Radicals in arithmetic

Palenstijn, W.J.

Chapter 5

Near-primitive roots and higher rank

5.1 Introduction

In this chapter we generalize the results from Chapter 1 to a broader setting.

Let K be a number field, and let $V \subset K^*$ be a finitely generated subgroup with $\mathrm{rank}(V/V_{\mathrm{tors}}) \geq 1$ and t a positive integer. We consider the set $M = M(K, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $\mathrm{ord}_{\mathfrak{q}}(v) = 0$ for all $v \in V$, and
- $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}] \mid t$.

This is a special case of the broader context considered by H.W. Lenstra [18]. If we take V to be generated by a single element, this element is called a *near-primitive root* modulo the primes $\mathfrak{q}$ satisfying the conditions. Over the rationals, these densities have previously been computed; see Wagstaff [35] and Moree [23].

If on the other hand we take $t = 1$, but V generated by multiple elements, this leads to higher rank analogues of Artin's conjecture. For $K = \mathbf{Q}$, this topic has been treated by Cangelmi and Pappalardi [6], and is covered in a way very similar to the approach in this chapter by Moree and Stevenhagen [24].

The work of Cooke and Weinberger [9] shows that the set $M(K, V, t)$ has a natural density under the appropriate generalized Riemann hypotheses.

First of all, note that the set of primes $\mathfrak{q}$ not satisfying the first condition is finite, since V is finitely generated. After all, it is sufficient to check this condition for a set of generators of V.

Following the same strategy as in Chapter 1, we will see that the second condition can also be translated to splitting conditions on radical extension fields of K.

Specifically, for a (rational) prime p, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t, and define the radical extensions

$$K^* \subset B_p = \langle K^*, \mu_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \rangle.$$

Here $\sqrt[p^{e(p)}]{V}$ denotes the group of all elements x in a fixed algebraic closure $\bar{K}$ of K that satisfy $x^{p^{e(p)}} \in V$. Let B be the abelian group generated by all B_p, and let $E = E(B)$ be its entanglement group with respect to the action of the absolute Galois group of K.

Theorem 5.1. *The entanglement group $E = E(B)$ of B is finite.*

As $A = \mathrm{Aut}_{K^*}(B)$ is naturally isomorphic to the product of all $A_p = \mathrm{Aut}_{K^*}(B_p)$ and E is finite, only a finite number of A_p have a non-trivial image in E. This ensures that the (a priori infinite) product in the correction factor formula below is in fact a finite product.

Theorem 5.2. *Assuming GRH, the set $M(K, V, t)$ has a natural density equal to*

$$C(K, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C(K, V, t)$ is a rational correction factor given by

$$C(K, V, t) = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

We prove these two main theorems in the following section.

In this generality, the results from Chapter 1 no longer suffice to give explicit expressions for E and $\chi(A_p)$. In the remainder of the chapter we will address these issues, using the theory from Chapters 2 and 4.

5.2 Proof of main theorems

In this section we will prove Theorems 5.1 and 5.2. As in the introduction, let K be a number field, $V \subset K^*$ a finitely generated subgroup with $\mathrm{rank}(V/V_{\mathrm{tors}}) \geq 1$ and t a positive integer. We will consider the set $M = M(K, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $\mathrm{ord}_{\mathfrak{q}}(v) = 0$ for all $v \in V$, and
- $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}] \mid t$.

First of all, note that the set of primes $\mathfrak{q}$ not satisfying the first condition is finite, since V is finitely generated and it is sufficient to check this condition for a

set of generators of V. We will therefore only consider primes $\mathfrak{q}$ satisfying the first condition in the remainder of this section.

For the second condition, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t. Then for a given prime $\mathfrak{q}$ of K, the index $[(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}]$ divides t if and only if for all (rational) primes p the power $p^{e(p)}$ does not divide the index.

For a given prime p with $\mathfrak{q} \nmid p$, we have

$$p^{e(p)} \mid [(\mathcal{O}_K/\mathfrak{q})^* : \bar{V}]$$

if and only if

$$p^{e(p)} \mid (N\mathfrak{q} - 1) \text{ and all elements of } \bar{V} \text{ are } p^{e(p)}\text{-th powers in } \mathcal{O}_K/\mathfrak{q}$$

if and only if

$$\mathfrak{q} \text{ splits completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}).$$

We conclude that, up to a finite number, the set of primes $M(K, V, t)$ we are interested in is the set of primes $\mathfrak{q}$ of K that do not split completely in any of the extensions $K \subset K_p = K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V})$ with $\mathfrak{q} \nmid p$.

As in Chapter 1, for each individual rational prime p the density of primes satisfying this condition has a simple expression given by the Chebotarëv density theorem:

$$1 - \frac{1}{[K_p : K]}.$$

Moreover, we can again combine these conditions at finitely many different primes p by looking at the splitting behaviour in the compositum.

If we take n to be a product of primes to consider, we define K_n to be the compositum of the fields K_p for the p dividing n. Also, we define G_n to be the Galois group $\mathrm{Gal}(K_n/K)$, and S_n as

$$S_n = \{\sigma \in G_n : \sigma\,|_{K_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

Chebotarëv implies that the set of primes $\mathfrak{q}$ of K that do not split completely in any of the p dividing n has a density equal to the ratio $\#S_n/\#G_n$.

The results of Cooke and Weinberger [9] also apply in this generality, and show that if we assume the Generalized Riemann Hypothesis (GRH) for the fields K_n, the primes in M have a natural density of

$$\lim_{n\to\infty} \frac{\#S_n}{\#G_n}.$$

In this limit the positive integers n are ordered by divisibility.

We will compute these quotients using the tools of radical group extensions and entanglement developed in the previous chapters. To that end, recall from the introduction in this chapter the definition of the radical extensions $K^* \subset B_p$:

$$B_p = \left\langle K^*, \mu_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \right\rangle.$$

Also, as before, for a positive integer n, we write B_n for the abelian group generated by all B_p for primes $p \mid n$, and B for the abelian group generated by *all* B_p.

A key ingredient in the derivation of the conjectured Artin densities in this chapter is the finiteness of the entanglement group of B with the action of the absolute Galois group of K, which is provided by Theorem 5.1 and which we prove here.

Proof of Theorem 5.1. Recall from Chapter 2 that $E(B)$ equals $E(B_{\mathrm{ab}})$, so it suffices to show that $E(B_{\mathrm{ab}})$ is finite.

Write w for the number of roots of unity in K, and define the integer n as the product of all primes p satisfying

$$p \mid w\Delta_{K/\mathbf{Q}}.$$

We aim to separate the n-part from the non-n-part of B_{ab}, which we will make precise below. To this end, note that B_{ab}/K^* is torsion, so it is the direct sum of its p-parts, for which we write $(B_{\mathrm{ab}})_p/K^*$. For a prime p, this subgroup $(B_{\mathrm{ab}})_p$ consists of the radicals in B_{ab} of p-power order mod K^*. In our current setting, those correspond exactly to the elements of B_{ab} that are also in B_p. Furthermore, by Proposition 2.23 we see that $B_p \cap B_{\mathrm{ab}}$ equals $(B_p)_{\mathrm{ab}}$. We conclude that

$$B_{\mathrm{ab}}/K^* = \bigoplus_{p \text{ prime}} (B_p)_{\mathrm{ab}}/K^*.$$

For any prime p, the group $(B_p)_{\mathrm{ab}}$ as defined in Section 2.5 is given by

$$(B_p)_{\mathrm{ab}} = \{x \in B_p : x^w \in \mu_{p^{e(p)}}K^*\}.$$

If p is a prime not dividing w, then we have that for any $x \in (B_p)_{\mathrm{ab}}$, the order of $\bar{x}$ in B_p/K^* is coprime with w. Therefore $x^w \in \mu_{p^{e(p)}}K^*$ is equivalent to $x \in \mu_{p^{e(p)}}K^*$. We obtain that

$$p \nmid w \Rightarrow (B_p)_{\mathrm{ab}} = \mu_{p^{e(p)}}K^*. \tag{5.3}$$

Now write $C_n = (B_n)_{\mathrm{ab}}$ and, since primes not dividing n in particular do not divide w, define C_n' as

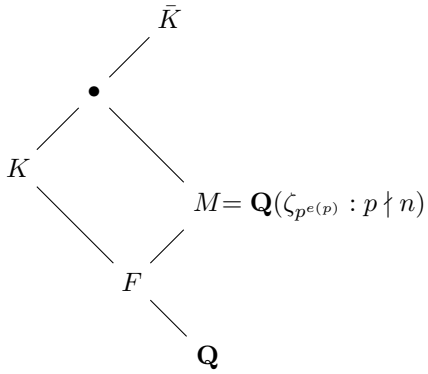
$$C_n' = \langle K^*, \zeta_{p^{e(p)}} : p \nmid n\rangle.$$

This allows us to decompose B_{ab} as a fibered sum over K^*

$$B_{\mathrm{ab}} = C_n \oplus_{K^*} C_n',$$

and $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ as

$$\mathrm{Aut}_{K^*}(B_{\mathrm{ab}}) = \mathrm{Aut}_{K^*}(C_n) \times \mathrm{Aut}_{K^*}(C_n'). \tag{5.4}$$



We write $M = \mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)$. Consider the following restriction map:

$$\varphi : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(M/\mathbf{Q}).$$

The invariant field F of the image of φ is given by the intersection $K \cap M$. The extension $F/\mathbf{Q}$ is then unramified at primes $p \nmid n$ since $K/\mathbf{Q}$ is unramified there. Also, $F/\mathbf{Q}$ is unramified at primes $p \mid n$ since $M/\mathbf{Q}$ is unramified there. We conclude that $F/\mathbf{Q}$ is unramified at all primes, so F is equal to $\mathbf{Q}$.

Therefore $\mathrm{Gal}(\bar{K}/K)$ maps surjectively to the Galois group of M over $\mathbf{Q}$, which is in turn naturally isomorphic to $\mathrm{Aut}_{K^*}(C_n')$.

Furthermore, the factor $\mathrm{Aut}_{K^*}(C_n)$ of $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ is finite, so the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{Aut}_{K^*}(B_{\mathrm{ab}})$ is of finite index. □

Since $E(B)$ is finite, we know there is an integer n such that $E(B)$ equals $E(B_n)$. In fact, with some extra work we can extend the strategy followed in the above proof to give an explicit sufficient condition for such n. While it is not strictly necessary for Theorem 5.2, we already give the proof here since it builds directly on the previous arguments.

Theorem 5.5. *Again write w for the number of roots of unity in K, and let n be a positive integer divisible by all primes p satisfying*

$$p \mid w\Delta_{K((B_w)_{\mathrm{ab}})/\mathbf{Q}}.$$

Then the natural map $E(B) \to E(B_n)$ is an isomorphism.

Proof. Define C_n and C_n' analogously to how they were defined in the proof of Theorem 5.1 above: $C_n = (B_n)_{\mathrm{ab}}$ and

$$C_n' = \langle K^*, \zeta_{p^{e(p)}} : p \nmid n \rangle.$$

Because of Equation 5.3, we can see that

$$K(C_n) = K((B_n)_{\mathrm{ab}}) = K((B_w)_{\mathrm{ab}}, \zeta_{p^{e(p)}} : p \mid n) = K((B_w)_{\mathrm{ab}}) \cdot \mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n).$$

All rational primes ramifying in $K((B_w)_{\mathrm{ab}})/\mathbf{Q}$ divide n by definition of n, and all rational primes ramifying in $\mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n)/\mathbf{Q}$ also divide n. We conclude that $K(C_n)/\mathbf{Q}$ is unramified outside of the primes dividing n.

For brevity, define $M = \mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)$. Proceeding entirely analogously to the reasoning in the proof of Theorem 5.1, the intersection $K(C_n) \cap M$ is now equal to $\mathbf{Q}$, and one can deduce from this that $\mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n))$ maps surjectively to the Galois group of M over $\mathbf{Q}$. This group is in turn naturally isomorphic to $\mathrm{Aut}_{K^*}(C_n')$.

We complete the proof assisted by the following diagram of abelian groups with exact rows and columns, where the first center vertical map is provided by Equation 5.4.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n)) & \longrightarrow & \mathrm{Gal}(K(B_{\mathrm{ab}})/K) & \longrightarrow & \mathrm{Gal}(K(C_n)/K) & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{K^*}(C_n') & \longrightarrow & \mathrm{Aut}_{K^*}(C_n) \times \mathrm{Aut}_{K^*}(C_n') & \longrightarrow & \mathrm{Aut}_{K^*}(C_n) & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & E(B_{\mathrm{ab}}) & \longrightarrow & E(C_n) & \longrightarrow & 0
\end{array}$$

Since the map $f : \mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n)) \to \mathrm{Aut}_{K^*}(C_n')$ is a surjection, the map from $E(B_{\mathrm{ab}}) \to E(C_n)$ is injective. It is also surjective, and since C_n is defined as $(B_n)_{\mathrm{ab}}$, this gives the equality claimed by the present Theorem. □

Now that we know the entanglement group is finite, we can proceed with the derivation of the conjectured density formula given by Theorem 5.2.

Proof of Theorem 5.2. The computation of the density with the correction factor in the form of a character sum can now continue as in Chapter 1.

Recall from the start of this section that we want to compute the limit

$$\lim_{n \to \infty} \frac{\#S_n}{\#G_n}.$$

To express this in terms of $A_n = \mathrm{Aut}_{K^*}(B_n)$ rather than in the Galois groups G_n, define T_n as follows.

$$T_n = \{\sigma \in A_n : \sigma|_{B_p} \neq \mathrm{id} \text{ for all } p \mid n\}.$$

This gives the equality $S_n = T_n \cap G_n$ inside A_n.

Now assume that n is an integer large enough to have $E = E(B) = E(B_n)$. (Refer to Theorem 5.5 for an explicit sufficient condition for this.) Then, because E is an abelian group, the characteristic function 1_{G_n} of G_n inside A_n is given by

$$1_{G_n}(s) = \frac{1}{\#E} \sum_{\chi \in E^\vee} \chi(s).$$

We apply this as follows.

$$\begin{aligned}\frac{\#S_n}{\#G_n} &= \frac{\#(T_n \cap G_n)}{\#G_n} = \frac{1}{\#E\#G_n}\sum_{s\in T_n} 1_{G_n}(s) \\ &= \frac{1}{\#A_n}\sum_{s\in T_n}\sum_{\chi\in E^\vee}\chi(s)\end{aligned}$$

We swap the order of the summations, and continue using the multiplicative structure of T_n.

$$\frac{\#S_n}{\#G_n} = \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{p|n}\frac{1}{\#T_p}\sum_{s\in T_p}\chi(s)$$

Since for all χ we have $\chi(1)=1$, we can change the inner sum to run over all of A_p.

$$\frac{\#S_n}{\#G_n} = \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{p|n}\frac{1}{\#A_p-1}\left(-1+\sum_{s\in A_p}\chi(s)\right)$$

If $\chi(A_p)$ is not trivial, then $\sum_{s\in A_p}\chi(s)$ equals 0. Otherwise, it equals $\#A_p$.

$$\begin{aligned}\frac{\#S_n}{\#G_n} &= \frac{\#T_n}{\#A_n}\sum_{\chi\in E^\vee}\prod_{\substack{p \text{ prime}\\ \chi(A_p)\neq 1}}\frac{-1}{\#A_p-1} \\ &= C(K,V,t)\prod_{p|n}\left(1-\frac{1}{\#A_p}\right)\end{aligned}$$

Since $C(K,V,t)$ does not depend on n, taking the limit of n to infinity gives the desired expression. □

5.3 Explicit density computations

In section 1.3 the exponent of the radical groups in question is squarefree, and we have used that to decompose B_{ab} as μW with μ a group of roots of unity and W a group of Kummer roots of elements of K. In the more general context of the present chapter, B_{ab} cannot be written in this way, but we can extend B with extra roots of unity to enable this. In Proposition 4.9 we saw how to do this over $\mathbf{Q}$, and the following Proposition gives the generalization for arbitrary number fields.

Proposition 5.6. *Let $C \subset D$ be a Galois radical extension such that D/C is of finite exponent dividing n. Let w be the order of $C[n]$, the n-torsion subgroup of C. If the order of $D[nw]$ equals nw, then D_{ab} can be decomposed as $D_{\mathrm{ab}} = \mu W$ with $\mu = D_{\mathrm{tors}}$ and $W = \{x \in D : x^w \in C\}$.*

Proof. We first recall the definition of D_{ab} from Section 2.5, adapted to the context of the proposition.

$$D_{\mathrm{ab}} = \{x \in D : x^w \in D_{\mathrm{tors}}C\}.$$

The inclusion $\mu W \subset D_{\mathrm{ab}}$ is clear, so we proceed with the opposite inclusion.

Suppose x is an element of D_{ab}, so we have $x^w \in \zeta C$ for an element $\zeta \in D_{\mathrm{tors}}$. We aim to show that we have $x \in \mu W$, or, equivalently, $x^w \in D^w_{\mathrm{tors}}C$. Since we know $x^n \in C$, we see $\zeta^{n/w} \in x^n C \subset C$, and we have $\zeta^{n/w} \in C_{\mathrm{tors}}$.

Now consider the quotient map $\pi : D_{\mathrm{tors}} \to D_{\mathrm{tors}}/C_{\mathrm{tors}}$. The restriction $\pi|_{D[n]}$ has kernel $C[n] = C[w]$ of order w, by definition of w and since all finite subgroups of D (and C) are cyclic. Since $D[n]$ has order n, the image $\pi(D[n])$ in $D_{\mathrm{tors}}/C_{\mathrm{tors}}$ is of order n/w and therefore equal to $(D_{\mathrm{tors}}/C_{\mathrm{tors}})[\frac{n}{w}]$.

Because we have $\zeta \in D_{\mathrm{tors}}$ and $\zeta^{n/w} \in C_{\mathrm{tors}}$, we see that ζC_{tors} is in $\pi(D[n])$, so we have $\zeta \in D[n]C_{\mathrm{tors}}$. Finally, since $\#D[nw] = nw$, we have that $D[n] = D[nw]^w \subset D^w_{\mathrm{tors}}$, and therefore $\zeta \in D^w_{\mathrm{tors}}C$. We now conclude that $x^w \in \zeta C \subset D^w_{\mathrm{tors}}C$, and therefore $x \in \mu W$. □

For a prime p, define $e'(p)$ and B'_p as

$$p^{e'(p)} = p^{e(p)} \cdot \#K^*[p^{e(p)}];$$
$$B'_p = \mu_{p^{e'(p)}} B_p = \left\langle K^*, \mu_{p^{e'(p)}}, \sqrt[p^{e(p)}]{V} \right\rangle.$$

For positive integers n, analogously to the definitions of B_n and K_n, we define the group B'_n as the group generated by all B'_p for $p \mid n$ and the field K'_n as $K(B'_n)$. The radical extensions $K^* \subset B'_n$ now satisfy the conditions of Proposition 5.6 by construction.

Example 5.7.

The following is a typical example in which B_{ab} is not generated by roots of unity and Kummer roots, but B'_{ab} is. Let l be a rational prime, and let ζ_l be a primitive l-th root of unity in a fixed algebraic closure $\bar{\mathbf{Q}}$. Consider the case $K = \mathbf{Q}(\zeta_l)$, $V = \langle 2^l \zeta_l \rangle$, $t = l$.

Then we see that B_l is given by

$$B_l = \left\langle K^*, \zeta_{l^2}, \sqrt[l^2]{2^l \zeta_l} \right\rangle.$$

If we choose elements $\sqrt[l]{2}$ and ζ_{l^3} inside $\bar{K}$, then B_l contains an element $x = \zeta_{l^3}\sqrt[l]{2}$. This element x is contained in B_{ab}, since x^l is contained in $\mu_{l^2}K^*$. Since $\sqrt[l]{2}$ is itself a Kummer root, but ζ_{l^3} cannot be written as a Kummer root times a root of unity inside B_l, we can conclude that x cannot be written in this way, and B_{ab} cannot be decomposed as a subgroup of roots of unity and a subgroup of Kummer roots.

The situation changes when we extend B_l to B'_l as above:

$$B'_l = \left\langle K^*, \zeta_{l^3}, \sqrt[l^2]{2^l \zeta_l} \right\rangle.$$

While x is also an element of B'_{ab}, in this case we clearly do obtain x as a product of a Kummer root $\sqrt[l]{2}$ times a root of unity ζ_{l^3} inside B'_l.

Finally define B' as the group generated by all B'_p, and $E' = E(B')$ as its entanglement group. Besides deriving E from E', and then evaluating the correction factor formula from Theorem 5.2, it is also possible to directly compute the correction factor from E'.

To this end, consider the automorphism group $\mathrm{Aut}_B(B')$. Since B' is generated by a single root of unity that is a Kummer radical over B, the group $\mathrm{Aut}_B(B')$ is cyclic. Let σ be its generator. If we then write $A'_p = \mathrm{Aut}_{K^*}(B'_p)$, the following theorem gives an expression for the correction factor.

Theorem 5.8. *The correction factor $C(K, V, t)$ defined in Theorem 5.2 is equal to*

$$\sum_{\substack{\chi \in E'^{\vee} \\ \chi(\bar{\sigma})=1}} \prod_{\substack{p \text{ prime} \\ \chi(A'_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

Proof. The equivalence of this formula and the one from Theorem 5.2 follows directly from these two claims:

1. $E^{\vee}$ is equal to $\{\chi \in E'^{\vee} : \chi(\bar{\sigma}) = 1\}$;
2. For $\chi \in E^{\vee} \subset E'^{\vee}$ we have $\chi(A'_p) = 1 \Leftrightarrow \chi(A_p) = 1$.

We prove them in order. For the first claim, note that the kernel of the restriction map $\mathrm{Aut}_{K^*}(B') \to \mathrm{Aut}_{K^*}(B)$ is generated by σ. This implies that the kernel of the induced (surjective) map $E(B') \to E(B)$ is generated by $\bar{\sigma}$. Identifying $E(B)$ with $E(B')/\langle\bar{\sigma}\rangle$ then shows that $E^{\vee}$ consists of the characters in $E'^{\vee}$ that are trivial on $\langle\bar{\sigma}\rangle$, as claimed.

For the second claim, let χ be a character of E, where we again consider $E^{\vee}$ as a subgroup of $E'^{\vee}$. Recall that we can factor A' as $\prod_p A'_p$ and A as $\prod_p A_p$. This leads to the following commutative diagram.

$$\begin{array}{ccccc} A'_p & \twoheadrightarrow & A_p & & \\ \downarrow & & \downarrow & & \\ A' & \twoheadrightarrow & A & \xrightarrow[\chi]{} & \mathbf{C}^* \end{array}$$

The group of interest $\chi(A'_p)$ is the image of the composition

$$A'_p \hookrightarrow A' \twoheadrightarrow A \xrightarrow{\chi} \mathbf{C}^*.$$

As the commutativity of the diagram shows, this composed map factors via A_p, so we see that $\chi(A_p) = 1 \Rightarrow \chi(A'_p) = 1$. The opposite implication is trivial, proving the second claim. □

Example 5.9.

We illustrate this theorem, and the methods in this chapter in general, by computing an Artin density (assuming GRH).

Take $K = \mathbf{Q}(\zeta_3)$, and $x = 8\zeta_3$, and $V = \langle x \rangle$, and $t = 3$. In Example 5.7 we saw that we need to enlarge B with extra roots of unity in this case. Proposition 5.6 implies that adding 4th and 27th roots of unity is sufficient, but in this case only adding 27th roots already suffices, as we shall see.

Define B'_p for primes p as

$$B'_p = \langle K^*, \zeta_p, \sqrt[p]{x} \rangle \text{ if } p \neq 3, \text{ and}$$

$$B'_3 = \langle K^*, \zeta_{27}, \sqrt[9]{x} \rangle = \langle K^*, \zeta_{27}, \sqrt[3]{2} \rangle.$$

By Theorem 5.5, only the primes 2 and 3 affect entanglement, and $E(B') = E(B'_6) = E((B'_6)_{\mathrm{ab}})$. In fact, B'_6 is itself equal to $(B'_6)_{\mathrm{ab}}$ since it is generated by roots of unity and Kummer roots.

We have that

$$B'_2 = \langle K^*, \zeta_2, \sqrt[2]{8\zeta_3} \rangle = \langle K^*, \zeta_3\sqrt{2} \rangle; \text{ and}$$

$$B'_6 = \langle K^*, \zeta_{27}, \sqrt[3]{2}, \sqrt{2} \rangle.$$

We now take $\mu = \mu_{27}$ and $W = \langle K^*, \sqrt[6]{2} \rangle$. We then obtain $B'_6 = \mu W$. Defining G_W to be the absolute Galois group of $K(W) = K(\sqrt[6]{2})$, the expression for the entanglement group we obtain from Corollary 2.31, with $C = W$ and $D = \mu$, is

$$E' = \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W).$$

Since we have $\mu \cap W = \mu_3$ and $K(W) \cap \mathbf{Q}(\mu)$ equals $\mathbf{Q}(\mu_3)$, we see that E' is trivial.

For all primes $p \neq 3$, we have $\#A_p = p(p-1)$. For $p = 3$ on the other hand, we get $\#A_3 = 9$.

Assuming GRH, we then arrive at a density of

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{16}{15} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

Example 5.10.

In the previous example, we took the case from Example 5.7 with $l = 3$. In this example we take $l = 2$, so we get $K = \mathbf{Q}$, and $x = -4$, and $V = \langle x \rangle$, and $t = 2$.

As before, we need to add extra roots of unity: in this case 8th roots.

Define B'_p for primes p as

$$B'_p = \langle K^*, \zeta_p, \sqrt[p]{x} \rangle \text{ if } p \neq 2, \text{ and}$$

$$B'_2 = \langle K^*, \zeta_8, \sqrt[4]{x} \rangle = \langle K^*, \zeta_8, \sqrt{2} \rangle.$$

By Theorem 5.5, only the prime 2 affects entanglement, and $E(B') = E(B'_2) = E((B'_2)_{\mathrm{ab}})$. If we define $\mu = \mu_8$ and $W = \langle \mathbf{Q}^*, \sqrt{2} \rangle$, then B'_2 equals μW, so $(B'_2)_{\mathrm{ab}}$ equals B'_2.

Define G_W to be the absolute Galois group of $K(W) = \mathbf{Q}(\sqrt{2})$. We then again get the following expression for $E(B')$ from Corollary 2.31, again with $C = W$ and $D = \mu$.

$$E' = \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W).$$

We have $\mu \cap W = \{\pm 1\}$ and $K(W) \cap \mathbf{Q}(\mu)$ equals $\mathbf{Q}(\sqrt{2})$, so the image of G_W in $\mathrm{Aut}(\mu) = \mathrm{Aut}(\mu_8)$ equals $\langle \zeta_8 \mapsto \zeta_8^{-1} \rangle$.

So E' is an entanglement group of order 2. Let χ be the non-trivial character in $E'^{\vee}$.

To compute the correction factor, we use Theorem 5.8. First, take σ to be the generator of $\mathrm{Aut}_B(B')$, which sends ζ_8 to ζ_8^5. Then the image of σ in E' is not trivial, since it is not in the image of G_W.

Since $E(B') = E(B'_2)$, we see that A'_2 can only map surjectively to E', so $\chi(A'_2)$ is not trivial.

Since $\#A'_2$ equals 4, this gives a correction factor of

$$1 + \frac{-1}{3} = \frac{2}{3}.$$

For all odd primes, we have $\#A_p = p(p-1)$, so, assuming GRH, we then obtain the density

$$\frac{2}{3} \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{2}{3} \cdot \frac{3}{2} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) = \text{Artin's constant}.$$

We conclude this chapter with two remarks on different generalizations of Artin densities.

One possible generalization is adding a congruence condition to the primes $\mathfrak{q}$ considered. (See Moree [21], for $K = \mathbf{Q}$.) This can be translated to a condition on $\mathrm{Frob}_{\mathfrak{q}}$ in a ray class field F over K. One can in fact handle such Frobenius conditions for an arbitrary Galois extension F of K, cf. Lenstra [18]. If we extend the radical group B considered with extra radicals to include the radical part of F, we get extra

conditions on $\mathrm{Frob}_{\mathfrak{q}}$ inside the automorphism groups A_n, which in turn lead to a smaller T_n.

The resulting density does not necessarily permit a character sum formula using the methods described in this chapter, since the smaller group T_n does not necessarily factor as a product $\prod_{p|n} T_p$. Also, if F is itself not generated by radicals, then the restriction of the map $\mathrm{Gal}(F/K) \to \mathrm{Gal}(F \cap K(B)/K)$ to a set $C \subset \mathrm{Gal}(F/K)$ closed under conjugation will not in general have fibers of the same size, which will require extra administration.

For $K = \mathbf{Q}$ and a congruence condition modulo n, the ray class field F is in fact equal to $\mathbf{Q}(\zeta_n)$. In this case, the two difficulties described above do not occur, and we are able to get a character sum formula for the density. For details, we refer to [20].

In this chapter we have considered the set $M = M(K, x, t)$ of primes $\mathfrak{q}$ of K for which an element $x \in K^*$ generates a subgroup of $(\mathcal{O}_K/\mathfrak{q})^*$ of index dividing t. Moree [23] considers the set of primes $M' = M'(\mathbf{Q}, x, t)$ where this index is *equal* to t. The density of M' can be derived from $M(K, x, t')$ for all $t' \mid t$ using Möbius inversion, but there is a more direct way to use the theory from this chapter to compute it, which is also described in detail for a related method by Lenstra, Moree and Stevenhagen [20].

For a prime p, we define $C_p = \langle K^*, \zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V} \rangle$ and also the subgroup $C'_p = \langle K^*, \zeta_{p^{e(p)-1}}, \sqrt[p^{e(p)-1}]{V} \rangle \subset C_p$. For a positive integer n we define from these the groups C_n and C'_n generated by C_p respectively C'_p for all $p \mid n$. Define the automorphism groups $A_n = \mathrm{Aut}_{K^*}(C_n)$ and $A'_n = \mathrm{Aut}_{C'_n}(C_n) \subset A_n$. Also let G_n be the Galois group $\mathrm{Gal}(K(C_n)/K)$ and E_n the entanglement group of C_n with the action of G_n. Theorem 5.1 applies to this situation, and implies there is a limit entanglement group E such that if n is divisible by all of a finite set of critical primes, E_n is equal to E.

Theorem 5.11. *Assuming GRH, the set $M'(K, V, t)$ has a natural density equal to*

$$C'(K, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C'(K, V, t)$ is a rational correction factor given explicitly by

$$C'(K, V, t) = \left(\prod_{p|t} \frac{\#A'_p - 1}{\#A_p - 1}\right) \left(\sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A'_p) \neq 1}} \frac{-1}{\#A'_p - 1}\right).$$

Proof. Using the notation from this chapter, the main difference with Theorem 5.2 is that for a prime p, the set S_p of allowed Frobenius elements at p will no longer be $G_p \setminus \{1\}$. The condition that led to this at p for index dividing t was:

$$\mathfrak{q} \text{ does not split completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}).$$

In the case where we are interested in index *equal* to t, this becomes:

$$\begin{gathered}\mathfrak{q} \text{ does not split completely in } K \subset K(\zeta_{p^{e(p)}}, \sqrt[p^{e(p)}]{V}), \text{ and} \\ \mathfrak{q} \textit{ does} \text{ split completely in } K \subset K(\zeta_{p^{e(p)-1}}, \sqrt[p^{e(p)-1}]{V}).\end{gathered}$$

Using C_p and C_p' as defined above the Theorem, this leads to the condition at p that $\mathrm{Frob}_{\mathfrak{q}}$ in $\mathrm{Gal}(K(C_p)/K)$ is an element of the subset $\mathrm{Gal}(K(C_p)/K(C_p')) \setminus \{1\}$. Translating this to the context of automorphisms of abelian groups, this gives us:

$$\frac{\#(\mathrm{Gal}(K(C_p)/K(C_p')) \setminus \{1\})}{\#\mathrm{Gal}(K(C_p)/K)} = \frac{\#((\mathrm{Aut}_{C_p'}(C_p) \setminus \{1\}) \cap \mathrm{Gal}(K(C_p)/K))}{\#\mathrm{Gal}(K(C_p)/K)}.$$

From this expression one can derive a character sum formula for the density, analogously to the approach followed in the proof of Theorem 5.2 in Section 5.2. To this end, recall $A_p' = \mathrm{Aut}_{C_p'}(C_p)$ and define

$$T_n = \{\sigma \in A_n : \sigma|_{B_p} \in A_p' \setminus \{1\} \text{ for all primes } p \mid n\}.$$

We then get the following computation, if we assume all primes dividing t also to divide n.

$$\begin{aligned}\frac{\#(T_n \cap G_n)}{\#G_n} &= \frac{1}{\#E\#G_n} \sum_{s \in T_n} 1_{G_n}(s) = \frac{1}{\#A_n} \sum_{s \in T_n} \sum_{\chi \in E^\vee} \chi(s) \\ &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \frac{1}{\#T_p} \sum_{s \in T_p} \chi(s)\end{aligned}$$

Since for all χ we have $\chi(1) = 1$, we can change the inner sum to run over all of A_p'.

$$\frac{\#(T_n \cap G_n)}{\#G_n} = \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{p \mid n} \frac{1}{\#A_p' - 1} \left(-1 + \sum_{s \in A_p'} \chi(s) \right)$$

If $\chi(A_p')$ is not trivial, then $\sum_{s \in A_p'} \chi(s)$ equals 0. Otherwise, it equals $\#A_p'$.

$$\begin{aligned}\frac{\#(T_n \cap G_n)}{\#G_n} &= \frac{\#T_n}{\#A_n} \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p') \neq 1}} \frac{-1}{\#A_p' - 1} \\ &= \left(\prod_{p \mid n} \left(1 - \frac{1}{\#A_p} \right) \right) \left(\prod_{p \mid t} \frac{\#A_p' - 1}{\#A_p - 1} \right) \left(\sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p') \neq 1}} \frac{-1}{\#A_p' - 1} \right)\end{aligned}$$

Only the first product now depends on n, and taking the limit of n to infinity then gives the density of $M'(K, V, t)$, assuming GRH. We conclude that with the correction factor $C'(K, V, t)$ defined in the Theorem, we get the desired expression for the density. □