{\mathcal{W}}(c, X; \mathcal{M})$ is independent of the realisable class $c \in \mathcal{R}(O_K G)$.

4. EULER PRODUCTS

Recall (see Proposition 3.10) that \mathfrak{F} denotes the subset of $I(\Lambda)$ defined by

$$\mathfrak{F} = \{\text{co}(f) \mid f \in \mathbf{F}\}.$$

Definition 4.1. We define functions $D(s)$ and $D_{\mathcal{M}}(s)$ of a complex variable s by

$$D(s) := \sum_{\mathfrak{a} \in \mathfrak{F}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}; \quad D_{\mathcal{M}}(s) := \sum_{\substack{\mathfrak{a} \in \mathfrak{F} \\ (\mathfrak{a}, \mathcal{M})=1}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}. \quad (4.1)$$

For any $\mathfrak{c} \in \text{Cl}'_{\mathcal{M}}(\Lambda)$, we set

$$D_{\mathfrak{c}}(s) := \sum_{\mathfrak{a} \in \mathfrak{F} \cap \mathfrak{c}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}; \quad D_{\mathfrak{c}, \mathcal{M}}(s) := \sum_{\substack{\mathfrak{a} \in \mathfrak{F} \cap \mathfrak{c} \\ (\mathfrak{a}, \mathcal{M})=1}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}. \quad (4.2)$$

Each of the functions above also depends upon the choice of \mathcal{W} ; we omit this dependence from our notation. \square

Let χ be any character of $\text{Cl}'_{\mathcal{M}}(\Lambda)$, and set $T' := T \setminus \{1\}$. Then via the Wedderburn decomposition (3.4) of Λ , we may write $\chi = (\chi_t)_{t \in T'}$, where each χ_t is a character of the ray class group modulo \mathcal{M} of $K(t)$. We may view χ as being a map on the set of all integral ideals $\mathfrak{a} = (\mathfrak{a}_t)_{t \in T'}$ in the standard manner by setting $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}_1 \neq O_K$ or if \mathfrak{a} is not coprime to \mathcal{M} .

Definition 4.2. For each character χ of $\text{Cl}'_{\mathcal{M}}(\Lambda)$, we define

$$D(s, \chi) = \sum_{\mathfrak{a} \in \mathfrak{F}} \chi(\mathfrak{a}) [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}. \quad (4.3)$$

\square

With the above definitions, we have

$$D_{\mathfrak{c}, \mathcal{M}}(s) = \frac{1}{|\text{Cl}'_{\mathcal{M}}(\Lambda)|} \sum_{\chi} \bar{\chi}(\mathfrak{c}) D(s, \chi), \quad (4.4)$$

where the sum is over all characters χ of $\text{Cl}'_{\mathcal{M}}(\Lambda)$.

Definition 4.3. (cf. [2, Chapter I]) Let $\mathfrak{a} = (\mathfrak{a}_t)_{t \in T}$ be any ideal in $I(\Lambda)$. We define the *module index* $[\Lambda : \mathfrak{a}]_{O_K}$ to be the O_K -ideal given by

$$[\Lambda : \mathfrak{a}]_{O_K} := \prod_{t \in T} N_{K(t)/K}(\mathfrak{a}_t). \quad (4.5)$$

\square

Lemma 4.4. For each integral O_K -ideal \mathfrak{b} , set

$$\nu(\mathfrak{b}) := |\{\mathfrak{a} \in \mathfrak{F} \mid [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]_{O_K} = \mathfrak{b}\}|.$$

Then ν is multiplicative, i.e. if $\mathfrak{b}_1, \mathfrak{b}_2$ are coprime O_K -ideals, we have

$$\nu(\mathfrak{b}_1 \mathfrak{b}_2) = \nu(\mathfrak{b}_1) \nu(\mathfrak{b}_2).$$

Proof. It follows from Proposition 3.10 that if $\mathfrak{a}_1, \mathfrak{a}_2$ are in \mathfrak{F} , and $[\Lambda : d_{\mathcal{W}}(\mathfrak{a}_1)]_{O_K}$ and $[\Lambda : d_{\mathcal{W}}(\mathfrak{a}_2)]_{O_K}$ are coprime, then $\mathfrak{a}_1 \mathfrak{a}_2$ lies in \mathfrak{F} also. Hence, for any choice of ideals $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{F}$ with $[\Lambda : d_{\mathcal{W}}(\mathfrak{a}_i)]_{O_K} = \mathfrak{b}_i$ ($i = 1, 2$), we have

$$\begin{aligned} [\Lambda : d_{\mathcal{W}}(\mathfrak{a}_1 \mathfrak{a}_2)]_{O_K} &= [\Lambda : d_{\mathcal{W}}(\mathfrak{a}_1)]_{O_K} \cdot [\Lambda : d_{\mathcal{W}}(\mathfrak{a}_2)]_{O_K} \\ &= \mathfrak{b}_1 \cdot \mathfrak{b}_2, \end{aligned}$$

and so we deduce that $\nu(\mathfrak{b}_1 \mathfrak{b}_2) \geq \nu(\mathfrak{b}_1) \nu(\mathfrak{b}_2)$.

To show the reverse inequality, set $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$, and let $\mathfrak{a} \in \mathfrak{F}$ be any ideal such that $[\Lambda : d_{\mathcal{W}}(\mathfrak{a})]_{O_K} = \mathfrak{b}$. For each $i = 1, 2$, let \mathfrak{a}_i be the product of all primes \mathfrak{P} of Λ with \mathfrak{P} a prime factor of \mathfrak{a} and $[\Lambda : \mathfrak{P}]_{O_K}$ a prime factor of \mathfrak{b}_i . Then we have

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \quad \mathfrak{a}_i \in \mathfrak{F}, \quad \text{and} \quad [\Lambda : \mathfrak{a}_i]_{O_K} = \mathfrak{b}_i, \quad (i = 1, 2). \quad (4.6)$$

Furthermore, it follows via uniqueness of factorisation in Λ and O_K that \mathfrak{a}_1 and \mathfrak{a}_2 are the unique ideals satisfying (4.6). This implies that $\nu(\mathfrak{b}_1\mathfrak{b}_2) \leq \nu(\mathfrak{b}_1)\nu(\mathfrak{b}_2)$, and so we finally deduce that $\nu(\mathfrak{b}_1\mathfrak{b}_2) = \nu(\mathfrak{b}_1)\nu(\mathfrak{b}_2)$ as asserted. \square

Proposition 4.5. *The functions $D(s)$ and $D(s, \chi)$ admit Euler product expansions over the rational primes:*

$$D(s) = \prod_p D_p(s), \quad D(s, \chi) = \prod_p D_p(s, \chi).$$

Proof. Suppose that $\mathfrak{a} \in \mathfrak{F}$, with $[\Lambda : d_{\mathcal{W}}(\mathfrak{a})]_{O_K} = \mathfrak{b}$. Then it follows from Proposition 3.10 that

$$[\Lambda : d_{\mathcal{W}}(\mathfrak{a})] = [O_K : \mathfrak{b}].$$

This in turn implies that

$$\begin{aligned} D(s) &= \sum_{\mathfrak{a} \in \mathfrak{F}} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})] \\ &= \sum_{\substack{\mathfrak{b} \in I(O_K) \\ \mathfrak{b} \subseteq O_K}} \nu(\mathfrak{b}) [O_K : \mathfrak{b}]^{-s}. \end{aligned}$$

Since ν is multiplicative, we have

$$D(s) = \prod_{\substack{\mathfrak{p} \in I(O_K) \\ \mathfrak{p} \text{ prime}}} D_{\mathfrak{p}}(s),$$

where

$$D_{\mathfrak{p}}(s) = 1 + \sum_{m=1}^{\infty} \nu(\mathfrak{p}^m) [O_K : \mathfrak{p}]^{-ms}.$$

Next, we observe that since $\mathfrak{a} \in \mathfrak{F}$ implies that \mathfrak{a} is squarefree (see Proposition 3.10), it follows that we can find a positive integer N , say, independent of \mathfrak{p} , such that $\nu(\mathfrak{p}^m) = 0$ for all $m > N$. (In fact $N = |G| \cdot \max\{\mathcal{W}(t) \mid t \in T\}$ will do.) We may therefore write

$$D_{\mathfrak{p}}(s) = 1 + \sum_{m=1}^N \nu(\mathfrak{p}^m) [O_K : \mathfrak{p}]^{-ms},$$

and we define $D_p(s)$ by

$$D_p(s) = \prod_{\mathfrak{p}|p} D_{\mathfrak{p}}(s).$$

Then (again using the fact that ν is multiplicative), we see that

$$D(s) = \prod_p D_p(s),$$

as claimed.

We now show that $D(s, \chi)$ also admits an Euler product expansion. For each rational prime p , set

$$\mathfrak{F}(p) := \{\mathfrak{a} \in \mathfrak{F} \mid [\Lambda : \mathfrak{a}] \text{ is a non-negative power of } p\}.$$

Observe that $\mathfrak{a} \in \mathfrak{F}(p)$ if and only if all prime factors of \mathfrak{a} in Λ lie above p , and we have that

$$D_p(s) = \sum_{\mathfrak{a} \in \mathfrak{F}(p)} [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}.$$

We therefore deduce that

$$D(s, \chi) = \prod_p D_p(s, \chi),$$

where

$$D_p(s, \chi) = \sum_{\mathfrak{a} \in \mathfrak{F}(p)} \chi(\mathfrak{a}) [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}.$$

This establishes the desired result. \square

5. THE ASYMPTOTIC BEHAVIOUR OF $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$

In this section we shall obtain an expression for

$$\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M}) := \{f \in \mathbf{F} \cap \mathfrak{c} \mid (\text{co}(f), \mathcal{M}) = 1 \text{ and } [\Lambda : d_{\mathcal{W}}(\text{co}(f))] \leq X\}$$

for each $\mathfrak{c} \in J(K\Lambda)/\mathcal{P}_{\mathcal{M}}$ when X is large. We shall do this by appealing to the following version of the D elange-Ikehara Tauberian theorem.

Theorem 5.1. *Suppose that $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is a Dirichlet series with non-negative coefficients, and that it is convergent for $\Re(s) > a > 0$. Assume that in its domain of convergence,*

$$f(s) = g(s)(s - a)^{-w} + h(s)$$

holds, where $g(s), h(s)$ are holomorphic functions in the closed half-plane $\Re(s) \geq a$, $g(a) \neq 0$, and $w > 0$. Then, as $X \rightarrow \infty$, we have

$$\sum_{n \leq X} a_n \sim \frac{g(a)}{a \cdot \Gamma(w)} \cdot X^a \cdot (\log X)^{w-1}.$$

Proof. See [8, p. 21]. \square

We see from (4.4) that each function $D_{\mathbf{c},\mathcal{M}}(s)$ is convergent in some right-hand half-plane, because $D(s, \chi)$ has an Euler-product expansion for all $\chi \in \widehat{\text{Cl}'_{\mathcal{M}}(\Lambda)}$. It also follows from the definitions that each $D_{\mathbf{c},\mathcal{M}}(s)$ is a Dirichlet series with non-negative coefficients. If we write

$$D_{\mathbf{c},\mathcal{M}}(s) = \sum_{n=0}^{\infty} a_n n^{-s}.$$

then we have

$$\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M}) = \sum_{n \leq X} a_n.$$

For each $\mathbf{c} \in J(K\Lambda)/\mathcal{P}_{\mathcal{M}}$, let $\beta(\mathbf{c}; \mathcal{M})$ denote right-most pole of $D_{\mathbf{c},\mathcal{M}}(s)$ in the complex plane. Let $\delta(\mathbf{c}; \mathcal{M})$ denote the order of this pole, and set $a(\mathbf{c}; \mathcal{M}) := \Re(\beta(\mathbf{c}; \mathcal{M}))$. Write

$$\tau(\mathbf{c}; \mathcal{M}) := \lim_{s \rightarrow \beta(\mathbf{c}; \mathcal{M})} (s - \beta(\mathbf{c}; \mathcal{M}))^{\delta(\mathbf{c}; \mathcal{M})} D_{\mathbf{c},\mathcal{M}}(s).$$

Proposition 5.2. *As $X \rightarrow \infty$, we have*

$$\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M}) \sim \frac{\tau(\mathbf{c}; \mathcal{M})}{a(\mathbf{c}; \mathcal{M}) \cdot \Gamma(\delta(\mathbf{c}; \mathcal{M}))} \cdot X^{a(\mathbf{c}; \mathcal{M})} \cdot (\log X)^{\delta(\mathbf{c}; \mathcal{M})-1}.$$

Proof. This follows directly from Theorem 5.1. □

Definition 5.3. If

$$\kappa_{\mathcal{W}}(\mathbf{c}_1, X; \mathcal{M}) \sim \kappa_{\mathcal{W}}(\mathbf{c}_2, X; \mathcal{M}) \tag{5.1}$$

as $X \rightarrow \infty$ for all $\mathbf{c}_1, \mathbf{c}_2 \in \text{Cl}'_{\mathcal{M}}(\Lambda)$, then we shall say that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} .

It is not hard to see that (5.1) holds for all $\mathbf{c}_1, \mathbf{c}_2 \in \text{Cl}'_{\mathcal{M}}(\Lambda)$ if and only if the numbers $\tau(\mathbf{c}; \mathcal{M})$, $a(\mathbf{c}; \mathcal{M})$, $\delta(\mathbf{c}; \mathcal{M})$ and $\beta(\mathbf{c}; \mathcal{M})$ do not vary with \mathbf{c} . □

We shall see in Section 7 that, in general, $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is not asymptotically independent of \mathbf{c} .

6. DIRICHLET L -SERIES

We now turn our attention to certain Dirichlet L -series associated to Λ .

Definition 6.1. Suppose that $\chi = (\chi_t)_{t \in T^v}$ is a character of $\text{Cl}'_{\mathcal{M}}(\Lambda)$. We define

$$L_{\Lambda}(s, \chi) := \sum_{\substack{\mathfrak{a} \in I(\Lambda) \\ \mathfrak{a} \subseteq \Lambda}} \chi(\mathfrak{a}) [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}.$$

□

Remark 6.2. (1) For each character $\chi = (\chi_t)_{t \in T'}$ of $\text{Cl}'_{\mathcal{M}}(\Lambda)$, the function $L_{\Lambda}(s, \chi)$ is a product of L -functions of number fields. If we set

$$L_t(s, \chi_t) = \sum_{\substack{\mathfrak{b} \in I(O_{K(t)}) \\ \mathfrak{b} \subseteq O_{K(t)}}} \chi_t(\mathfrak{b}) \mathfrak{b}^{-\mathcal{W}(t)s},$$

then corresponding to the Wedderburn decomposition (3.4) of $K\Lambda$, we have

$$L_{\Lambda}(s, \chi) = \prod_{t \in T'} L_t(s, \chi_t). \quad (6.1)$$

It follows from standard properties of Dirichlet L -series that $L_t(\frac{1}{\mathcal{W}(t)}, \chi_t) \neq 0$ if $\chi_t \neq 1$ and that $L_t(s, \mathbf{1}_t)$ has a simple pole at $s = 1/\mathcal{W}(t)$.

(2) The function $L_{\Lambda}(s, \chi)$ has an Euler product given by

$$L_{\Lambda}(s, \chi) = \prod_p L_{\Lambda, p}(s, \chi),$$

where

$$L_{\Lambda, p}(s, \chi) = \sum_{\mathfrak{a} \in \mathfrak{F}(p)} \chi(\mathfrak{a}) [\Lambda : d_{\mathcal{W}}(\mathfrak{a})]^{-s}.$$

Let $P_1, \dots, P_{n(p)}$ be the invertible primes of Λ which lie above the rational prime p . (Note that the integer $n(p)$ is bounded above independently of p .) Then we also have

$$L_{\Lambda, p} = \prod_{i=1}^{n(p)} \chi(P_i) [\Lambda : d_{\mathcal{W}}(P_i)]^{-s}.$$

□

In Section 7 we shall compare the functions $L_{\Lambda}(s, \chi)$ and $D(s, \chi)$ by examining corresponding terms in their Euler product expansions. In order to do this, we shall need the following two technical lemmas from [3].

Lemma 6.3. ([3, Lemma 1.1]) *Expand*

$$F(z_1, \dots, z_n) := \prod_{i=1}^n (1 - z_i)^{-1}$$

as an infinite series of monomials in z_1, \dots, z_n . Suppose that $0 < r \leq r_0 < 1$, and that there is a positive integer $m \leq n$ such that $|z_i| \leq r$ and $i \leq m$ and $|z_i| < r^2$ for $i > m$.

Then, if $f(z_1, \dots, z_n)$ is any subseries of the series for $F(z_1, \dots, z_n)$ containing the terms $1 + \sum_{i=1}^m z_i$, we have

$$|F(z_1, \dots, z_n) - f(z_1, \dots, z_n)| \leq \left[\frac{n(n+1)}{2(1-r_0)^{n+2}} + n \right] r^2.$$

Proof. Since the series for $F - f$ has only positive coefficients, it follows that an upper bound for $|F - f|$ may be obtained by setting $z_i = r$ for $i \leq m$, and $z_i = r^2$ for $i > m$, and by replacing $f(z_1, \dots, z_n)$ with $1 + \sum_{i=1}^m z_i$.

For the terms of degree one in $F - f$, we have

$$\left| \sum_{i=m+1}^n z_i \right| \leq nr^2.$$

Also, as each term of degree k with $k \geq 2$ has absolute value at most r^k , it follows that the sum of all such terms (for all $k \geq 2$) has absolute value at most $(1 - r)^{-n} - (1 + nr)$. Applying the Extended Mean Value Theorem twice to the functions

$$h_1(x) = (1 - x)^{-n} - (1 + nr), \quad h_2(x) = x^2$$

on the interval $(0, r)$ yields the inequality

$$0 < (1 - r)^{-n} - (1 + nr) \leq \frac{n(n+1)}{2(1-r)^{n+2}} \cdot r^2.$$

Therefore, since $r \leq r_0 < 1$, we obtain

$$|F(z_1, \dots, z_n) - f(z_1, \dots, z_n)| \leq \frac{n(n+1)}{2(1-r)^{n+2}} \cdot r^2 + nr^2.$$

This completes the proof. □

Lemma 6.4. ([3, Lemma 1.2] *Let $\phi(s)$ and $\phi^*(s)$ be Dirichlet series with Euler products*

$$\phi(s) = \prod_p \phi_p(s), \quad \phi^*(s) = \prod_p \phi_p^*(s)$$

over the rational primes. Suppose that $\phi(s)$ and $\phi^(s)$ are absolutely convergent for $\Re(s) > 1$.*

Suppose further that:

(i) *For every p , $\phi_p(s)$ and $\phi_p^*(s)$ are analytic for $\Re(s) > 0$;*

(ii) *Given a real number σ_0 with $0 < \sigma_0 < 1$, there exists $B(\sigma_0) = B > 0$ such that*

$$\left| \frac{\phi_p^*(s) - \phi_p(s)}{\phi_p^*(s)} \right| < B \cdot p^{-2\sigma_0}$$

for every p and $\sigma = \Re(s) \geq \sigma_0$.

Then $\phi(s) = \phi^(s)\psi(s)$, where $\psi(s)$ is analytic for $\Re(s) > 1/2$. If $z \in \mathbf{C}$ satisfies $\Re(z) > 1/2$, and if $\phi_p(z) \neq 0$ for all p , then $\psi(z) \neq 0$.*

Proof. We first observe that (i) implies that $\phi_p(s)/\phi_p^*(s)$ is meromorphic for $\Re(s) > 0$, and so it follows from (ii) that in fact $\phi_p(s)/\phi_p^*(s)$ is analytic for $\Re(s) > 0$. For $\Re(s) > 1$, define

$$\psi(s) = \prod_p \frac{\phi_p(s)}{\phi_p^*(s)} = \prod_p \left[1 - \frac{\phi_p^*(s) - \phi_p(s)}{\phi_p^*(s)} \right].$$

We see from (ii) that this product converges whenever $\sum_p p^{-2\sigma}$ converges, i.e. for $\Re(s) = \sigma > 1/2$. This implies that $\psi(s)$ is analytic for $\Re(s) > 1/2$.

It is easy to verify that we have $\phi(s) = \phi^*(s)\psi(s)$ as a formal identity. If $\phi_p(z) \neq 0$ for all p , then none of the factors of $\psi(z)$ are zero. Since the product defining $\psi(z)$ is absolutely convergent, it follows that $\psi(z) \neq 0$, as claimed. \square

7. THE POLES OF $D(s, \chi)$ AND $D_{c, \mathcal{M}}(s)$

In this section, using techniques described in [3], we shall examine the poles of $D(s, \chi)$ and $D_{c, \mathcal{M}}(s)$. We shall do this by comparing the Euler product expansion of $D(s, \chi)$ with that of $L_\Lambda(s, \chi)$ and applying Lemmas 6.3 and 6.4.

Proposition 7.1. *For each rational prime p with $p \nmid \mathcal{M}$, we have*

$$|L_{\Lambda, p}(s, \chi) - D_p(s, \chi)| \leq \left[\frac{n(n+1)}{(1-2^{-\sigma_0})^{n+2}} + n \right] p^{-2\alpha_{\mathcal{W}}\Re(s)},$$

for any real number σ_0 satisfying $0 < \sigma_0 < \alpha_{\mathcal{W}}\Re(s)$.

Proof. We first observe that the series defining $D_p(s, \chi)$ is a subseries of the series defining $L_{\Lambda, p}(s, \chi)$. Also, the series defining $D_p(s, \chi)$ contains the terms

$$1 + \sum_{i=1}^m \chi(P_i) [\Lambda : d_{\mathcal{W}}(P_i)]^{-s},$$

where the P_i are arranged so that P_1, \dots, P_m satisfy $[\Lambda : P_i] = p$, and P_{m+1}, \dots, P_n satisfy $[\Lambda : P_i] \geq p^2$.

In Lemma 6.3, we take

$$z_i := \chi(P_i) [\Lambda : d_{\mathcal{W}}(P_i)]^{-s}, \quad F(z_1, \dots, z_n) := L_{\Lambda, p}(s, \chi), \quad f(z_1, \dots, z_n) := D_p(s, \chi).$$

We observe that, for $1 \leq i \leq n$, we have

$$[\Lambda : d_{\mathcal{W}}(P_i)] \geq p^{\alpha_{\mathcal{W}}},$$

and so

$$\begin{aligned} |[\Lambda : d_{\mathcal{W}}(P_i)]| &\geq |p^{-\alpha s}| \\ &= p^{-\alpha \Re(s)}. \end{aligned}$$

Hence, if we set $r = p^{-\alpha\Re(s)}$ and $r_0 = 2^{-\sigma_0}$ with $0 < \sigma_0 \leq \alpha\Re(s)$, then we have $0 < r \leq r_0 < 1$, $|z_i| \leq r$ for $1 \leq i \leq m$, and $|z_i| \leq r^2$ for $m+1 \leq i \leq n$. So, the conditions of Lemma 6.3 are satisfied, and we have

$$|L_{\Lambda,p}(s, \chi) - D_p(s, \chi)| \leq \left[\frac{n(n+1)}{(1-2^{-\sigma_0})^{n+2}} + n \right] p^{-2\alpha_{\mathcal{W}}\Re(s)},$$

as claimed. \square

Proposition 7.2. *For each character $\chi = (\chi_t)_{t \in T'}$ of $\text{Cl}'_{\mathcal{M}}(\Lambda)$, we may write*

$$D(s, \chi) = L_{\Lambda}(s, \chi) \cdot \psi(s, \chi),$$

where $\psi(s, \chi)$ is analytic for $\Re(s) > 1/2\alpha_{\mathcal{W}}$.

If $z \in \mathbf{C}$ satisfies $\Re(z) > 2\alpha_{\mathcal{W}}$, and $D_p(z, \chi) \neq 0$ for all p , then $\psi(z, \chi) \neq 0$.

Proof. To prove the desired result, we are going to apply Lemma 6.4 with

$$\phi(s) = D(s, \chi), \quad \phi^*(s) = L_{\Lambda}(s, \chi).$$

We first note that for each prime p with $p \nmid \mathcal{M}$, the Euler factor $L_{\Lambda,p}(s, \chi)$ is analytic for $\Re(s) > 0$. This implies that $D_p(s, \chi)$ is also analytic for $\Re(s) > 0$, because the series defining $D_p(s, \chi)$ is a subseries of the series defining $L_{\Lambda,p}(s, \chi)$.

Set $N := \dim_{\mathbf{Q}}(K\Lambda)$. We have

$$\begin{aligned} |L_{\Lambda,p}(s, \chi)|^{-1} &= \prod_{i=1}^{n(p)} |(1 - \chi(P_i)[\Lambda : d_{\mathcal{W}}(P_i)]^{-s})| \\ &\leq (1 - p^{-\alpha_{\mathcal{W}}\Re(s)})^N. \end{aligned}$$

In particular, this implies that

$$|L_{\Lambda,p}(s, \chi)|^{-1} \leq (1 + 2^{-\sigma_0})^N \tag{7.1}$$

for all $p \nmid \mathcal{M}$ and for all $s \in \mathbf{C}$ with $\alpha\Re(s) \geq \sigma_0$. Applying Proposition 7.1 gives

$$|L_{\Lambda,p}(s, \chi)| \cdot \left| \frac{L_{\Lambda,p}(s, \chi) - D_p(s, \chi)}{L_{\Lambda,p}(s, \chi)} \right| \leq \left[\frac{n(n+1)}{(1-2^{-\sigma_0})^{n+2}} + n \right] p^{-2\alpha_{\mathcal{W}}\Re(s)}.$$

We therefore see from (7.1) that

$$\begin{aligned} \left| \frac{L_{\Lambda,p}(s, \chi) - D_p(s, \chi)}{L_{\Lambda,p}(s, \chi)} \right| &\leq \left[\frac{n(n+1)}{(1-2^{-\sigma_0})^{n+2}} + n \right] p^{-2\alpha_{\mathcal{W}}\Re(s)} \cdot (1 + 2^{-\sigma_0})^N \\ &= B(\sigma_0) \cdot p^{-2\alpha_{\mathcal{W}}\Re(s)}, \end{aligned}$$

say. Hence condition (ii) of Lemma 6.4 is satisfied, but with $\sigma = \alpha_{\mathcal{W}}\Re(s)$, rather than $\sigma = \Re(s)$.

Lemma 6.4 therefore implies that we may write

$$D(s, \chi) = L_\Lambda(s, \chi) \cdot \psi(s, \chi),$$

where $\psi(s, \chi)$ is analytic for $\Re(s) > 1/2\alpha_{\mathcal{W}}$.

The final assertion follows just as in the proof of Lemma 6.4. \square

Definition 7.3. For each positive integer n and each character $\chi \in \widehat{\text{Cl}'_{\mathcal{M}}(\Lambda)}$, set

$$d_n(\chi) := |\{t \in T' \mid \chi_t = \mathbf{1} \text{ and } \mathcal{W}(t) = n\}|;$$

$$d_n := \max_{\chi} \{d_n(\chi)\};$$

$$b_n(\chi) := \lim_{s \rightarrow \frac{1}{n}} \left(s - \frac{1}{n}\right)^{d_n} D(\chi, s).$$

\square

Proposition 7.4. *Let $1 \leq n < 2\alpha_{\mathcal{W}}$ be a positive integer.*

(a) *The function $D(\mathbf{1}, s)$ has a pole of exact order $d_n(\mathbf{1})$ at $s = 1/n$.*

(b) *If $\chi \neq \mathbf{1}$, then $D(\chi, s)$ has a pole of order at most $d_n(\chi)$ at $s = 1/n$.*

(c) *For each $\mathfrak{c} \in \text{Cl}'_{\mathcal{M}}(\Lambda)$, the function $D_{\mathfrak{c}, \mathcal{M}}(s)$ has a pole of order at most d_n at $s = 1/n$, and*

$$\lim_{s \rightarrow \frac{1}{n}} \left(s - \frac{1}{n}\right) D_{\mathfrak{c}, \mathcal{M}}(s) = \frac{1}{|\text{Cl}'_{\mathcal{M}}(\Lambda)|} \sum_{\chi} \bar{\chi}(\mathfrak{c}) b_n(\chi).$$

Proof. From (6.1) and Proposition 7.2, we have

$$D(s, \chi) = L_\Lambda(s, \chi) \cdot \psi(s, \chi) = \left[\prod_{t \in T'} L_t(s, \chi_t) \right] \cdot \psi(s, \chi), \quad (7.2)$$

where $\psi(s, \chi)$ is analytic for $\Re(s) > 1/2\alpha_{\mathcal{W}}$. For each $t \in T'$, the Dirichlet L -function $L_t(s, \chi_t)$ is entire unless $\chi_t = \mathbf{1}_t$ in which case it has a single (simple) pole at $s = 1/\mathcal{W}(t)$. This implies that, for *any* positive integer n , the function $L_\Lambda(s, \chi)$ has a pole of order exactly $d_n(\chi)$ (which of course may be equal to zero!) at $s = 1/n$.

If $1 \leq n < 2\alpha_{\mathcal{W}}$, then it follows from (7.2) that $D(s, \chi)$ has a pole of exact order $d_n(\chi)$, unless $\psi(1/n, \chi) = 0$, in which case the pole might be of lower order. We note that each Euler factor $D_p(1/n, \mathbf{1})$ is non-zero because it is a finite sum of positive terms. Hence Proposition 7.2 implies that $\psi(1/n, \mathbf{1}) \neq 0$, and so $D(s, \mathbf{1})$ has a pole of order exactly $d_n(\mathbf{1})$, as claimed. This proves parts (a) and (b).

Part (c) follows immediately from (4.4). \square

Lemma 7.5. *For any positive integer n with $1 \leq n \leq 2\alpha_{\mathcal{W}}$, the number*

$$\lim_{s \rightarrow \frac{1}{n}} \left(s - \frac{1}{n} \right)^{d_n} D_{\mathbf{c}, \mathcal{M}}(s)$$

is independent of \mathbf{c} if and only if $b_n(\chi) = 0$ for all $\chi \neq \mathbf{1}$.

Proof. This follows directly from Proposition 7.4(c), via linear independence of characters. \square

We can now state a necessary and sufficient condition for $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ to be asymptotically independent of \mathbf{c} .

Proposition 7.6. *We have that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} if and only if $b_{\alpha_{\mathcal{W}}}(\chi) = 0$ for all $\chi \neq \mathbf{1}$.*

Proof. This follows directly from Lemma 7.5 and Definition 5.3. We first note that Proposition 7.4(a) implies that $b_{\alpha_{\mathcal{W}}}(\mathbf{1})$ is always strictly greater than zero. If $b_{\alpha_{\mathcal{W}}}(\chi) = 0$ for all $\chi \neq \mathbf{1}$, then it is easy to see that the numbers $\tau(\mathbf{c}; \mathcal{M})$, $a(\mathbf{c}; \mathcal{M})$ and $\delta(\mathbf{c}; \mathcal{M})$ are independent of \mathbf{c} , which in turn implies that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is independent of \mathbf{c} also.

On the other hand, if $b_{\alpha_{\mathcal{W}}}(\chi) \neq 0$ for some $\chi \neq \mathbf{1}$, then Proposition 7.4(c) implies (via linear independence of characters) that $\tau(\mathbf{c}; \mathcal{M})$ is not independent of \mathbf{c} , and so we deduce that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ cannot be independent of \mathbf{c} either. \square

Corollary 7.7. *(a) If $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} , then for each $\mathbf{c} \in \text{Cl}'_{\mathcal{M}}(\Lambda)$ we have that $a(\mathbf{c}; \mathcal{M}) = 1/\alpha_{\mathcal{W}}$. Also, $D_{\mathbf{c}, \mathcal{M}}(s)$ has a pole of exact order $d_{\mathcal{W}}$ at $s = 1/\alpha_{\mathcal{W}}$, and*

$$\lim_{s \rightarrow \frac{1}{\alpha_{\mathcal{W}}}} \left(s - \frac{1}{\alpha_{\mathcal{W}}} \right) D_{\mathbf{c}, \mathcal{M}}(s) = b_{\alpha_{\mathcal{W}}}(\mathbf{1}).$$

(b) If \mathcal{W} is constant on T' , then $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} , and $d_{\mathcal{W}} = |T'|$.

Proof. This follows readily from the definitions. \square

8. AN EQUIDISTRIBUTION RESULT

Let $c \in \mathcal{R}(O_K G)$ be a realisable class. In this section we shall discuss the number $N_{\mathcal{W}}(c, X; \mathcal{M})$ of tame Galois G -extensions K_h/K for which $(O_h) = c$, $(D_{\mathcal{W}}(K_h/K), \mathcal{M}) = 1$ and $D_{\mathcal{W}}(K_h/K) \leq X$ under the assumption that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} .

Suppose therefore that $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} . Recall (see Definition 3.1) that we have a homomorphism

$$\psi : H_{tr}^1(K, G) \rightarrow \mathcal{C}(O_K G)$$

with finite kernel, and a surjective homomorphism (see Proposition 3.9)

$$f_{\mathcal{M}} : \text{Cl}'_{\mathcal{M}}(\Lambda) \rightarrow \frac{J(K\Lambda)}{\mathcal{P}_{\theta}}.$$

Theorem 8.1. *With the above hypotheses and notation, we have*

$$N_{\mathcal{W}}(c, X; \mathcal{M}) \sim \frac{\alpha_{\mathcal{W}} \cdot |\text{Ker}(\psi)| \cdot |\text{Ker}(f_{\mathcal{M}})| \cdot b_{\alpha_{\mathcal{W}}}(\mathbf{1})}{\Gamma(d_{\mathcal{W}}(\mathbf{1}))} \cdot X^{\frac{1}{\alpha_{\mathcal{W}}}} \cdot (\log X)^{d_{\mathcal{W}}(\mathbf{1})-1}$$

as $X \rightarrow \infty$.

Proof. This follows directly from (3.6), Proposition 5.2 and Corollary 7.7. \square

We thus see that if $\kappa_{\mathcal{W}}(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} , then the tame Galois G -extensions K_h of K with $D_{\mathcal{W}}(K_h/K)$ coprime to \mathcal{M} are equidistributed amongst the realisable classes in $\text{Cl}(O_K G)$ as $X \rightarrow \infty$.

Example 8.2. Let us now consider the case treated by K. Foster in [3]. Let l be a prime, and suppose that G is an elementary abelian l -group of order l^k . Suppose also that $\mathcal{W} = \mathcal{W}_{\text{disc}}$ (see Example 3.15(1)). For each $t \in T'$, we have

$$\mathcal{W}(t) = \frac{(|t| - 1)|G|}{|t|} = \frac{(l - 1)l^k}{l} = l^{k-1}(l - 1) = \phi(|G|),$$

where ϕ denotes the Euler ϕ -function. Hence \mathcal{W} is constant on T' , and so Corollary 7.7(b) implies that $\kappa(\mathbf{c}, X; \mathcal{M})$ is asymptotically independent of \mathbf{c} . If we take

$$\mathcal{M} = |G|^2 \Lambda = l^2 \Lambda,$$

then for each $c \in \mathcal{R}(O_K G)$, we have $N_{\mathcal{W}}(c, X; \mathcal{M}) = N_{\text{disc}}(c, X; \mathcal{M})$ because, since G is an l -group, a G -extension K_h/K is tamely ramified if and only if it is unramified at all primes dividing l .

We have that $\alpha_{\mathcal{W}} = 1/|\phi(G)|$, and $d_{\mathcal{W}}(\mathbf{1}) = |T'|$. Theorem 8.1 and Corollary 7.7 therefore imply that

$$N_{\mathcal{W}}(c, X) \sim \frac{\phi(|G|) \cdot |\text{Ker}(f_{\mathcal{M}})| \cdot b_{\alpha_{\mathcal{W}}}(\mathbf{1})}{\Gamma(|T'|)} \cdot X^{1/\phi(|G|)} \cdot (\log(X))^{|T'|-1}. \quad (8.1)$$

The tower law for discriminants implies that for each tamely ramified G -extension K_h/K we have

$$\text{disc}(K_h/\mathbf{Q}) = D_{\mathcal{W}}(K_h/K) \text{disc}(K/\mathbf{Q})^{|G|}$$

and this in turn implies that

$$N_{\text{disc}}(c, X) = N_{\mathcal{W}}(c, X / \text{disc}(K/\mathbf{Q})^{|G|}). \quad (8.2)$$

From (8.1) and (8.2), we have

$$\begin{aligned} N_{\mathcal{W}}(c, X) &\sim \frac{\phi(|G|) \cdot |\text{Ker}(f_{\mathcal{M}})| \cdot b_{\alpha_{\mathcal{W}}}(\mathbf{1})}{\Gamma(|T'|)} \cdot \left(\frac{X}{\text{disc}(K/\mathbf{Q})^{|G|}} \right)^{1/\phi(|G|)} \cdot \log \left(\frac{X}{\text{disc}(K/\mathbf{Q})^{|G|}} \right)^{|T'|-1} \\ &= \frac{|\text{Ker}(f_{\mathcal{M}})| \cdot b_{\alpha_{\mathcal{W}}}(\mathbf{1})}{\Gamma(|T'|)} \cdot Y \cdot \log(Y)^{|T'|-1}, \end{aligned}$$

where $Y^{\phi(|G|)} \cdot \text{disc}(K/\mathbf{Q})^{|G|} = X$.

Theorem A of the Introduction now follows immediately. \square

Example 8.3. Suppose now that G is any finite abelian group. Let $\mathcal{W} = \mathcal{W}_{\text{ram}}$ (see Example 3.15(2)), and set $\mathcal{M} = |G|^2\Lambda$. Then, for each $c \in \mathcal{R}(O_K G)$, it follows from the definitions that $N_{\mathcal{D}}(c, X)$ (see Theorem A of the Introduction) is equal to $N_{\mathcal{W}}(c, X; \mathcal{M})$.

As \mathcal{W} is constant on T' , Corollary 7.7(b) implies that $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$ is asymptotically independent of \mathfrak{c} . It is not hard to check that $\alpha_{\mathcal{W}} = 1$ and $d_{\mathcal{W}}(\mathbf{1}) = |T'|$. Theorem 8.1 now implies that

$$N_{\mathcal{W}}(c, X; \mathcal{M}) \sim \frac{|\text{Ker}(\psi)| \cdot |\text{Ker}(f_{\mathcal{M}})| \cdot b_{\alpha_{\mathcal{W}}}(\mathbf{1})}{\Gamma(|T'|)} \cdot X \cdot (\log X)^{|T'|-1}.$$

This implies Theorem B of the Introduction. \square

Remark 8.4. Theorem 8.1 implies that if $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$ is asymptotically independent of \mathfrak{c} , then the second part of Question 3.17 has an affirmative answer, i.e. the limit

$$Z_{\mathcal{W}}(c; \mathcal{M}) := \lim_{X \rightarrow \infty} \frac{N_{\mathcal{W}}(c, X; \mathcal{M})}{M_{\mathcal{W}}(X)}$$

is independent of $c \in \mathcal{R}(O_K G)$. What happens if the assumption that $\kappa_{\mathcal{W}}(\mathfrak{c}, X; \mathcal{M})$ is asymptotically independent of \mathfrak{c} is dropped? In this case, (3.6) strongly suggests that it is probably no longer true in general that $Z_{\mathcal{W}}(c; \mathcal{M})$ is independent of c ; one would expect the behaviour of $Z_{\mathcal{W}}(c; \mathcal{M})$ with respect to c to depend very much upon the choice of \mathcal{W} . At present we have no results or examples in this situation. It might be possible to use the methods of this paper to produce examples in the setting of function fields; we hope to treat this topic in a future paper. \square

REFERENCES

- [1] A. Agboola, D. Burns, *On the Galois structure of equivariant line bundles on curves*, American J. Math. **120** (1998), 1121–1163.
- [2] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press (1986).

- [3] K. Foster, *An equal-distribution result for Galois module structure*, Ph.D. Thesis, University of Illinois at Urbana-Champaign (1987).
- [4] B. Köck, *Operations on locally free classgroups*, Math. Ann. **314** (1999), 667–702.
- [5] B. Köck, *Symmetric powers of Galois modules on Dedekind schemes*, Comp. Math. **124** (2000), 195–217.
- [6] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.
- [7] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle **375/376** (1987), 259-306.
- [8] W. Narkiewicz, *Number theory*, World Scientific (1983).
- [9] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, preprint (2008).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CA 93106.

E-mail address: `agboola@math.ucsb.edu`