Division points in arithmetic

Javan Peykar, A.

CHAPTER 2

Reductions of multiplicative subgroups of number fields

1. Introduction

Let K be a number field, and let W be a finitely generated subgroup of K^*. Let $\mathcal{O}_K$ be the ring of integers of K. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\mathrm{v}_\mathfrak{p}\colon K \longrightarrow \mathbf{Z} \cup \{\infty\}$ be the $\mathfrak{p}$-adic valuation function, let $\mathcal{O}_{K,\mathfrak{p}}$ be the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, and let $\kappa(\mathfrak{p})$ be the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$. Let Ω_K be the set of maximal ideals of $\mathcal{O}_K$, let

$$S = \{\mathfrak{p} \in \Omega_K : \text{ there is } w \in W \text{ such that } \mathrm{v}_\mathfrak{p}(w) \neq 0\},$$

and note that S is finite. Then for $\mathfrak{p} \in \Omega_K \setminus S$ we have $W \subset \mathcal{O}_{K,\mathfrak{p}}^*$. Thus, the canonical ring morphism $\mathcal{O}_{K,\mathfrak{p}} \longrightarrow \kappa(\mathfrak{p})$ induces a group morphism $\pi_\mathfrak{p}\colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Let V be a subgroup of W such that W/V is finite cyclic. Note that for any $\mathfrak{p} \in \Omega_K \setminus S$ the kernel of $\pi_\mathfrak{p}$ is such a subgroup of W. Let

$$A(W,V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_\mathfrak{p}) \subset V\}.$$

For any subset N of Ω_K we write $\mathrm{d}(N)$ for its natural density, if it exists. In this chapter we show that the set $A(W,V)$ has a natural density $\mathrm{d}(A(W,V))$ in Ω_K, and prove properties of this density of both qualitative and quantitative nature.

Theorem 6 (Main theorem)**.**

(a) *The set $A(W,V)$ has a natural density $\mathrm{d}(A(W,V))$ in Ω_K.*

(b) *The density $\mathrm{d}(A(W,V))$ is rational.*

(c) *As a function of K, W and V, the density $\mathrm{d}(A(W,V))$ is computable.*

(d) *Let V' be a subgroup of W containing V, and suppose that W is infinite. Then $\mathrm{d}(A(W,V)) = \mathrm{d}(A(W,V'))$ if and only if $V = V'$.*

(e) *The density $\mathrm{d}(A(W,V))$ is positive.*

(f) *We have $\mathrm{d}(A(W,V)) = 1$ if and only if $V = W$ or W is finite.*

See Theorem 2.24 and Theorem 2.25 in Section 2.7 for the proof.

Suppose x and y are positive integers with the property that for all positive integers n the set of prime numbers dividing $x^n - 1$ is equal to the set of prime numbers dividing $y^n - 1$. Pál Erdös asked, at the 1988 number theory conference in Banff, whether it follows that x is equal to y. This question was labeled the *support problem*, and was answered affirmatively by C. Corrales-Rodrigáñez and R. Schoof in [CRS97], who, in the same paper, formulated and proved an elliptic analogue of the support problem. One can find many generalisations and variations of the support problem in the literature, see [Kha03, Proposition 3], [BGK05], [Lar02], [Wes03], [Bar10], [Per09], [Per12]. As an application of Theorem 6(e), we give an alternative solution to the following two generalisations of the support problem.

Throughout this chapter, we use the phrase *almost all* as a substitute for *all but finitely many*.

Theorem 7. *Let K be a number field, and let X and Y be finitely generated subgroups of K^*.*

(a) *Let $S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X \cup Y : \mathrm{v}_\mathfrak{p}(x) \neq 0\}$. Then $Y \subset X$ if and only if for almost all $\mathfrak{p} \in \Omega_K \setminus S'$ we have $Y \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}}$.*

(b) *Suppose that $Y \subset X$. Let l be a prime number. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X : \mathrm{v}_\mathfrak{p}(x) \neq 0\}.$$

Then

$$(X : Y) < \infty \text{ and } l \nmid (X : Y)$$

if and only if

$$\text{for almost all } \mathfrak{p} \in \Omega_K \setminus S' \text{ we have } l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}}).$$

See Theorem 2.27 and Theorem 2.28 in Section 2.8 for the proof.

Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a subgroup of W such that W/V is finite cyclic. The existence of the natural density of $A(W, V)$ is obtained by a version of Chebotarev's density theorem for infinite algebraic extensions of a number field. Using this theorem, we also obtain a formula for $\mathrm{d}(A(W, V))$ that is, however, a finite product of infinite sums. In order to obtain a closed-form formula for $\mathrm{d}(A(W, V))$ we investigate the radical extensions of K occurring in this formula. We refer to Section 2.3 for the infinite version of Chebotarev's density theorem and to Section 2.4 for the proof of the existence and formula of $\mathrm{d}(A(W, V))$.

Let s be a Steinitz number, that is, let $s = \prod_p p^{e(p)}$, where p runs over all prime numbers and $e(p) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$. Let $\overline{K}$ be an algebraic closure of K and define

$$W^{1/s} = \{x \in \overline{K}^* : \exists d \in \mathbf{Z}_{\geq 1} : d | s \text{ and } x^d \in W\}.$$

The field $K(W^{1/s})$ is Galois over K and any field automorphism of $K(W^{1/s})$ over K is determined by its action on $W^{1/s}$, that is, we can identify $\mathrm{Gal}(K(W^{1/s})/K)$ with a subgroup of the group $\mathrm{Aut}_W(W^{1/s})$ of automorphisms of $W^{1/s}$ that are the identity on W. By abuse of notation we denote this subgroup also by $\mathrm{Gal}(K(W^{1/s})/K)$. We remark that $\mathrm{Aut}_W(W^{1/s})$ is the profinite group

$$\varprojlim_d \mathrm{Aut}_W(W^{1/d})$$

where d runs over all positive integers dividing s. As $\mathrm{Gal}(K(W^{1/s})/K)$ is compact and $\mathrm{Aut}_W(W^{1/s})$ is Hausdorff, the subgroup $\mathrm{Gal}(K(W^{1/s})/K)$ of $\mathrm{Aut}_W(W^{1/s})$ is closed.

For a prime p let v_p be the p-adic valuation function. Moreover, for a group G write $\exp(G)$ for its exponent.

Theorem 8. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let s be a Steinitz number.*

(a) *Then $\mathrm{Gal}(K(W^{1/s})/K)$ is an open subgroup of $\mathrm{Aut}_W(W^{1/s})$.*

(b) *Suppose that $s = p^\infty$, where p is prime. Let*

$$F = \begin{cases} K(\mu_4) & \text{if } p = 2, \\ K(\mu_p) & \text{otherwise.} \end{cases}$$

Then $\exp((W^{1/s} \cap F^*)/W)$ is an integer, and moreover, for

$$j = \mathrm{v}_p(\exp((W^{1/s} \cap F^*)/W))$$

and for all $i \in \mathbf{Z}_{\geq j}$ we have

$$\mathrm{Aut}_{W^{1/p^i}}(W^{1/s}) \subset \mathrm{Gal}(K(W^{1/s})/K).$$

See Section 2.5 for the proof of this theorem.

By using elementary group theory, we are able to calculate the order of an automorphism group of the form $\mathrm{Aut}_{W^{1/x'}}(W^{1/x})$, where W is as in the theorem above, $x', x \in \mathbf{Z}_{\geq 1}$ and x' divides x. As a result, we obtain the following closed-form expression for the density $\mathrm{d}(A(W,V))$.

Theorem 9. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a subgroup of W such that W/V is finite cyclic. Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Let $n = \mathrm{rk}(W)$ (see* Definition 1.2*), and let $\mathcal{P}$ be the set of prime divisors of m. Let $(j_p)_{p\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \prod_{p\in\mathcal{P}} \Big[\tfrac{1}{[L(U^{1/p^{j_p}}):L]} \cdot \tfrac{p^n(p-1)}{p^{n+1}-1} + \textstyle\sum_{i=0}^{j_p-1} \Big(\tfrac{1}{[L(U^{1/p^i}):L]} - \tfrac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \Big) \Big].$$

For the sake of showcasing, we remark that in certain cases the above lengthy formula breaks down to a rather simple formula, presented by the following corollary.

Corollary. *Suppose that for every $p \in \mathcal{P}$ we have*

$$\mathrm{Gal}(L(U^{1/p^\infty})/L) = \mathrm{Aut}_U(U^{1/p^\infty}).$$

Then

$$\mathrm{d}(A(W,V)) = \frac{1}{[L:K]} \prod_{p\in\mathcal{P}} \frac{p^n(p-1)}{p^{n+1}-1}.$$

In addition, suppose that $[L:K] = \phi(m)m^{n-1}$, where ϕ is Euler's totient function. Then we have

$$\mathrm{d}(A(W,V)) = \frac{1}{m^n} \cdot \prod_{p\in\mathcal{P}} \frac{p^{n+1}}{p^{n+1}-1}.$$

See Section 2.6 for the proof of Theorem 9 and its corollary.

At last, using the closed-form formula given in Theorem 9, we are able to make the following quantitative observations about $\mathrm{d}(A(W,V))$.

Theorem 10. *Let K, W, V, m, U, L, n, $\mathcal{P}$, and $(j_p)_{p\in\mathcal{P}}$ be as in* Theorem 9. *Then the density $\mathrm{d}(A(W,V))$ exists and equals a positive rational number in the interval*

$$\left[\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)},\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right)\right]$$

whose denominator divides $m^n\cdot\prod_{p\in\mathcal{P}}\big(p^{(n+1)j_p-1}\cdot(p^{n+1}-1)\big)$.

See Section 2.7 for the proof of this theorem.

The present chapter is organised as follows.

In Section 2.2 we recall the necessary definitions and lemmas of measure theory. In Section 2.3 we state the infinite version of Chebotarev's density theorem. In Section 2.4 we prove the existence of the density of Theorem 6 and give a formula for it. In Section 2.5 we prove Theorem 8, and in Section 2.6 we prove Theorem 9. In Section 2.7 we prove Theorem 10 and the remaining parts of Theorem 6. At last, Section 2.8 contains the proof of Theorem 7.

2. Haar measure on profinite groups

In this section we briefly recall the theory of Haar measures on profinite groups. For a more elaborate treatment of the subject see [HR79], [FJ08] or [RV99].

Definition 2.1. Let X be a set, and let Σ be a σ-algebra over X. A *measure* on Σ is a function $\lambda\colon\Sigma\longrightarrow\mathbf{R}\cup\{\infty\}$ that satisfies:

(a) For all $E \in \Sigma$ we have $\lambda(E) \geq 0$;

(b) We have $\lambda(\emptyset) = 0$;

(c) For all countable collections $\{E_i\}_{i \in I}$ of pairwise disjoint sets in Σ we have

$$\lambda\left(\coprod_{i \in I} E_i\right) = \sum_{i \in I} \lambda(E_i).$$

Proposition 2.2. *Let X be a set, let Σ be a σ-algebra on X, and let λ be a measure on Σ. Then the following statements hold.*

(a) *For $E_1, E_2 \in \Sigma$ with $E_1 \subset E_2$, we have $\lambda(E_1) \leq \lambda(E_2)$.*

(b) *For $E_1, E_2 \in \Sigma$ with $E_2 \subset E_1$ and $\lambda(E_2) < \infty$, we have $\lambda(E_1 \setminus E_2) = \lambda(E_1) - \lambda(E_2)$.*

(c) *For any countable collection $\{E_i\}_{i \in I}$ of sets in Σ we have*

$$\lambda\left(\bigcup_{i \in I} E_i\right) \leq \sum_{i \in I} \lambda(E_i).$$

Proof. See [Bau01, §1.3]. ∎

Let G be a profinite group. The σ-algebra $\mathcal{B}(G)$ generated by all open sets of G is called the *Borel algebra* of G. An element of $\mathcal{B}(G)$ is called a *Borel set* of G.

Theorem 2.3. *Let G be a profinite group. Then there is a unique measure λ on $\mathcal{B}(G)$ satisfying:*

(a) *For every $g \in G$ and $E \in \mathcal{B}(G)$ we have $\lambda(gE) = \lambda(E)$;*

(b) $\lambda(G) = 1$.

Proof. See [FJ08, Theorem 18.2.1]. ∎

Definition 2.4. Let G be a profinite group. We call the unique measure on $\mathcal{B}(G)$ of Theorem 2.3 the *Haar measure* on G and denote it by λ_G, or just λ when the group G is understood. Elements of $\mathcal{B}(G)$ are called *measurable under the Haar measure* or *Haar measurable*.

Lemma 2.5. *Let G be a profinite group. Then the following statements hold.*

(a) *Let $H \subset G$ be a Haar measurable subgroup of finite index. Then*

$$\lambda(H) = 1/[G : H].$$

(b) *Let $H \subset G$ be a Haar measurable subgroup that is not of finite index in G. Then $\lambda(H) = 0$.*

Proof. See [FJ08, §18.1]. ∎

Lemma 2.6. *Let $\pi\colon G \longrightarrow H$ be a surjective morphism of profinite groups. Then for each $E \in \mathcal{B}(H)$ we have $\pi^{-1}(E) \in \mathcal{B}(G)$ and $\lambda_H(E) = \lambda_G(\pi^{-1}(E))$.*

Proof. See [FJ08, Proposition 18.2.2]. ∎

Lemma 2.7. *Let $n \in \mathbf{Z}_{\geq 1}$. Let $G_1, \ldots, G_n$ be profinite groups with Haar measures $\lambda_1, \ldots, \lambda_n$, respectively. Let $G = \prod_{i=1}^n G_i$. For $i = 1, \ldots, n$ let $E_i \in \mathcal{B}(G_i)$. Then $\lambda_G(E_1 \times \cdots \times E_n) = \lambda_1(E_1) \cdots \lambda_n(E_n)$.*

Proof. See [FJ08, Proposition 18.4.2]. ∎

3. Chebotarev density theorem for infinite extensions

In this section we briefly recall the theory of infinite Galois extensions of number fields to state the Chebotarev density theorem for an infinite Galois extension of a number field. For details and proofs we refer to [Ser89] or [Neu99].

Let K be an algebraic extension of $\mathbf{Q}$. We denote the set of maximal ideals of $\mathcal{O}_K$ by Ω_K. For $\mathfrak{p} \in \Omega_K$ we denote the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$ by $\kappa(\mathfrak{p})$. Now, suppose K is a number field, and let L be an infinite Galois extension of K with Galois group G. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ a maximal ideal of $\mathcal{O}_L$ extending $\mathfrak{p}$, that is, $\mathfrak{q} \cap K = \mathfrak{p}$. Then the *decomposition group*

$$\mathrm{D}(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

of $\mathfrak{q}$ over $\mathfrak{p}$ is a closed subgroup of G. There is a canonical morphism of topological groups

$$r\colon\ \mathrm{D}(\mathfrak{q}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})),$$

which is surjective. The kernel of r, called the *inertia group* $\mathrm{I}(\mathfrak{q}/\mathfrak{p})$ of $\mathfrak{q}$ over $\mathfrak{p}$, is trivial if and only if $\mathfrak{p}$ is unramified in L.

Suppose that $\mathfrak{p}$ is unramified. Then r is an isomorphism of topological groups. Note that $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ is topologically generated by the Frobenius morphism

$$\mathrm{Frob}_{\mathfrak{p}}\colon \kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q})$$

sending $x \in \kappa(\mathfrak{q})$ to $x^{\#\kappa(\mathfrak{p})}$. We denote the inverse image of $\mathrm{Frob}_{\mathfrak{p}}$ under r by $\mathrm{Frob}(\mathfrak{q}/\mathfrak{p})$ and call it the *Frobenius element* of $\mathfrak{q}$ over $\mathfrak{p}$ in G. The Frobenius elements of the different maximal ideals extending $\mathfrak{p}$ form a conjugacy class in G. We write $(\mathfrak{p}, L/K)$ for the conjugacy class consisting of the Frobenius elements $\mathrm{Frob}(\mathfrak{q}/\mathfrak{p})$ where $\mathfrak{q}$ runs over all primes of L extending $\mathfrak{p}$.

Let C be a subset of G. Let $\overline{C}$ be the closure of C in G, and let C^{o} be the interior of C in G. Then the boundary ∂C of C is equal to $\overline{C} \setminus C^{\mathrm{o}}$. Equivalently, we have $\partial C = \overline{C} \cap \overline{G \setminus C}$.

Let P be a subset of Ω_K. Recall that the natural density $\mathrm{d}(P)$ of P in Ω_K is equal to

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in P : \#\kappa(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \Omega_K : \#\kappa(\mathfrak{p}) \leq x\}}.$$

We have the following version of the Chebotarev density theorem that can also handle infinite Galois extensions of number fields.

Theorem 2.8. *Let K be a number field, and let L be a Galois extension of K that is unramified outside a finite set of primes S of K. Let C be a Haar measurable subset of $\mathrm{Gal}(L/K)$ that is closed under conjugation. Assume that the boundary ∂C has Haar measure 0. Then the set*

$$\{\mathfrak{p} \in \Omega_K \setminus S : (\mathfrak{p}, L/K) \subset C\}$$

has a natural density in Ω_K that is equal to $\lambda(C)$.

Proof. See [Ser89, Corollary 2, page I-9]. ∎

4. Existence of the density

Definition 2.9. Let W be a group, and let V be a subgroup of W. Then V is called *cofinite* if V is of finite index in W. Moreover V is called *cocyclic* if W/V is a cyclic group.

Let K be a field, and let $\overline{K}$ be an algebraic closure of K. Let W be a subgroup of K^*, and let s be a Steinitz number not divisible by $\mathrm{char}\, K$. Define

$$W^{1/s} = \{x \in \overline{K}^* : \exists n \in \mathbf{Z}_{\geq 1} : n \mid s \text{ and } x^n \in W\}.$$

Observe that $W^{1/s} = \bigcup_n W^{1/n}$, where n runs over all positive integers dividing s. As usual, we write μ_s for the group of s-th roots of unity $\{1\}^{1/s}$.

Now, let K be a number field, and for $\mathfrak{p} \in \Omega_K$ let $\mathrm{v}_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation function. Let W be a finitely generated subgroup of K^*, and let

$$S = \{\mathfrak{p} \in \Omega_K : \exists w \in W : \mathrm{v}_\mathfrak{p}(w) \neq 0\},$$

and remark that S is finite. For every $\mathfrak{p} \in \Omega_K \setminus S$ the canonical projection $\mathcal{O}_K \longrightarrow \kappa(\mathfrak{p})$ induces a group morphism $\pi_\mathfrak{p} \colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Let V be a cocyclic cofinite subgroup of W of index m, and write $\mathcal{P}(m)$ for the set of prime divisors of m. Moreover, let

$$A(W,V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_\mathfrak{p}) \subset V\}.$$

To ease notation we will write $\mathcal{P}$ for $\mathcal{P}(m)$ and A for $A(W,V)$ throughout this section.

In this section we prove the following theorem.

Theorem 2.10. *Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Then A has a natural density, which equals*

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right).$$

Lemma 2.11. *Let W be a group, and let V be a cofinite subgroup of W. Let*

$$\pi \colon W \longrightarrow W'$$

be a group morphism. Then $\ker \pi \subset V$ if and only if $(W : V) = (\pi(W) : \pi(V))$.

Proof. Let $N = \ker \pi$. Observe that $\pi(V) = \pi(VN)$, so that

$$\pi(W)/\pi(V) \cong (W/N)/(VN/N) \cong W/VN$$

as sets. Hence, we have $(\pi(W) : \pi(V)) = (W : VN)$. It follows that

$$(\pi(W) : \pi(V)) = (W : V)$$

if and only if $V = VN$. This is equivalent to V containing N. ∎

Throughout the rest of this section let K, W, V, A, m, $\mathcal{P}$, U, and L be as in Theorem 2.10.

Let $\varphi \colon \Omega_L \longrightarrow \Omega_K$ be given by $\mathfrak{q} \mapsto \mathfrak{q} \cap K$, and let

$$S' = \varphi^{-1}(S) \cup \{\mathfrak{q} \in \Omega_L : m \in \mathfrak{q}\}.$$

Then for every $\mathfrak{q} \in \Omega_L \setminus S'$ we have the reduction map $\pi_\mathfrak{q} \colon U \longrightarrow \kappa(\mathfrak{q})^*$, where $\kappa(\mathfrak{q})$ is the residue field of L at $\mathfrak{q}$. Then we let $A' = A'(W, V) = \{\mathfrak{q} \in \Omega_L \setminus S' : \ker(\pi_\mathfrak{q}|_W) \subset V\}$.

Lemma 2.12. *Suppose that* $\mathrm{d}(A')$ *exists. Then* $\mathrm{d}(A)$ *exists and we have*

$$\mathrm{d}(A) = \frac{1}{[L:K]}\,\mathrm{d}(A').$$

Proof. First, note that for all $\mathfrak{q} \in \Omega_L \setminus S'$ we have $\pi_\mathfrak{q}(W) = \pi_{\varphi(\mathfrak{q})}(W)$, so that

$$\ker(\pi_\mathfrak{q}|_W) = \ker(\pi_{\varphi(\mathfrak{q})}|_W).$$

On the other hand, for $\mathfrak{p} \in A$ and $\mathfrak{q} \in \Omega_L \setminus S'$ dividing $\mathfrak{p}$, we have $\mathfrak{q} \in A'$. It follows that for all $\mathfrak{p} \in \Omega_K \setminus S$ and $\mathfrak{q} \in \Omega_L \setminus S'$ dividing $\mathfrak{p}$, we have $\mathfrak{p} \in A$ if and only if $\mathfrak{q} \in A'$.

Now, let $\mathfrak{p} \in A$, and let $\mathfrak{q} \in \Omega_L \setminus S'$ be a prime dividing $\mathfrak{p}$. Then by Lemma 2.11 we have $(\pi_\mathfrak{p}(W) : \pi_\mathfrak{p}(V)) = m$, which implies that m divides $\#\kappa(\mathfrak{p})^*$ and

$$\pi_\mathfrak{p}(V) \subset \kappa(\mathfrak{p})^{*m}.$$

It follows that $\mathfrak{p}$ splits completely in $K(V^{1/m}) = L$. Thus, for $x \in \mathbf{R}_{\geq 1}$ we have

$$\#\{\mathfrak{q} \in \Omega_L : \mathfrak{q} \in A' \wedge \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\} = [L:K]\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \wedge \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}.$$

Hence we have

$$\begin{aligned}
\mathrm{d}(A') &= \lim_{x\to\infty} \frac{\#\{\mathfrak{q} \in \Omega_L : \mathfrak{q} \in A' \text{ and } \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}} \\
&= \lim_{x\to\infty} \frac{[L:K]\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}} \\
&= [L:K] \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}.
\end{aligned}$$

As

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}{\#\{\mathfrak{p} \in \Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}} = 1,$$

we have

$$\begin{aligned} \mathrm{d}(A') &= [L:K] \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}} \\ &= [L:K] \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}} \\ &= [L:K]\, \mathrm{d}(A). \end{aligned}$$

It follows that $\mathrm{d}(A)$ exists and that $\mathrm{d}(A) = \frac{1}{[L:K]}\, \mathrm{d}(A')$. ∎

Lemma 2.13. *We have* $A' = \{\mathfrak{q} \in \Omega_L \setminus S' : \pi_{\mathfrak{q}}(W) = \pi_{\mathfrak{q}}(U)\}$.

Proof. Let $\mathfrak{q} \in \Omega_L \setminus S'$. Observe that $V = U^m$, and that $(\pi_{\mathfrak{q}}(U) : \pi_{\mathfrak{q}}(U^m))$ divides m, since $\kappa(\mathfrak{q})^*$ is cyclic. Moreover, as $U = V^{1/m}$ contains a primitive mth root of unity, it follows that m divides $\#\pi_{\mathfrak{q}}(U)$ and $(\pi_{\mathfrak{q}}(U) : \pi_{\mathfrak{q}}(V)) = m$. It follows that $\pi_{\mathfrak{q}}(U) = \pi_{\mathfrak{q}}(W)$ if and only if $(\pi_{\mathfrak{q}}(W) : \pi_{\mathfrak{q}}(V)) = m$. On the other hand, we have by Lemma 2.11 that $(\pi_{\mathfrak{q}}(W) : \pi_{\mathfrak{q}}(V)) = m$ if and only if $\ker(\pi_{\mathfrak{q}}|_W) \subset V$. ∎

Let $m^\infty = \prod_{p\in\mathcal{P}} p^\infty$. Let $\overline{L}$ be an algebraic closure of L, and write G for its Galois group over L. Since $W \subset U$, we have for every $p \in \mathcal{P}$ the following tower

$$\begin{aligned} L \subset L(W^{1/p}) \subset L(U^{1/p}) \subset L(U^{1/p}, W^{1/p^2}) \subset \cdots \\ \cdots \subset L(U^{1/p^i}) \subset L(U^{1/p^i}, W^{1/p^{i+1}}) \subset L(U^{1/p^{i+1}}) \subset L(U^{1/p^{i+1}}, W^{1/p^{i+2}}) \subset \cdots \\ \cdots \subset L(U^{1/p^\infty}) \subset L(U^{1/m^\infty}) \subset \overline{L} \end{aligned}$$

of Galois extensions of L.

For all $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$ let

$$G_{p,i} = \mathrm{Gal}(\overline{L}/L(U^{1/p^i})),$$

and for $i \in \mathbf{Z}_{\geq 0}$, let

$$H_{p,i} = \mathrm{Gal}(\overline{L}/L(U^{1/p^i}, W^{1/p^{i+1}})) \subset G_{p,i}.$$

Note that for all $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ we have

$$G_{p,\infty} \subset \cdots \subset G_{p,i+1} \subset H_{p,i} \subset G_{p,i} \subset \cdots \subset G_{p,0}$$

by the above. Moreover, define

$$C_{p,i} = G_{p,i} \setminus H_{p,i},$$

and

$$C_p = \bigcup_{i=0}^{\infty} C_{p,i}.$$

One easily sees that C_p is a disjoint union of sets $C_{p,i}$. At last, we define $C = \bigcap_{p \in \mathcal{P}} C_p$.

Lemma 2.14. *The subset C of G is closed under conjugation and open in G.*

Proof. As for all $p \in \mathcal{P}$ and for all $i \in \mathbf{Z}_{\geq 0}$, the sets $G_{p,i}$ and $H_{p,i}$ are normal subgroups of G of finite index, it follows that $C_{p,i} = G_{p,i} \setminus H_{p,i}$ is closed under conjugation and open in G. Thus $C = \bigcap_{p \in \mathcal{P}} C_p$ is closed under conjugation and open in G. ∎

Lemma 2.15. *The boundary ∂C of C in G satisfies $\lambda(\partial C) = 0$, where λ is the Haar measure on G (see 2.4).*

Proof. For $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ let

$$D_{p,i} = H_{p,i} \setminus G_{p,i+1}.$$

Then observe that $G \setminus C$ contains the open set

$$D = \bigcup_{p,i} D_{p,i}$$

of G, where p runs over $\mathcal{P}$ and i runs over $\mathbf{Z}_{\geq 0}$. Hence $\partial C \subset G \setminus (C \cup D)$.

Now, for $\sigma \in G$ let N_σ be the Steinitz number $\prod_{p \in \mathcal{P}} p^{\sigma_p}$ with $\sigma_p \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$ the largest element such that $\sigma \in G_{p,i}$, where we order $\mathbf{Z}_{\geq 0} \cup \{\infty\}$ in the natural way, that is $\sigma_p = \sup\{i : \sigma \in G_{p,i}\}$.

Let $\sigma \in G$ and suppose that N_σ is an integer. This implies that for every $p \in \mathcal{P}$ there exists $i \in \mathbf{Z}_{\geq 0}$ such that $\sigma \in G_{p,i} \setminus G_{p,i+1}$. Then one easily sees that either $\sigma \in C$ or $\sigma \in D$. Thus $\sigma \in \partial C$ implies that N_σ is an infinite Steinitz number. As there are only finitely many primes dividing m, it follows that $\partial C \subset \bigcup_{p \in \mathcal{P}} \mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$. Since the field $L(U^{1/p^\infty})$ contains the infinite extension $L(\mu_{p^\infty})$ of L, the former is also infinite over L. Therefore, the group $\mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$ is of infinite index in G. Then by Lemma 2.5(b) the Haar measure of $\mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$ is 0. Thus, by Proposition 2.2 the Haar measure of ∂C is 0. ∎

Lemma 2.16. *We have* $\mathrm{d}(A') = \lambda_G(C)$ *(see text above* Lemma 2.12 *for the definition of* A'*).*

Proof. Let $\mathfrak{q} \in \Omega_L \setminus S'$. As $\zeta_m \in U$, we have $(\pi_\mathfrak{q}(U) : \pi_\mathfrak{q}(U^m)) = m$. Moreover

$$U^m \subset W \subset U,$$

so that $(\pi_\mathfrak{q}(U) : \pi_\mathfrak{q}(W))$ divides m. It follows that $\pi_\mathfrak{q}(U) = \pi_\mathfrak{q}(W)$ if and only if for all $p \in \mathcal{P}$ there is $i \in \mathbf{Z}_{\geq 0}$ such that p^i divides $(\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(U))$ and p^{i+1} does not divide $(\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(W))$.

Let $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$, and note that $\mathfrak{q}$ splits completely in $L(U^{1/p^i})$ if and only if

$$p^i \mid (\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(U)).$$

Similarly $\mathfrak{q}$ does not split completely in $L(W^{1/p^{i+1}})$ if and only if

$$p^{i+1} \nmid (\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(W)).$$

Now, let $M = L(U^{1/m^\infty})$, let $G' = \mathrm{Gal}(M/L)$, and let C' be the image of C under the canonical surjective map $G \longrightarrow G'$. Observe that there are only finitely many primes ramifying in M. We will show that $\mathrm{d}(A') = \lambda_{G'}(C')$. Then by Lemma 2.6 we have $\mathrm{d}(A') = \lambda_G(C)$, which finishes the proof.

To this end, recall that $\mathfrak{q}$ splits completely in an intermediate extension F of M/L if and only if for any prime ideal Q of M dividing $\mathfrak{q}$ we have $\mathrm{Frob}(Q/\mathfrak{q})|_F = \mathrm{id}$ if and only if

$$(\mathfrak{q}, M/L)|_F = \{\sigma|_F : \sigma \in (\mathfrak{q}, M/L)\} = \{\mathrm{id}\}.$$

Thus, we have $\pi_{\mathfrak{q}}(U) = \pi_{\mathfrak{q}}(W)$ if and only if for all $p \in \mathcal{P}$ there is $i \in \mathbf{Z}_{\geq 0}$ such that

$$(\mathfrak{q}, M/L)|_{L(U^{1/p^i})} = \{\mathrm{id}\} \text{ and } (\mathfrak{q}, M/L)|_{L(U^{1/p^i}, W^{1/p^{i+1}})} \neq \{\mathrm{id}\}.$$

By Lemma 2.13 we have $A' = \{\mathfrak{q} \in \Omega_L \setminus S' : \pi_{\mathfrak{q}}(U) = \pi_{\mathfrak{q}}(W)\}$. Hence, by the equivalences that we just saw we have

$$A' = \{\mathfrak{q} \in \Omega_L \setminus S' : (\mathfrak{q}, M/L) \subset C'\}.$$

Then by Theorem 2.8 and Lemma 2.15 we have $\mathrm{d}(A') = \lambda_{G'}(C')$. ∎

Proof of Theorem 2.10. For $p \in \mathcal{P}$ let $G_p = \mathrm{Gal}(L(U^{1/p^\infty})/L)$, and for $i \in \mathbf{Z}_{\geq 0}$ let

$$G_p(i) = \mathrm{Gal}(L(U^{1/p^\infty})/L(U^{1/p^i})),$$

$$H_p(i) = \mathrm{Gal}(L(U^{1/p^\infty})/L(U^{1/p^i}, W^{1/p^{i+1}}))$$

and $C_p(i) = G_p(i) \setminus H_p(i)$.

Let $p \in \mathcal{P}$ and note that L contains the pth roots of unity. Hence, for every $i \in \mathbf{Z}_{\geq 0}$ the field $L(U^{1/p^i})$ is of p-power degree over L. It follows that the fields $L(U^{1/p^\infty})$ for $p \in \mathcal{P}$ are linearly disjoint over L, so that the canonical morphism

$$\varphi\colon G \longrightarrow \prod_{p \in \mathcal{P}} G_p$$

of profinite groups is surjective. One easily sees that

$$\varphi(C) = \prod_{p \in \mathcal{P}} \coprod_{i=0}^{\infty} C_p(i),$$

so that by Lemma 2.7 and Lemma 2.6 we have

$$\lambda_G(C) = \prod_{p\in\mathcal{P}} \lambda_{G_p}\left(\coprod_{i=0}^{\infty} C_p(i)\right).$$

Using Definition 2.1, Proposition 2.2 and Lemma 2.5, we find

$$\begin{aligned}
\mathrm{d}(A') = \lambda_G(C) &= \prod_{p\in\mathcal{P}} \sum_{i=0}^{\infty} \big(\lambda_{G_p}(G_p(i)) - \lambda_{G_p}(H_p(i))\big) \\
&= \prod_{p\in\mathcal{P}} \sum_{i=0}^{\infty} \left(\frac{1}{\big[L(U^{1/p^i}) : L\big]} - \frac{1}{\big[L(U^{1/p^i}, W^{1/p^{i+1}}) : L\big]}\right) \\
&= \prod_{p\in\mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{\big[L(U^{1/p^i}) : L\big]} \left(1 - \frac{1}{\big[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})\big]}\right).
\end{aligned}$$

The desired formula for $\mathrm{d}(A)$ now follows by applying Lemma 2.12. ∎

5. Galois representations on radical groups

For G a group and H a subgroup of G, we write $\mathrm{Aut}_H(G)$ for the set of group automorphisms of G that are the identity on H.

Let L be a field, let U be a subgroup of L^*, and let s be a Steinitz number that is not divisible by $\mathrm{char}\, L$. The field $L(U^{1/s})$ over L is Galois and any field automorphism of $L(U^{1/s})$ is determined by its action on $U^{1/s}$, that is, we can identify $\mathrm{Gal}(L(U^{1/s})/L)$ with a subgroup of $\mathrm{Aut}_U(U^{1/s})$. By abuse of notation we denote this subgroup also by $\mathrm{Gal}(L(U^{1/s})/L)$. If U is finitely generated, the group $\mathrm{Aut}_U(U^{1/s})$ is the profinite group

$$\varprojlim_d \mathrm{Aut}_U(U^{1/d}),$$

where d runs over all positive integers dividing s. As $\mathrm{Gal}(L(U^{1/s})/L)$ is compact and $\mathrm{Aut}_U(U^{1/s})$ is Hausdorff, the subgroup $\mathrm{Gal}(L(U^{1/s})/L)$ of $\mathrm{Aut}_U(U^{1/s})$ is closed.

For L a number field, U a subgroup of L^*, and s a Steinitz number, we define

$$\mathrm{Sat}_s(U) = U^{1/s} \cap L^*$$

and

$$\mathrm{Cyc}_s(U) = U^{1/s} \cap L(\mu_s)^*.$$

In some cases, we expand our notation to $\mathrm{Sat}_s(U, L)$ and $\mathrm{Cyc}_s(U, L)$ for these groups, to clarify the base field L in which we view U as a subset. When s is $\infty = \prod_p p^\infty$ where p runs over all prime numbers, we leave out the subscript s from the notation, which is consistent with the notation of the previous chapter (see Section 1.2).

For a group G we write $\exp(G)$ for its exponent. Moreover, recall that for a prime number p we write v_p for the p-adic valuation function.

In this section we prove the following theorem.

Theorem 2.17. *Let L be a number field, let U be a finitely generated subgroup of L^*, and let s be a Steinitz number.*

(a) *Then there is $d \in \mathbf{Z}_{\geq 1}$ such that for every $d' \in \mathbf{Z}_{\geq 1}$ with $d|d'|s$ we have*

$$\mathrm{Aut}_{U^{1/d'}}(U^{1/s}) \subset \mathrm{Gal}(L(U^{1/s})/L).$$

(b) *Suppose that $s = p^\infty$, where p is prime. Let*

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2, \\ L(\mu_p) & \text{otherwise}. \end{cases}$$

Then $\exp(\mathrm{Sat}_s(U, F)/U)$ is finite, and there is $j \in \mathbf{Z}_{\geq 0}$ with

$$j \leq \mathrm{v}_p(\exp(\mathrm{Sat}_s(U, F)/U))$$

such that for all $i \in \mathbf{Z}_{\geq j}$ we have

$$\mathrm{Aut}_{U^{1/p^i}}(U^{1/s}) \subset \mathrm{Gal}(L(U^{1/s})/L).$$

Lemma 2.18. *Let $s = p^\infty$, where p is a prime. Let F be a number field with $\mu_p \subset F^*$, and if $p = 2$, with $\mu_4 \subset F^*$. Let $U \subset F^*$ be a subgroup such that $\mathrm{Sat}_s(U) = U$. Then $\mathrm{Cyc}_s(U) = \mu_s \cdot U$.*

Proof. The inclusion $\supset$ clearly holds. Moreover, the quotient

$$\mathrm{Cyc}_s(U)/(U \cdot \mu_s)$$

is p-primary, so it suffices to show that this quotient has no element of order p. To this end, let $x \in F(\mu_s)^*$ such that $x^p \in U \cdot \mu_s$. We will show that $x \in U \cdot \mu_s$. Note that there are $u \in U$ and $\zeta \in \mu_s$ such that $x^p = u \cdot \zeta$. Let ξ be a pth root of ζ, and let $y = x/\xi \in F(\mu_s)^*$. Then we will show that $y \in U$, which implies that $x \in U \cdot \mu_s$, as desired. Suppose that $y \in F^*$. As $U = \mathrm{Sat}_s(U)$ and $y^p \in U$, it follows that $y \in U$, as desired.

Suppose that $y \notin F^*$. Since F^* contains μ_p, and also μ_4 if $p = 2$, we have

$$\mathrm{Gal}(F(\mu_s)/F) \cong \mathbf{Z}_p$$

as profinite groups. Moreover, as $y^p \in U \subset F^*$, it follows that $F(y)$ is the unique subextension of $F(\mu_s)/F$ of degree p over F. Then by Kummer theory we have that

$$F(y) = F(\epsilon^{1/p}),$$

where ϵ is a generator of $\mu_s(F)$, and moreover, there are $i \in \{1, \ldots, p-1\}$ and $a \in F^*$ such that

$$y^p = \epsilon^i \cdot a^p.$$

Now, as $\mathrm{Sat}_s(U) = U$, we have $\epsilon \in U$. Furthermore, since $a^p \in U$, we have $a \in U$. It follows that $y = \eta \cdot a$ for some $\eta \in \mu_s$, that is, we have $y \in \mu_s \cdot U$, as desired. ∎

Throughout the rest of this section, let L be a number field, let U be a finitely generated subgroup of L^*, let $n = \mathrm{rk}(U)$ (see Definition 1.2), let s be a Steinitz number, let $\Gamma_s = \mathrm{Gal}(L(\mu_s)/L)$, let $A_s = \mathrm{Aut}_{\mu_s \cap U}(\mu_s)$, let $G = \mathrm{Gal}(L(U^{1/s})/L)$, and let $A = \mathrm{Aut}_U(U^{1/s})$.

Lemma 2.19. *The groups* $\mathrm{Sat}_s(U)$ *and* $\mathrm{Cyc}_s(U)/\mu_s$ *are finitely generated of rank* n.

Proof. By Lemma 1.4, the groups U and $\mathrm{Sat}(U)$ are finitely generated of rank n, and $\mathrm{Cyc}(U)/\mu$ is free of rank n. Since $U \subset \mathrm{Sat}_s(U) \subset \mathrm{Sat}(U)$, we have that $\mathrm{Sat}_s(U)$ is finitely generated of rank n.

Let $(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$ be the torsion subgroup of $\mathrm{Cyc}_s(U)$. Note that the quotient

$$\mathrm{Cyc}_s(U)/(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$$

maps injectively to $\mathrm{Cyc}(U)/\mu$. As the latter is a free abelian group of rank n, it follows that $\mathrm{Cyc}_s(U)/(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$ is free of rank n.

Let $w = \mu(L)$, and observe that

$$\mu_s \subseteq (\mathrm{Cyc}_s(U))_{\mathrm{tor}} \subseteq U_{\mathrm{tor}}^{1/s} \subseteq \mu_{ws}.$$

As μ_{ws}/μ_s is finite, it follows that $\mathrm{Cyc}_s(U)/\mu_s$ is finitely generated. ∎

Lemma 2.20. (a) *The Galois group* Γ_s *is open in* A_s.

(b) *Suppose that* $s = p^\infty$, *where* p *is prime. Let* $\mu_s \cap L^* = \mu_{p^e}$. *Suppose that* $e \in \mathbf{Z}_{\geq 1}$. *If* $p = 2$, *suppose that* $e \in \mathbf{Z}_{\geq 2}$. *Then*

$$\Gamma_s = \mathrm{Aut}_{\mu_{p^e}}(\mu_s)$$

inside A_s.

Proof. By the irreducibility of the cyclotomic polynomials over $\mathbf{Q}$, we may identify the Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_s)/\mathbf{Q})$ with $\mathrm{Aut}(\mu_s)$. Moreover

$$\Gamma_s \cong \mathrm{Gal}(\mathbf{Q}(\mu_s)/(L \cap \mathbf{Q}(\mu_s))),$$

as profinite groups. As $L \cap \mathbf{Q}(\mu_s)$ is a finite extension of $\mathbf{Q}$, it follows that Γ_s is a closed subgroup of finite index in $\mathrm{Aut}(\mu_s)$. It follows that Γ_s is open in A_s, as desired.

Suppose s, p, and e are as in (b). There is a canonical isomorphism

$$\varphi\colon\ \mathrm{Aut}(\mu_s) \longrightarrow \mathbf{Z}_p^*$$

of profinite groups, so $\varphi(\Gamma_s)$ is an open subgroup of $\mathbf{Z}_p^*$.

As every element of Γ_s is the identity on μ_{p^e}, the image $\varphi(\Gamma_s)$ is contained in the subgroup $1 + p^e\mathbf{Z}_p$ of $\mathbf{Z}_p^*$. Moreover, since $\mu_{p^{e+1}} \not\subset L$, the image $\varphi(\Gamma_s)$ is not contained in $1 + p^{e+1}\mathbf{Z}_p$.

Now, because $e \geq 2$ for $p = 2$, we have $1 + p^e\mathbf{Z}_p \cong \mathbf{Z}_p$ as profinite groups. The latter implies that $1+p^e\mathbf{Z}_p$ is topologically generated by any element not in $1+p^{e+1}\mathbf{Z}_p$. Thus $\varphi(\Gamma_s)$ is equal to $1+p^e\mathbf{Z}_p$. We conclude that the image of Γ_s inside A_s is equal to $\mathrm{Aut}_{\mu_{p^e}}(\mu_s)$. This proves (b). ∎

Proof of Theorem 2.17. As μ_s is a direct summand of $U^{1/s}$, the natural map

$$r\colon A \longrightarrow A_s$$

sending f to $f|_{\mu_s}$ is surjective. Moreover, one easily checks that the kernel $\mathrm{Aut}_{\mu_s\cdot U}(U^{1/s})$ of r is canonically isomorphic to $\mathrm{Hom}(U^{1/s}/(\mu_s \cdot U), \mu_s)$ as a profinite group.

On the other hand, by Kummer theory the kernel of the restriction morphism $G \longrightarrow \Gamma_s$ is canonically isomorphic to $\mathrm{Hom}(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s)$ as a profinite group. The surjective morphism $U^{1/s}/(\mu_s \cdot U) \longrightarrow U^{1/s}/\operatorname{Cyc}_s(U)$ of discrete groups gives rise to a canonical injective morphism

$$\mathrm{Hom}(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s) \longrightarrow \mathrm{Hom}(U^{1/s}/(\mu_s \cdot U), \mu_s)$$

of profinite groups that makes the following diagram of profinite groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}\big(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s\big) & \longrightarrow & G & \longrightarrow & \Gamma_s & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}\big(U^{1/s}/(\mu_s \cdot U), \mu_s\big) & \longrightarrow & A & \longrightarrow & A_s & \longrightarrow & 0 \end{array} \qquad (*)$$

commutative, where all other maps are defined above.

The kernel of $U^{1/s}/(\mu_s \cdot U) \longrightarrow U^{1/s}/\operatorname{Cyc}_s(U)$ is equal to $\operatorname{Cyc}_s(U)/(\mu_s \cdot U)$. Therefore the cokernel of the left vertical map is contained in $\operatorname{Hom}(\operatorname{Cyc}_s(U)/(\mu_s \cdot U), \mu_s)$. As by Lemma 2.19 the quotient $\operatorname{Cyc}_s(U)/(\mu_s \cdot U)$ is finite, it follows that the cokernel of the left vertical map is finite.

On the other hand, by Lemma 2.20 the profinite group Γ_s is open in A_s, implying that the cokernel $\operatorname{coker}(\Gamma_s \longrightarrow A_s)$ is finite. Hence $\operatorname{coker}(G \longrightarrow A)$ is finite. As G is closed in A (see beginning of this section), it follows that G is open in A. Equivalently, there is $d \in \mathbf{Z}_{\geq 1}$ such that

$$\operatorname{Aut}_{U^{1/d}}(U^{1/s}) \subset \operatorname{Gal}(L(U^{1/s})/L).$$

Moreover, for every $d' \in \mathbf{Z}_{\geq 1}$ with $d|d'|s$ we have

$$\operatorname{Aut}_{U^{1/d'}}(U^{1/s}) \subset \operatorname{Aut}_{U^{1/d}}(U^{1/s}),$$

which finishes the proof of (a).

Suppose that $s = p^\infty$, where p is prime. By (a) we know that there is $j \in \mathbf{Z}_{\geq 0}$ such that for every $i \in \mathbf{Z}_{\geq j}$

$$\operatorname{Aut}_{U^{1/p^i}}(U^{1/s}) = \operatorname{Gal}(L(U^{1/s})/L(U^{1/p^i})).$$

Let

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2, \\ L(\mu_p) & \text{otherwise.} \end{cases}$$

and let $U' = \operatorname{Sat}_s(U, F)$. Then Lemma 2.19 implies that $\exp(U'/U)$ is finite. Let

$$e = \mathrm{v}_p(\exp(U'/U)).$$

We will show that j can be taken equal to e, which finishes the proof. To this end, we will prove that $\operatorname{Aut}_{U'}(U'^{1/s}) \subset G$.

First, note that $\mu_s \cap F^* = \mu_s \cap U'$. Then Lemma 2.20(b) implies that

$$\mathrm{Gal}(F(\mu_s)/F) = \mathrm{Aut}_{U' \cap \mu_s}(\mu_s).$$

Since $F(\mu_s) = L(\mu_s)$, it follows that

$$\mathrm{Aut}_{U' \cap \mu_s}(\mu_s) = \mathrm{Gal}(L(\mu_s)/F).$$

On the other hand, by Lemma 2.18 we have

$$\mathrm{Cyc}_s(U, F) = \mu_s \cdot U'.$$

Moreover, since $U'^{1/s} = U^{1/s}$, we have

$$\mathrm{Hom}(U^{1/s}/\mathrm{Cyc}_s(U', F), \mu_s) = \mathrm{Hom}(U^{1/s}/(\mu_s \cdot U'), \mu_s).$$

Replacing L by F and U by U' in $(*)$, we obtain

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}\big(U^{1/s}/\mathrm{Cyc}_s(U', F), \mu_s\big) & \longrightarrow & \mathrm{Gal}(L(U^{1/s})/F) & \longrightarrow & \mathrm{Gal}(L(\mu_s)/F) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}\big(U^{1/s}/(\mu_s \cdot U'), \mu_s\big) & \longrightarrow & \mathrm{Aut}_{U'}(U^{1/s}) & \longrightarrow & \mathrm{Aut}_{U' \cap \mu_s}(\mu_s) & \longrightarrow & 0 \end{array}$$

where, by the above, the left and right vertical maps are isomorphisms. It follows that

$$\mathrm{Gal}(L(U^{1/s})/F) = \mathrm{Aut}_{U'}(U^{1/s}),$$

so that $\mathrm{Aut}_{U'}(U^{1/s}) \subset G$. At last, as $U' \subset U^{1/p^e}$, we have

$$\mathrm{Aut}_{U^{1/p^e}}(U^{1/s}) \subset \mathrm{Aut}_{U'}(U^{1/s}) \subset G,$$

which finishes the proof. ∎

6. Rationality of the density

Throughout this section, let K be a number field, let W be a finitely generated subgroup of K^*, and let V be cocyclic cofinite subgroup of W. Let $m = (W : V)$, let $\mathcal{P}$ be the set of prime divisors of m, let $n = \mathrm{rk}(W)$ (see Definition 1.2), let $U = V^{1/m}$, and let $L = K(U)$. We remark that $W/V \cong \mathbf{Z}/m\mathbf{Z}$ implies that $W \subset U$.

In this section, we prove a closed-form expression of the density $\mathrm{d}(A(W,V))$ using the formula given in Theorem 2.10 and Theorem 2.17.

Theorem 2.21. *Let $(j_p)_{p\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then the density $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \prod_{p\in\mathcal{P}} \Big[\tfrac{1}{[L(U^{1/p^{j_p}}):L]} \cdot \tfrac{p^n(p-1)}{p^{n+1}-1} + \textstyle\sum_{i=0}^{j_p-1} \Big(\tfrac{1}{[L(U^{1/p^i}):L]} - \tfrac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \Big) \Big].$$

We remark that one can find suitable $(j_p)_{p\in\mathcal{P}}$, as in the theorem above, in Theorem 2.17.

Corollary 2.22. *Suppose that for every $p \in \mathcal{P}$ we have*

$$\mathrm{Gal}(L(U^{1/p^\infty})/L) = \mathrm{Aut}_U(U^{1/p^\infty}).$$

Then

$$\mathrm{d}(A(W,V)) = \frac{1}{[L:K]} \prod_{p\in\mathcal{P}} \frac{p^n(p-1)}{p^{n+1}-1}.$$

In addition, suppose that $[L:K] = \phi(m)m^{n-1}$, where ϕ is Euler's totient function. Then we have

$$\mathrm{d}(A(W,V)) = \frac{1}{m^n} \cdot \prod_{p\in\mathcal{P}} \frac{p^{n+1}}{p^{n+1}-1}.$$

Proof. The proof follows directly from Theorem 2.21 by putting $j_p = 0$ for all $p \in \mathcal{P}$. ∎

Lemma 2.23. *Let $p \in \mathcal{P}$, and let $i \in \mathbf{Z}_{\geq 0}$. Then the following hold.*

(a) *The degree $[L(U^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p^{n+1}, and if $i \geq j_p$, it is equal to p^{n+1}.*

(b) *The degree $[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p, and if $i \geq j_p$, it is equal to p.*

Proof. Let $s = p^\infty$. As U is a finitely generated abelian group of rank n and $\mu_m \subset U$, we have $U \cong \frac{1}{u}\mathbf{Z}/\mathbf{Z} \oplus \mathbf{Z}^n$, where $u \in \mathbf{Z}_{\geq 1}$ is divisible by m. Then we have

$$U^{1/p^i} \cong \frac{1}{up^i}\mathbf{Z}/\mathbf{Z} \oplus \left(\frac{1}{p^i}\mathbf{Z}\right)^n,$$

so that

$$\begin{aligned} \mathrm{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) &\cong \mathrm{Hom}\left(\frac{U^{1/p^{i+1}}}{U^{1/p^i}}, U^{1/p^{i+1}}\right) \\ &\cong \mathrm{Hom}\left(\left(\frac{1}{p}\mathbf{Z}/\mathbf{Z}\right)^{n+1}, \frac{1}{up^{i+1}}\mathbf{Z}/\mathbf{Z} \oplus \left(\frac{1}{p^{i+1}}\mathbf{Z}\right)^n\right). \end{aligned}$$

Since

$$\#\,\mathrm{Hom}\left((\mathbf{Z}/p\mathbf{Z})^{n+1}, \mathbf{Z}/up^{i+1}\mathbf{Z} \oplus \left(\frac{1}{p^{i+1}}\mathbf{Z}\right)^n\right) = p^{n+1},$$

we have that

$$\#\,\mathrm{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) = p^{n+1}.$$

Now, note that

$$\mathrm{Gal}(L(U^{1/p^{i+1}})/L(U^{1/p^i})) \subset \mathrm{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}),$$

which implies that $[L(U^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p^{n+1}.

Now, suppose that $i \in \mathbf{Z}_{\geq j_p}$. Then by Theorem 2.17

$$\mathrm{Gal}(L(U^{1/s})/L(U^{1/p^i})) = \mathrm{Aut}_{U^{1/p^i}}(U^{1/s}).$$

Moreover, by [Pal14, Theorem 2.12] the sequence

$$0 \longrightarrow \mathrm{Aut}_{U^{1/p^{i+1}}}(U^{1/s}) \longrightarrow \mathrm{Aut}_{U^{1/p^i}}(U^{1/s}) \longrightarrow \mathrm{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) \longrightarrow 0$$

of profinite groups is exact. Then by Galois theory

$$p^{n+1} = \#\operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) = [L(U^{1/p^{i+1}}) : L(U^{1/p^i})].$$

This proves (a).

For (b), note that $W^{1/p^i} \subset L(U^{1/p^i})^*$. Hence, by Kummer theory

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = (W^{1/p^i} : L(U^{1/p^i})^{*p} \cap W^{1/p^i}).$$

Recall that $U^m = V \subset W$, so that $(U^m)^{1/p^i} \subset W^{1/p^i}$. One easily checks that

$$W^{1/p^{i-1}} \cdot (U^m)^{1/p^i} \subset W^{1/p^i} \cap L(U^{1/p^i})^{*p}.$$

As $W^{1/p^{i-1}} \cdot (U^m)^{1/p^i}$ maps to the unique subgroup of index p of the cyclic group

$$W^{1/p^i}/(U^m)^{1/p^i}$$

of order m, it follows that $(W^{1/p^i} : W^{1/p^i} \cap L(U^{1/p^i})^{*p})$ divides p. Hence

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] \mid p.$$

On the other hand, the degree $[L(U^{1/p^{i+1}}) : L(U^{1/p^i}, W^{1/p^{i+1}})]$ divides p^n, as the p^{i+1}th roots of unity are already contained in $L(U^{1/p^i}, W^{1/p^{i+1}})$. Hence for $i \geq j_p$ we have

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = p,$$

as desired. ∎

Proof of Theorem 2.21. Write $A = A(W, V)$. Then by Theorem 2.10 we have

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right).$$

By Lemma 2.23, we have for all $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq j_p}$

$$[L(U^{1/p^{i+1}}) : L(U^{1/p^i})] = p^{n+1}$$

and

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = p.$$

Hence

$$\sum_{i=j_p}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right)$$

is equal to

$$\frac{1}{[L(U^{1/p^{j_p}}) : L]} \sum_{i=0}^{\infty} \frac{1}{p^{(n+1)i}} \left(1 - \frac{1}{p}\right) = \frac{1}{[L(U^{1/p^{j_p}}) : L]} \cdot \frac{p^n(p-1)}{p^{n+1}-1}.$$

Using this in the expression for $\mathrm{d}(A)$, we find

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \left[\frac{1}{[L(U^{1/p^{j_p}}) : L]} \cdot \frac{p^n(p-1)}{p^{n+1}-1} + \sum_{i=0}^{j_p-1} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right)\right],$$

which is the desired formula. ∎

7. Main theorem

In this section we

Theorem 2.24. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a cocyclic cofinite subgroup of W. Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Let $n = \mathrm{rk}(W)$ (see* Definition 1.2*), and let $\mathcal{P}$ be the set of primes dividing m. Let $(j_p)_{p \in \mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then the following statements hold.

(a) *The density* $\mathrm{d}(A(W,V))$ *exists and equals a positive rational number in the interval*

$$\left[\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)},\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right)\right]$$

whose denominator divides $m^n\cdot\prod_{p\in\mathcal{P}}\big(p^{(n+1)j_p-1}\cdot(p^{n+1}-1)\big)$.

(b) $\mathrm{d}(A(W,V))=1$ *if and only if* $V=W$ *or* W *is finite.*

(c) $\mathrm{d}(A(W,V))$ *is computable as a function of* K, W *and* V.

Proof. By Theorem 2.21 we have that $\mathrm{d}(A(W,V))$ exists and is equal to

$$\tfrac{1}{[L:K]}\prod_{p\in\mathcal{P}}\Big[\tfrac{1}{[L(U^{1/p^{j_p}}):L]}\cdot\tfrac{p^n(p-1)}{p^{n+1}-1}+\textstyle\sum_{i=0}^{j_p-1}\Big(\tfrac{1}{[L(U^{1/p^i}):L]}-\tfrac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L]}\Big)\Big],$$

which is rational. We first note that $[L:K]$ divides $\phi(m)m^{n-1}$, where ϕ is Euler's totient function.

Now, let $p\in\mathcal{P}$. By Lemma 2.23 we have for all $i\in\mathbf{Z}_{\geq 0}$ that

$$[L(U^{1/p^{i+1}}):L(U^{1/p^i})]\mid p^{n+1}$$

and

$$[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]\mid p.$$

To ease the notation, for $i\in\mathbf{Z}_{\geq 0}$ write

$$T_i=\frac{1}{[L(U^{1/p^i}):L]}-\frac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L]},$$

and note that

$$T_i=\frac{1}{[L(U^{1/p^i}):L]}\left(1-\frac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]}\right).$$

Hence $[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]=1$ implies $T_i=0$. Using Lemma 2.23 we obtain for $p\in\mathcal{P}$

$$\frac{1}{[L(U^{1/p^{j_p}}):L]}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+\sum_{i=0}^{j_p-1}T_i\geq\frac{1}{p^{(n+1)j_p}}\cdot\frac{p^{n+1}-p^n}{p^{n+1}-1}=\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)},$$

so that

$$\begin{aligned}\mathrm{d}(A(W,V)) &\geq \frac{1}{[L:K]}\prod_{p\in\mathcal{P}}\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)}\\ &\geq \frac{1}{\phi(m)m^{n-1}}\prod_{p\in\mathcal{P}}\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)}.\end{aligned}$$

Then using the identity $\phi(m) = m\cdot\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p}\right)$ in the latter, we obtain the lower bound

$$\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)}$$

for $\mathrm{d}(A(W,V))$. For the upper bound, note that

$$\sum_{i=0}^{j_p-1}T_i \leq 1-\frac{1}{[L(U^{1/p^{j_p}}):L]}.$$

Then for $p\in\mathcal{P}$ write $d_p = [L(U^{1/p^{j_p}}):L]$, so that we have

$$\begin{aligned}\frac{1}{d_p}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+\sum_{i=0}^{j_p-1}T_i &\leq \frac{1}{d_p}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+1-\frac{1}{d_p}\\ &\leq 1-\frac{1}{p^{(n+1)j_p}}\left(1-\frac{p^n(p-1)}{p^{n+1}-1}\right)\\ &= 1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)},\end{aligned}$$

where we use that $d_p \leq p^{(n+1)j_p}$ (see Lemma 2.23). Thus, as $[L:K]\geq 1$, an upper bound for $\mathrm{d}(A(W,V))$ is

$$\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right).$$

Now, we want to find $x\in\mathbf{Z}_{\geq 1}$ such that $x\cdot\mathrm{d}(A(W,V))\in\mathbf{Z}$. To this end, note that

$$\phi(m)m^{n-1}\cdot[L:K]^{-1}\in\mathbf{Z}.$$

Moreover, by Lemma 2.23 we have

$$p^{(n+1)j_p}\cdot[L(U^{1/p^{j_p}}):L]^{-1}\in\mathbf{Z}.$$

As for $i \in \{0, \ldots, j_p - 1\}$ the fields $L(U^{1/p^i})$ and $L(U^{1/p^i}, W^{1/p^{i+1}})$ are contained in $L(U^{1/p^{j_p}})$, we have

$$p^{(n+1)j_p} \cdot \sum_{i=0}^{j_p-1} T_i \in \mathbf{Z}.$$

It follows that the denominator of $\mathrm{d}(A(W,V))$ divides

$$\phi(m) m^{n-1} \prod_{p \in \mathcal{P}} \left(p^{(n+1)j_p} \cdot \frac{p^{n+1}-1}{p-1} \right),$$

which by using $\phi(m) = m \cdot \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)$ is equal to

$$m^n \cdot \prod_{p \in \mathcal{P}} \left(p^{(n+1)j_p - 1} \cdot \left(p^{n+1} - 1\right) \right),$$

as desired.

From the lower bound, we see that $\mathrm{d}(A(W,V))$ is nonzero. From the upper bound, we see that $\mathrm{d}(A(W,V)) = 1$ only if $m = 1$ or $n = 0$, that is, only if $V = W$ or W is finite. On the other hand, if $V = W$ or W is finite, we easily see that $\mathrm{d}(A(W,V)) = 1$. This proves (a) and (b).

To prove (c), we will show that there exists an algorithm that terminates after finitely many steps, whose input is K, W, and V, and whose output is the density $\mathrm{d}(A(W,V))$. Let K, W, V, n, $\mathcal{P}$, U, and L be as in the theorem. By Theorem 2.21 we have that $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \textstyle\prod_{p \in \mathcal{P}} \left[\frac{1}{[L(U^{1/p^{jp}}):L]} \cdot \frac{p^n(p-1)}{p^{n+1}-1} + \sum_{i=0}^{j_p-1} \left(\frac{1}{[L(U^{1/p^i}):L]} - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \right) \right],$$

so it suffices to show that there exist three algorithms for calculating (1) $\mathcal{P}$, (2) $(j_p)_{p \in \mathcal{P}}$, and (3) the degrees of the field extensions $[L(U^{1/p^i}) : L]$ and $[L(U^{1/p^i}, W^{1/p^{i+1}}) : L]$ for $i \in \{0, \ldots, j_p\}$. The algorithms for (1) and (3) are well-known from elementary computational algebraic number theory for which we refer to [Coh96]. It remains to show that for each $p \in \mathcal{P}$ we can compute j_p.

To this end, let $p \in \mathcal{P}$, and let $s = p^\infty$. Let

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2 \\ L & \text{otherwise.} \end{cases}$$

Compute and write

$$U = \coprod_{i=1}^{k} u_i \cdot U^p,$$

and compute

$$S_0 = \langle x \in F : x^p \in \{u_1, \ldots, u_k\} \rangle.$$

If $S_0 \subset U$, we have $\exp(\mathrm{Sat}_s(U, F)/U) = 1$ and put $j_p = 0$ (see Theorem 2.17). Otherwise, let $U_1 = U \cdot S_0$, and write

$$U_1 = \coprod_{i=1}^{k_1} u_{i,1} \cdot U_1^p.$$

Then compute

$$S_1 = \langle x \in F : x^p \in \{u_{1,1}, \ldots, u_{k_1,1}\} \rangle.$$

If $S_1 \subset U_1$, then we have $\exp(\mathrm{Sat}_s(U, F)/U) = p$ and put $j_p = 1$. Otherwise, repeat the above process to define U_2 and find S_2, and so on. By Lemma 2.19 the quotient $\mathrm{Sat}_s(U, F)/U$ is finite, so there is $i \in \mathbf{Z}$ such that $S_i \subset U_i$. Continue the above process until $S_i \subset U_i$, and put $j_p = i$. Then observe that $\exp(\mathrm{Sat}_s(U, F)/U) = p^{j_p}$. This shows that there is an algorithm to compute $(j_p)_{p \in \mathcal{P}}$, which finishes the proof of (c). ∎

Theorem 2.25. *Let K be a number field, and let W be a finitely generated subgroup of K^* of positive rank, and let V be a cocyclic cofinite subgroup of W. Let V' be a subgroup of W containing V. Then $\mathrm{d}(A(W, V)) = \mathrm{d}(A(W, V'))$ if and only if $V = V'$.*

Proof. First, note that $V = V'$ clearly implies $\mathrm{d}(A(W, V)) = \mathrm{d}(A(W, V'))$. To prove the reverse implication, let V' be a subgroup of W containing V, and assume $V' \neq V$. We

will show that $\mathrm{d}(A(W,V)) < \mathrm{d}(A(W,V'))$, which finishes the proof. As for V'' such that $V \subset V'' \subset V'$ we have

$$\mathrm{d}(A(W,V)) \leq \mathrm{d}(A(W,V'')) \leq \mathrm{d}(A(W,V')),$$

we may assume that V is of prime index, say q, in V'.

Now, let $m = (W : V)$, let $U = V^{1/m}$, let $L = K(U)$, let $A'(W,V)$ as defined above Lemma 2.12, and let $\overline{L}$ be an algebraic closure of L (and of K). For p dividing m and $i \in \mathbf{Z}_{\geq 0}$, let $G_{p,i}$, $H_{p,i}$, $C_{p,i}$, C_p and C be as defined above Lemma 2.14. Then by Lemma 2.16 and Lemma 2.12 we have

$$\mathrm{d}(A(W,V)) = \frac{1}{[L:K]} \cdot \lambda_{\mathrm{Gal}(\overline{L}/L)}(C).$$

Observe that $\mathrm{Gal}(\overline{L}/L)$ is a subgroup of $G = \mathrm{Gal}(\overline{L}/K)$ of index $[L : K]$. By abuse of notation we write C for the image of C in G, that is, henceforth we have

$$C = \{\sigma \in \mathrm{Gal}(\overline{L}/K) : \sigma|_U = \mathrm{id}_U,\ \forall p|m : \exists i \in \mathbf{Z}_{\geq 0} : \sigma|_{U^{1/p^i}} = \mathrm{id} \wedge \sigma|_{W^{1/p^{i+1}}} \neq \mathrm{id}\}.$$

Then we have

$$\mathrm{d}(A(W,V)) = \lambda_G(C).$$

Now, let $m/q = m' = (W : V')$, let $U' = V'^{1/m'}$, let $L' = K(U')$, and note that $V' \subset V^{1/q}$ implies that $U' \subset U$ and $L' \subset L$. For p dividing m' and $i \in \mathbf{Z}_{\geq 0}$ let $G'_{p,i}$, $H'_{p,i}$, $C'_{p,i}$, C'_p and C' be defined as above with L replaced by L' and U by U'. Moreover, by abuse of notation write C' for the image of C' in G, so that

$$C' = \{\sigma \in \mathrm{Gal}(\overline{L}/K) : \sigma|_{U'} = \mathrm{id}_{U'},\ \forall p|m' : \exists i \in \mathbf{Z}_{\geq 0} : \sigma|_{U'^{1/p^i}} = \mathrm{id} \wedge \sigma|_{W^{1/p^{i+1}}} \neq \mathrm{id}\}.$$

Then we have

$$\mathrm{d}(A(W,V')) = \lambda_G(C').$$

Moreover, for every prime p and $i \in \mathbf{Z}_{\geq 0}$ we have $U'^{1/p^i} \subset U^{1/p^i}$, so $C \subset C' \subset G$. We will show that there is a non-empty open subset of C' that is disjoint from C, which by the above and the fact that non-empty open subsets have positive density, proves that

$$\mathrm{d}(A(W,V)) < \mathrm{d}(A(W,V')),$$

as desired. Let $j \in \mathbf{Z}_{\geq 0}$ be such that $\mathrm{Aut}_{U^{1/q^j}}(U^{1/q^\infty}) \subset \mathrm{Gal}(L(U^{1/q^\infty})/L)$ (see Theorem 2.17).

Suppose first that q does not divide m'. For primes p dividing m', let

$$X_p = C_p = \bigcup_{i=0}^{\infty} G_{p,i} \setminus H_{p,i}$$

and

$$X_q = H_{q,j} \setminus G_{q,j+1}.$$

Note that $X_q \cap C_q = \emptyset$. We claim that the set

$$X = \bigcap_{p|m} X_p$$

has the desired properties of being a non-empty open subset of C' that is disjoint from C. That X is open is proved in the same way as Lemma 2.14. That each X_p, including X_q, is non-empty follows from Lemma 2.23 (at this point it is used that W is infinite, so that n in Lemma 2.23(a) is positive). Since for primes p dividing m the degrees of the fields $L(U^{1/p^\infty})$ over L are p-powers, they are all linearly disjoint over L, so X is non-empty as well. As q does not divide m', we have $X \subset C'$. From $X_q \cap C_q = \emptyset$ it follows that we have $X \cap C = \emptyset$. This finishes the proof of this case.

Now, suppose that q divides m'. We claim that for every $i \in \mathbf{Z}_{\geq 0}$ we have

$$U'^{1/q^i} = V^{1/(m'q^i)} \cdot W^{1/q^i}.$$

It suffices to prove the claim for $i = 0$. To this end, observe that

$$V^{1/m'} \cdot W \neq V^{1/m'},$$

because W/V is cyclic of order $m'q$. Moreover, as $W \subset U'$, it follows that

$$V^{1/m'} \cdot W \subset U'.$$

As V'/V has order q, also $U'/V^{1/m'}$ has order q. It follows that $U' = V^{1/m'} \cdot W$, which finishes the proof of the claim. We remark that for $i \in \mathbf{Z}_{\geq 1}$ we have

$$V^{1/(m'q^i)} = V^{1/(mq^{i-1})} = U^{1/q^{i-1}},$$

so that the claim states that

$$U'^{1/q^i} = U^{1/q^{i-1}} \cdot W^{1/q^i}.$$

As $U^q = V^{1/m'}$ is contained in $V'^{1/m'} = U'$, we have $U \subset U'^{1/q}$, so that

$$L' \subset L \subset L'(U'^{1/q}).$$

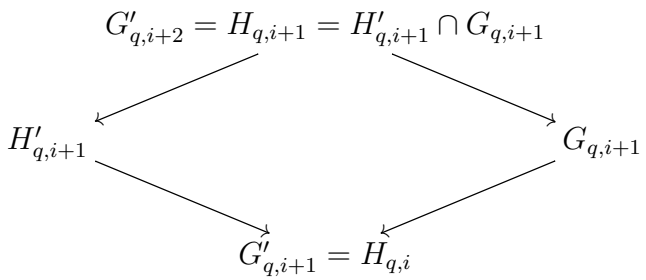
Then the claim implies that for every $i \in \mathbf{Z}_{\geq 0}$ we have

$$L'(U'^{1/q^{i+1}}) = L(U^{1/q^i}, W^{1/q^{i+1}}),$$

and moreover, since $W \subset U$, we have the following diagram

$$\begin{array}{ccccc} & & L'(U'^{1/q^{i+2}}) = L(U^{1/q^{i+1}}, W^{1/q^{i+2}}) & & \\ & \swarrow & & \searrow & \\ L'(U'^{1/q^{i+1}}, W^{1/q^{i+2}}) & & & & L(U^{1/q^{i+1}}) \\ & \searrow & & \swarrow & \\ & & L'(U'^{1/q^{i+1}}) = L(U^{1/q^i}, W^{1/q^{i+1}}) & & \end{array}$$

of fields, where the upper field is the composite of the fields on the left and right. The corresponding diagram of Galois groups looks as follows:



where the arrows in the diagram depict inclusions.

Now, for the prime divisors p of m' that are not equal to q, let

$$Y_p = C'_p = \bigcup_{i=0}^{\infty} G'_{p,i} \setminus H'_{p,i},$$

and let

$$Y_q = G'_{q,j+1} \setminus \big(H'_{q,j+1} \cup G_{q,j+1}\big).$$

Note that one has $Y_q \subset H_{q,j} \setminus G_{q,j+1}$, so that we have $Y_q \cap C_q = \emptyset$. We claim that the set $Y = \bigcap_{p|m} Y_p$ has the desired property of being a non-empty open subset of C' that is disjoint from C. That Y is open is proved in the same way as Lemma 2.14. We next prove that each Y_p is non-empty. For $p \neq q$ this follows directly from Lemma 2.23. For $q = p$, our choice of j and Lemma 2.23 imply first that $G_{q,j+1}$ has index q^n in $H_{q,j}$, and next that $H_{q,j+1}$ has index q in $G_{q,j+1}$, which by $H_{q,j+1} = H'_{q,j+1} \cap G_{q,j+1}$ implies that $G_{q,j+1}$ is not contained in $H'_{q,j+1}$, so that $H'_{q,j+1} \neq H_{q,j}$. Thus, since $n \in \mathbf{Z}_{>1}$, each of $G_{q,j+1}$ and $H'_{q,j+1}$ is a proper subgroup of $G'_{q,j+1} = H_{q,j}$, which implies that Y_q is non-empty. By linear disjointness, the set Y is non-empty as well. From $Y_q \cap C_q = \emptyset$ it follows that we have $Y \cap C = \emptyset$, while from

$$Y_q \subset G'_{q,j+1} \setminus H'_{q,j+1} \subset C'_q$$

we obtain $Y \subset C'$. This finishes the proof. ∎

Corollary 2.26. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a cofinite cocyclic subgroup of W. Let*

$$S = \{\mathfrak{p} \in \Omega_K : \text{ there is } w \in W \text{ such that } \mathrm{v}_{\mathfrak{p}}(w) \neq 0\}.$$

For $\mathfrak{p} \in \Omega_K \setminus S$ let $W_{\mathfrak{p}}$ denote the kernel of the restriction map $\pi_{\mathfrak{p}} \colon W \longrightarrow \kappa(\mathfrak{p})^*$. Let S' be a finite subset of $\Omega_K \setminus S$. Then there are $t \in \mathbf{Z}_{\geq 1}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \Omega_K \setminus S'$ such that

$$V = \langle W_{\mathfrak{p}_i} : i \in \{1, \ldots, t\}\rangle.$$

Proof. Let $T = \langle W_{\mathfrak{p}} : \mathfrak{p} \notin S', W_{\mathfrak{p}} \subset V\rangle$. Then T is cofinite and contained in V, and moreover, $\mathrm{d}(A(W,V)) > 0$ implies that T is cocyclic in W. Since T is finitely generated, there are $t \in \mathbf{Z}_{\geq 0}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \Omega_K \setminus S'$ such that $T = \langle W_{\mathfrak{p}_i} : i \in \{1, \ldots, t\}\rangle$. Now, one easily sees that $\mathrm{d}(A(W,T)) = \mathrm{d}(A(W,V))$. Hence Theorem 2.25 implies that $T = V$, as desired. ∎

8. Applications

Theorem 2.27. *Let K be a number field, and let X and Y be finitely generated subgroups of K^*. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X \cup Y : \mathrm{v}_{\mathfrak{p}}(x) \neq 0\}.$$

Suppose that for all primes $\mathfrak{p}$ in a subset of $\Omega_K \setminus S'$ of density one, we have

$$Y \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}}.$$

Then $Y \subset X$.

Proof. Suppose that $Y \not\subset X$, let $W = Y \cdot X$, and note that $X \subsetneq W$. As W is a finitely generated abelian group, there exist a prime number p and a surjective morphism

$$f \colon W \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

of groups with kernel containing X. Let $V = \ker f$, and note that $X \subset V$. As W/V is finite cyclic, Theorem 2.24 implies that

$$\mathrm{d}(\{\mathfrak{p} \in \Omega_K : W_\mathfrak{p} \subset V\}) > 0,$$

where $W_\mathfrak{p}$ is the kernel of the reduction map $\pi_\mathfrak{p} \colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Observe that for $\mathfrak{p} \in \Omega_K \setminus S'$ the condition $Y \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}}$ is equivalent to $X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}$, so that

$$\mathrm{d}(\{\mathfrak{p} \in \Omega_K : X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}\}) = 1.$$

Let $\mathfrak{p}$ be a prime of K such that $W_\mathfrak{p} \subset V$ and $X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}$. As $X \subset V$ and $W_\mathfrak{p} \subset V$, we have

$$\pi_\mathfrak{p}(X) = (X \cdot W_\mathfrak{p})/W_\mathfrak{p} \subset V/W_\mathfrak{p}.$$

Moreover, since f is surjective, we have

$$W_\mathfrak{p} \subset V \subsetneq W.$$

Hence $V/W_\mathfrak{p} \subsetneq W/W_\mathfrak{p}$. However

$$X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}} \cong W/W_\mathfrak{p},$$

which is a contradiction. It follows that $Y \subset X$. ∎

Theorem 2.28. *Let K be a number field, let X be a finitely generated subgroup of K^*, let Y be a subgroup of X, and let l be a prime number. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X : \mathrm{v}_\mathfrak{p}(x) \neq 0\}.$$

Suppose that for almost all $\mathfrak{p} \in \Omega_K \setminus S'$ we have

$$l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}}).$$

Then $(X : Y) < \infty$ and $l \nmid (X : Y)$.

Proof. Let $V = X^l \cdot Y$, and note that $Y \subset V \subset X$. For almost all $\mathfrak{p} \in \Omega_K$ we have $l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}})$. As $X \pmod{\mathfrak{p}}/V \pmod{\mathfrak{p}}$ is annihilated by l and for almost all $\mathfrak{p}$ we have

$$Y \pmod{\mathfrak{p}} \subset V \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}},$$

it follows that for almost all $\mathfrak{p}$ we have $X \pmod{\mathfrak{p}} = V \pmod{\mathfrak{p}}$. Then Theorem 2.27 implies that $X = V = X^l \cdot Y$, so that $(X/Y)^l = X/Y$. As X/Y is a finitely generated abelian group with the property that $(X/Y)^l = X/Y$, it follows that X/Y is finite of order coprime to l. ■