REDUCTIONS OF ALGEBRAIC INTEGERS II

ANTONELLA PERUCCA

ABSTRACT. Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. Fix some positive integer m, and consider the set of primes $\mathfrak{p}$ of K satisfying the following condition: the reduction of G modulo $\mathfrak{p}$ is well–defined and has size coprime to m. We show that the natural density of this set is a computable rational number by reducing to the case where m is prime, case which has been treated in the previous work *Reductions of algebraic integers* (joint with Christophe Debry, J. Number Theory, 2016).

1. INTRODUCTION

This paper is the continuation of [1] by Christophe Debry and the author, therefore we refer to this other work for the history of the problem and for further references. Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. Up to excluding finitely many primes $\mathfrak{p}$ of K, we always assume that the reduction of G modulo $\mathfrak{p}$ is well-defined. Fix some prime number ℓ, and consider the set of primes $\mathfrak{p}$ of K satisfying the following condition: the reduction of G modulo $\mathfrak{p}$ has size coprime to ℓ. In [1] it is proven that this set admits a natural density, which is a computable rational number.

We now deal with the generalization that consists of replacing ℓ by some positive integer m, which we may as well suppose to be square-free. So our aim is to show that the following natural density is a well-defined rational number, and how one can compute it:

$$D_{K,G,m} := \operatorname{dens}\{\mathfrak{p} : \operatorname{ord}(G \bmod \mathfrak{p}) \text{ is coprime to } m\}.$$

The condition on $\mathfrak{p}$ means that for every prime factor ℓ of m the group $(G \bmod \mathfrak{p})$ has order coprime to ℓ. We are thus requiring simultaneous conditions related to different prime numbers. The main question is whether those conditions are independent, which would heuristically give

$$D_{K,G,m} = \prod_{\ell} D_{K,G,\ell}\,. \tag{1}$$

Note that we may suppose that G is torsion–free because roots of unity of order coprime to m do not matter for the density while if G contains a root of unity of order not coprime to m then the order of $(G \bmod \mathfrak{p})$ is also not coprime to m for almost all $\mathfrak{p}$.

Write K_x for the cyclotomic extension of K obtained by adding the x-th roots of unity. The method of [1] relies on the fact that the Kummer extension $K_{\ell^n}(\sqrt[\ell^n]{G})$ over K_{ℓ^n} has maximal degree ℓ^{rn} (where r is the rank of G), unless the elements of G have some divisibility property

2000 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11R18, 11R21, 11Y40.
Key words and phrases. Number field, algebraic integer, reduction, Kummer theory, density.

in $K^\times$. There is one small exception for the case $\ell = 2$, which is related to the fact that the cyclotomic extension K_8/K need not to be cyclic. In short [1] relied on the fact that the Kummer extensions related to ℓ have nothing to do with the cyclotomic extensions related to ℓ.

However, Kummer extensions may in general be contained in cyclotomic extensions because if ℓ, ℓ' are distinct prime numbers then the field $K_{\ell'}$ could contain a cyclic extension of K of degree a power of ℓ (see Section 3). It is exactly this interplay between cyclotomic and Kummer extensions that we must treat delicately in the present paper.

We prove in Theorem 9 that the density $D_{K,G,m}$ can be expressed as an infinite sum involving splitting conditions in cyclotomic-Kummer extensions of K. Then we show that the density is always a computable rational number. In fact by Theorem 15 we know that $D_{K,G,m}$ can be written in terms of densities related to one single prime number, and those are known from [4] (for G of rank 1) and from [1] (for G of arbitrary rank).

In Theorem 11 we show that the product formula (1) is true if the following condition holds for every $n \geqslant 1$ and for every prime divisor ℓ of m: *the extensions $K_{\ell^n, \frac{m}{\ell}}$ and $K_{\ell^n}(\sqrt[\ell^n]{G})$ are linearly disjoint over K_{ℓ^n}.*

The product formula (1) is then true under the assumption $K_m = K$ (see Corollary 12) or under the assumption that m is odd and that $K_\ell \neq K$ holds for every prime divisor ℓ of m (see Proposition 13). The last condition holds in particular (if m is odd) for $\mathbb{Q}$ and for every quadratic field, unless $K = \mathbb{Q}(\zeta_3)$ and 3 divides m. We also answer in the negative the question whether (1) holds for m odd, see Example 18.

We have tested our results in several explicit examples, for which an approximated density (by considering the primes of small norm) has been computed with Sage [6].

2. Preliminaries on the Chebotarev Density Theorem

Let K be a number field, and call P_K the set of primes of K. For $\mathfrak{p} \in P_K$ we denote by $N(\mathfrak{p})$ the cardinality of the residue field at $\mathfrak{p}$. If $\Gamma \subseteq P_K$ and the following limit exists, we call it the Dirichlet density of Γ:

$$\mathrm{dens}_{Dir}(\Gamma) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \Gamma} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in P_K} N(\mathfrak{p})^{-s}}\,.$$

If the following limit exists, we call it the natural density of Γ:

$$\mathrm{dens}(\Gamma) = \lim_{n \to +\infty} \frac{\#\{\mathfrak{p} \in \Gamma : N(\mathfrak{p}) \leqslant n\}}{\#\{\mathfrak{p} \in P_K : N(\mathfrak{p}) \leqslant n\}}\,.$$

By the upper and lower density we respectively mean the limit inferior and superior: these exist and if they coincide then the density exists. Note that if the natural density exists then the Dirichlet density also exists and they coincide (however there are sets having a Dirichlet density and for which the natural density does not exist).

The following general result will allow us (in certain cases) to extend the base field:

Proposition 1. *Let K be a number field and let L be a finite Galois extension of K. Let Γ be a set of primes of K that split completely in L. Call Γ_L the set of primes of L which lie over*

the primes in Γ. *If* Γ_L *has a Dirichlet density then the same holds for* Γ *and we have*

$$\mathrm{dens}_{Dir}(\Gamma) = [L:K]^{-1} \cdot \mathrm{dens}_{Dir}(\Gamma_L)\,.$$

Proof. Call S the set of primes of K which split completely in L and call S_L the set of primes of L which lie over the primes of S. If $\mathfrak{p} \in S$ and $\mathfrak{q}$ is one of the $[L:K]$ primes of S_L lying over it then $\mathfrak{p}$ and $\mathfrak{q}$ have the same norm. On one hand the Chebotarev's Density Theorem gives

$$[L:K]^{-1} = \mathrm{dens}_{Dir}(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P_K} N(\mathfrak{p})^{-s}}$$

and on the other hand we know

$$1 = \mathrm{dens}_{Dir}(S_L) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{q}\in S_L} N(\mathfrak{q})^{-s}}{\sum_{\mathfrak{q}\in P_L} N(\mathfrak{q})^{-s}} = [L:K] \cdot \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{q}\in P_L} N(\mathfrak{q})^{-s}}$$

so we deduce

$$\lim_{s\to 1^+} \sum_{\mathfrak{p}\in P_K} N(\mathfrak{p})^{-s} = \lim_{s\to 1^+} \sum_{\mathfrak{q}\in P_L} N(\mathfrak{q})^{-s}\,.$$

We conclude because we have

$$\frac{\sum_{\mathfrak{p}\in\Gamma} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P_K} N(\mathfrak{p})^{-s}} = [L:K]^{-1} \cdot \frac{\sum_{\mathfrak{q}\in\Gamma_L} N(\mathfrak{q})^{-s}}{\sum_{\mathfrak{p}\in P_K} N(\mathfrak{p})^{-s}} \quad \xrightarrow{s\to 1^+} \quad [L:K]^{-1} \cdot \mathrm{dens}_{Dir}(\Gamma_L)\,.$$

□

The following result and its corollary are variants of the Chebotarev Density Theorem, where several field extensions are considered:

Theorem 2. *Let* K *be a number field. If* $F_1, \ldots, F_n$ *are linearly disjoint finite Galois extensions of* K *then the set consisting of the primes of* K *that do not split completely in any of those extensions has a natural density, and this equals*

$$\prod_{i=1}^{n} \Big(1 - \frac{1}{[F_i:K]}\Big)\,.$$

Proof. Call Γ the set of the primes of K that do not split completely in any of the extensions $F_1, \ldots, F_n$. By working with the compositum $F := F_1 \cdots F_n$ (and excluding the finitely many primes that ramify in F) we can interpret Γ as the primes of K whose F/K-Frobenius conjugacy class is contained in a certain conjugacy-invariant subset of $\mathrm{Gal}(F/K)$. The existence of the natural density for Γ then follows from the Chebotarev Density Theorem.

We prove the formula in the statement by induction on n, the case $n = 1$ being clear by the Chebotarev Density Theorem. For the induction step consider linearly disjoint extensions $F_1, \ldots, F_{n+1}$ of K and write for convenience $L = F_{n+1}$.

By the inductive hypothesis we know $\mathrm{dens}(\Gamma) = \prod_{i=1}^{n}(1 - [F_i:K]^{-1})$. Write $\Gamma' \subseteq \Gamma$ for the subset of the primes that split completely in L and let Γ'_L be the set of primes of L lying over the primes in Γ'. One can argue as above and show that Γ' has a natural density.

Any set consisting of primes of L that lie over primes of K which do not split completely in L has Dirichlet density 0. The fields $LF_1, \ldots, LF_n$ are linearly disjoint over L and Γ'_L consists

of the primes of L that do not split completely in any of those fields (up to a set of primes of L of Dirichlet density 0). So by the inductive hypothesis we get

$$\mathrm{dens}_{Dir}(\Gamma'_L) = \prod_{i=1}^{n} \Big(1 - \frac{1}{[LF_i : L]}\Big) = \prod_{i=1}^{n} \Big(1 - \frac{1}{[F_i : K]}\Big).$$

By Proposition 1 we then have

$$\mathrm{dens}_{Dir}(\Gamma') = [L : K]^{-1} \cdot \mathrm{dens}_{Dir}(\Gamma'_L) = \frac{1}{[F_{n+1} : K]} \cdot \prod_{i=1}^{n} \Big(1 - \frac{1}{[F_i : K]}\Big).$$

Since $\Gamma' \subseteq \Gamma$ and these two sets have a natural density then the same holds for their difference and we conclude the induction step because we have:

$$\mathrm{dens}(\Gamma \setminus \Gamma') = \mathrm{dens}(\Gamma) - \mathrm{dens}(\Gamma') = \prod_{i=1}^{n+1} \Big(1 - \frac{1}{[F_i : K]}\Big).$$

□

Corollary 3. *Let K be a number field, and let L be a finite Galois extension of K. If $F_1, \dots, F_n$ are linearly disjoint finite Galois extensions of L then the set of primes of K that split completely in L and do not split completely in any of the extensions $F_1, \dots, F_n$ has a natural density, and this equals*

$$[L : K]^{-1} \cdot \prod_{i=1}^{n} \Big(1 - \frac{1}{[F_i : L]}\Big).$$

Proof. For the existence of the natural density we may apply the Chebotarev Density Theorem. To prove the formula, it suffices to combine Proposition 1 and Theorem 2 (applied to L). □

3. Cyclotomic and Kummer extensions

Let K be a number field, and fix some algebraic closure $\bar{K}$. We write K_x for the cyclotomic extension of K obtained by adding the x-th roots of unity. If ℓ is a prime number, we use the notation K_{ℓ^∞} to denote the union of the fields K_{ℓ^n} for $n \geqslant 1$.

If G is a finitely generated subgroup of $K^\times$, we also write $K_x(\sqrt[y]{G})$ for the extension of K_x obtained by adding all elements of $\bar{K}$ whose y-th power belongs to G.

We make use of the following result of Schinzel:

Theorem 4 (Schinzel [5, Thm. 2], with an alternative proof in [3, 7])**.** *Let K be a number field, and let $a \in K^\times$. For $n \geqslant 1$ the extension $K_n(\sqrt[n]{a})/K$ is abelian if and only if $a^t = b^n$ holds for some $b \in K^\times$ and for some divisor t of n satisfying $K = K_t$.*

We now recall the definition of *strongly ℓ-indivisible* element. In the remaining of the section we use such elements to investigate the Kummer extensions.

Definition 5. *Let K be a number field, and ℓ a prime number. We say that $a \in K^\times$ is* strongly ℓ-indivisible *if, for every root of unity $\xi \in K$, $a\xi$ has no ℓ-th roots in K.*

Theorem 6. *Consider integers $n, d \geqslant 1$ such that ℓ^d divides n. If the condition*

$$K_n(\sqrt[\ell^d]{a}) = K_n$$

holds for some strongly ℓ-indivisible $a \in K^\times$ then we have $K_{\ell^d} = K$ and there is some odd prime factor q of n such that ℓ^d divides $[K_q : K]$, unless $\ell = 2$ and $K \neq K_4$ and $d = 1$ and $K(\sqrt{a}) \subseteq K_{2^\infty}$.

Proof. We know that the field $K_{\ell^d}(\sqrt[\ell^d]{a})$, which is contained in K_n by assumption, is an abelian extension of K. Thus by Theorem 4 we have $a^{\ell^e} = b^{\ell^d}$ for some $b \in K^\times$ and for some $e \geqslant 0$ satisfying $K_{\ell^e} = K$. Since a is strongly ℓ-indivisible, we must have $d \leqslant e$ and hence $K_{\ell^d} = K$ holds.

Again since a is strongly ℓ-indivisible we know by [4, Theorems 11 and 13] that unless $\ell = 2$ and $K \neq K_4$ and $d = 1$ and $K(\sqrt{a}) \subseteq K_{2^\infty}$ we must have

$$[K_{\ell^\infty}(\sqrt[\ell^d]{a}) : K_{\ell^\infty}] = \ell^d\,.$$

Let this be the case, and denote by n' the product of all odd prime factors q of n distinct from ℓ. We deduce that the extension $K_{n'}/K$ contains a cyclic subextension of degree ℓ^d. Since $\mathrm{Gal}(K_{n'}/K)$ is the product of the groups $\mathrm{Gal}(K_q/K)$, at least one of these has exponent divisible by ℓ^d and hence ℓ^d divides $[K_q : K]$. □

Theorem 7. *Consider integers $n, d \geqslant 1$ such that ℓ^d divides n. If $K_{\ell^d} = K$ holds, and if ℓ^d divides $[K_q : K]$ for some odd prime factor q of n, then there is some strongly ℓ-indivisible $a \in K^\times$ satisfying (for all choices of the ℓ^{d+1}-th root)*

$$K_n(\sqrt[\ell^d]{a}) = K_n \qquad \text{and} \qquad \sqrt[\ell^{d+1}]{a} \notin K_n\,.$$

Proof. By assumption there is a cyclic extension C of K of degree ℓ^d contained in K_q. Since $K_{\ell^d} = K$ holds, there is some $c \in K^\times$ satisfying $C = K(\sqrt[\ell^d]{c})$. The element c is strongly ℓ-indivisible because the field $K(\sqrt[\ell]{c})$ is contained in K_q but not in K and hence it is not contained in K_{ℓ^∞}. The field C is contained in K_n, so we are done if $\sqrt[\ell^{d+1}]{c} \notin K_n$ holds for all choices of the ℓ^{d+1}-th root. If not, take $b \in K^\times$ such that $K(\sqrt[\ell]{b})$ is not contained in $K_{n\ell}$: such an element exists because $K_{n\ell}$ contains only finitely many subextensions of degree ℓ while $K^\times/K^{\times\ell}$ is infinite. Then cb^{ℓ^d} is strongly ℓ-indivisible, and we have $\sqrt[\ell^d]{cb^{\ell^d}} \in K_n$. By construction $\sqrt[\ell^{d+1}]{cb^{\ell^d}}$ is not contained in K_n for any choice of the ℓ^{d+1}-th root. □

4. Prescribed torsion in the reductions

The aim of this section is computing the density of reductions that have some prescribed valuations for the size of the multiplicative group of the residue field.

Let $m \geqslant 2$ be a square-free integer, and write $m = \ell_1 \cdots \ell_f$ as a product of prime numbers. We define the m-adic valuation as the f-tuple of the ℓ_i-adic valuations. We then consider f-tuples of non-negative integers

$$A = (a_1, \ldots, a_f)\,.$$

We write $A+1$ if we increase all entries by 1 and S_iA if we increase only the i-th entry by 1 i.e. $(S_iA)_j = a_j$ for $j \neq i$ and $(S_iA)_i = a_i + 1$. In particular we have $A + 1 = S_1 \cdots S_f A$. We also define

$$m^A := \prod_{i=1}^{f} \ell_i^{a_i}$$

Let K be a number field, and let $\mathfrak{p}$ be a prime of K. If we have for the m-adic valuation $v_m(\#k_\mathfrak{p}^\times) = A$, then this means that $v_{\ell_i}(\#k_\mathfrak{p}^\times) = a_i$ holds for every $i = 1, \ldots, f$. In other words, we can write $\#k_\mathfrak{p}^\times = m^A \cdot m'$ with m' coprime to m.

We first write down a formula for the natural density of the set of primes $\mathfrak{p}$ of K such that the m-adic valuation of $\#k_\mathfrak{p}^\times$ equals A. We may neglect the finitely many primes of K that ramify in $K_{m^{A+1}}$ so we are looking for the primes that split completely in K_{m^A} and that for every i do not split completely in $K_{m^{S_iA}}$.

Proposition 8. *The set of primes $\mathfrak{p}$ of K such that the m-adic valuation of $k_\mathfrak{p}^\times$ equals A has a natural density, which we call δ_{K,m^A}. Define $\delta_{K,\ell_i^{a_i}}$ similarly by requiring the ℓ_i-adic valuation of $k_\mathfrak{p}^\times$ to be a_i. We then have*

$$\delta_{K,m^A} = \prod_{i=1}^{f} \left([K_{\ell^{a_i}} : K]^{-1} - [K_{\ell^{a_i+1}} : K]^{-1} \right) = \prod_{i=1}^{f} \delta_{K,\ell_i^{a_i}} .$$

Proof. The existence of the natural density follows from Corollary 3. The second equality is clear by the Chebotarev Density Theorem because for $\delta_{K,\ell_i^{a_i}}$ we count the primes of K that split completely in $K_{\ell_i^{a_i}}$ and that do not split completely in $K_{\ell_i^{a_i+1}}$.

For δ_{K,m^A} we count the primes of K that split completely in $L := K_{m^A}$ and that for every $i = 1, \ldots, f$ do not split completely in $K_{m^{S_iA}}$. By Corollary 3 we get

$$\delta_{K,m^A} = [L : K]^{-1} \cdot \prod_{i=1}^{f} \left(1 - [K_{m^{S_iA}} : L]^{-1} \right) = [L : K]^{-1} \cdot \prod_{i=1}^{f} \left(1 - [K_{\ell^{a_i+1}} : K_{\ell^{a_i}}]^{-1} \right).$$

We conclude because we have $[L : K] = \prod_{i=1}^{f} [K_{\ell^{a_i}} : K]$. □

5. General formulas for the density

We first investigate the existence of the density under consideration and write it as an infinite sum (according to the size of the multiplicative group of the residue field).

Let K be a number field, let G be a finitely–generated and torsion–free subgroup of $K^\times$, and let $m \geqslant 2$ be a square–free integer. We make use of the notation introduced in the beginning of Section 4. We always tacitly exclude the finitely many primes that ramify in the cyclotomic-Kummer extensions that we consider. Indeed there are only finitely many primes of K that ramify in $K_{m^n}(\sqrt[m^n]{G})$ for some $n \geqslant 1$, see [2, Lemma C.1.7].

Theorem 9. *Let $\Gamma_{K,G,m}$ be the set of primes of K for which the reduction of G has order coprime to m. Let Γ_{K,G,m^A} be the set of primes of K that split completely in $K_{m^A}(\sqrt[m^A]{G})$*

and that for every i do not split completely in $K_{m^{S_i A}}$. Then $\Gamma_{K,G,m}$ and Γ_{K,G,m^A} have a natural density, which we call $D_{K,G,m}$ and Δ_{K,G,m^A} respectively, and we have

$$D_{K,G,m} = \sum_A \Delta_{K,G,m^A} \,. \tag{2}$$

Proof. To ease notation we remove the subindex (K, G, m) and we write A for the subindex (K, G, m^A). We first prove that Δ_A is well-defined. Write $L := K_{m^A}(\sqrt[m^A]{G})$. For Γ_A we may equivalently consider the primes that split completely in L and that for every i do not split completely in $F_i = K_{m^{S_i A}}(\sqrt[m^A]{G})$. We conclude by applying Corollary 3.

Consider a prime $\mathfrak{p}$ of K such that the m-adic valuation of $k_\mathfrak{p}^\times$ equals A. Then $\mathfrak{p} \in \Gamma_{K,G,m}$ if and only if $\mathfrak{p} \in \Gamma_A$ because an element of $(G \bmod \mathfrak{p})$ has order coprime to m if and only if it has m^A-th roots in $k_\mathfrak{p}^\times$.

We have proven that $\Gamma = \cup_A \Gamma_A$ holds. Write $A \leqslant n$ if $a_i \leqslant n$ holds for all $i = 1, \dots, f$. Since the sets Γ_A are pairwise disjoint and each of them has natural density Δ_A we get that $\cup_{A \leqslant n} \Gamma_A$ has a natural density, given by

$$\operatorname{dens}\Big(\bigcup_{A \leqslant n} \Gamma_A \Big) = \sum_{A \leqslant n} \Delta_A \,.$$

Since this holds for every n then the lower natural density satisfies

$$\operatorname{dens}_-(\Gamma) \geqslant \sum_A \Delta_A \,.$$

To conclude we show that for the upper natural density we have

$$\operatorname{dens}_+(\Gamma) \leqslant \varepsilon(n) + \sum_{A \leqslant n} \Delta_A$$

for some function $\varepsilon(n)$ that goes to zero for n going to infinity. It then suffices to prove that the difference

$$\Gamma' := \Gamma \setminus \bigcup_{A \leqslant n} \Gamma_A$$

is contained in a set whose upper density goes to zero with n. This is true because the primes in Γ' split completely in $K_{\ell_i^n}$ for some $i = 1, \dots, f$ and hence Γ' is contained in a finite union of sets that have a natural density that goes to zero with n. □

In the remaining of the section we investigate cases in which the density $D_{K,G,m}$ is the product of the densities related to the prime divisors of m.

Lemma 10. *Let ℓ vary over the prime divisor of m. We have*

$$D_{K,G,m} = \prod_\ell D_{K,G,\ell}$$

if for every $n \geqslant 1$ the following two conditions hold, where $w = \frac{m}{\ell}$:

- **(i):** *the extensions $K_{\ell^n \cdot w}$ and $K_{\ell^n}(\sqrt[\ell^n]{G})$ are linearly disjoint over K_{ℓ^n};*
- **(ii):** *the extensions $K_{\ell \cdot w^n}$ and $K_{w^n}(\sqrt[w^n]{G})$ are linearly disjoint over K_{w^n}.*

Proof. Recall the notation $m = \ell_1 \cdots \ell_f$. We claim that we have $\Delta_{K,G,m^A} = \prod_{i=1}^f \Delta_{K,G,\ell_i^{a_i}}$. Then we can write by Theorem 9:

$$D_{K,G,m} = \sum_A \Delta_{K,G,m^A} = \sum_A \prod_{i=1}^f \Delta_{K,G,\ell_i^{a_i}} = \prod_{i=1}^f \sum_{a_i \geqslant 0} \Delta_{K,G,\ell_i^{a_i}} = \prod_{i=1}^f D_{K,G,\ell_i}\,.$$

So we are left to prove the claim. By Corollary 3 we can write

$$\Delta_{K,G,\ell_i^{a_i}} = [K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G}) : K]^{-1} \cdot \Big(1 - \frac{1}{[K_{\ell_i^{a_i+1}}(\sqrt[\ell_i^{a_i}]{G}) : K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G})]}\Big)$$

and also

$$\Delta_{K,G,m^A} = [K_{m^A}(\sqrt[m^A]{G}) : K]^{-1} \cdot \prod_{i=1}^f \Big(1 - \frac{1}{[K_{m^{S_iA}}(\sqrt[m^A]{G}) : K_{m^A}(\sqrt[m^A]{G})]}\Big)\,.$$

We are then just left to prove

$$[K_{m^A}(\sqrt[m^A]{G}) : K] = \prod_{i=1}^f [K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G}) : K] \tag{3}$$

and

$$[K_{m^{S_iA}}(\sqrt[m^A]{G}) : K_{m^A}(\sqrt[m^A]{G})] = [K_{\ell_i^{a_i+1}}(\sqrt[\ell_i^{a_i}]{G}) : K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G})]\,. \tag{4}$$

We always have

$$[K_{m^A}(\sqrt[m^A]{G}) : K_{m^A}] = \prod_{i=1}^f [K_{m^A}(\sqrt[\ell_i^{a_i}]{G}) : K_{m^A}]$$

and $[K_{m^A} : K] = \prod_{i=1}^f [K_{\ell_i^{a_i}} : K]$ so (3) reduces to the equality

$$[K_{m^A}(\sqrt[\ell^{a_i}]{G}) : K_{m^A}] = [K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G}) : K_{\ell_i^{a_i}}]\,.$$

Since the extension $K_{m^A}/K_{\ell_i^{a_i}\cdot\frac{m}{\ell_i}}$ has degree coprime to ℓ_i, we are done by condition (i).

For better readability we write $L := K_{\ell_i^{a_i}}(\sqrt[\ell_i^{a_i}]{G})$ and we call B the tuple obtained from A by removing a_i.

If $a_i = 0$ then $L = K$ and (4) is equivalent to knowing for every B:

$$[K_{\ell_i w_i^B}(\sqrt[w_i^B]{G}) : K_{w_i^B}(\sqrt[w_i^B]{G})] = [K_{\ell_i} : K]\,.$$

This exactly means that the extensions K_{ℓ_i} and $K_{w_i^B}(\sqrt[w_i^B]{G})$ are linearly disjoint over K. We may suppose that all entries of B are equal and write $w_i^B = w_i^b$ for some integer b. Since ℓ_i and w_i^b are coprime, it suffices that the extensions $K_{\ell_i w_i^b}$ and $K_{w_i^b}(\sqrt[w_i^b]{G})$ are linearly disjoint over $K_{w_i^b}$. This is ensured by condition (ii).

Now suppose $a_i > 0$. The right-hand side of (4) is a power of ℓ and hence we are left to show

$$[L_{\ell_i^{a_i+1} w^B} : L_{w^B}] = [L_{\ell_i^{a_i+1}} : L]\,,$$

which is true because w^B is coprime to ℓ_i. □

Theorem 11. *Let ℓ vary over the prime divisor of m. We have*

$$D_{K,G,m} = \prod_{\ell} D_{K,G,\ell}$$

if for every $n \geqslant 1$ the extensions $K_{\ell^n \cdot \frac{m}{\ell}}$ and $K_{\ell^n}(\sqrt[\ell^n]{G})$ are linearly disjoint over K_{ℓ^n}.

Proof. It suffices to prove that in Lemma 10 Condition (ii) is implied by Condition (i). If Condition (ii) does not hold then there is some prime divisor ℓ of m such that the extensions $K_{\ell \cdot w^n}$ and $K_{w^n}(\sqrt[w^n]{G})$ are not linearly disjoint over K_{w^n}. Then there must be a prime divisor q of w such that the same holds for $K_{\ell \cdot w^n}$ and $K_{w^n}(\sqrt[q^n]{G})$. Consequently, the extensions $K_{\ell \cdot q^n}$ and $K_{q^n}(\sqrt[q^n]{G})$ are not linearly disjoint over K_{q^n}. In particular $K_{\frac{m}{q} \cdot q^n}$ and $K_{q^n}(\sqrt[q^n]{G})$ are not linearly disjoint over K_{q^n}, which contradicts Condition (i) for q. □

Corollary 12. *If $K_m = K$ then the product formula of Theorem 11 holds.*

Proof. The assumption of Theorem 11 holds because we have $K_{\frac{m}{\ell}} = K$. □

Proposition 13. *Suppose that m is odd and that $K_\ell \neq K$ holds for all prime factors ℓ of m. Then the product formula of Theorem 11 holds.*

Proof. We prove that the condition of Theorem 11 holds. Write $F := K_{\ell^n}$ and $w := \frac{m}{\ell}$. Suppose that there is some prime divisor ℓ of m such that the extensions F_w and $F(\sqrt[\ell^n]{G})$ are not linearly disjoint over F. Clearly we have $n > 0$. The first extension is cyclic so there is some $g \in G$ such that F_w and $F(\sqrt[\ell^n]{g})$ are not linearly disjoint over F. There is some maximal $d < n$ such that there is some $a \in K^\times$ satisfying $a^{\ell^d} = g$. For any choice of $\sqrt[\ell]{a}$ the field $K(\sqrt[\ell]{a})$ is different from K but it is contained in F_w. Then a is strongly ℓ-indivisible because $K_\ell \neq K$. By Theorem 4 the identity $K_{\ell^n w}(\sqrt[\ell]{a}) = K_{\ell^n w}$ implies $K_\ell = K$, contradicting the assumption in the statement. □

6. Formulas to reduce to known cases

We develop a strategy to reduce the computation of a general density $D_{K,G,m}$ to the computation of finitely many densities that concern only one prime divisor of m.

Let K be a number field, let G be a finitely–generated and torsion–free subgroup of $K^\times$ and let $m \geqslant 2$ be a square–free integer. We also use the notation introduced in the beginning of Section 4. We want to reduce the calculation of

$$D_{K,G,m} := \operatorname{dens}\{\mathfrak{p} : \operatorname{ord}(G \bmod \mathfrak{p}) \text{ is coprime to } m\}$$

to the case where m is a prime number. We can accomplish this in finitely many steps up to increasing the base field, as the following results show. Since all densities are related to G, we have removed G from the notation for better readability.

Theorem 14. *If m is composite and ℓ is a prime factor of m we have*

$$D_{K,m} = D_{K,\frac{m}{\ell}} + [K_\ell : K]^{-1} \cdot (D_{K_\ell,m} - D_{K_\ell,\frac{m}{\ell}}) \,. \tag{5}$$

Proof. We use the notation of Theorem 9. We suppose w.l.o.g. $\ell = \ell_f$ and we write for convenience $L := K_\ell$ and $n := \frac{m}{\ell}$. By Theorem 9 we have

$$D_{K,m} = \sum_A \Delta_{K,m^A} = \sum_{A:a_f=0} \Delta_{K,m^A} + \sum_{A:a_f>0} \Delta_{K,m^A}\,.$$

If $a_f > 0$ we are considering primes that split completely in L and we can apply Proposition 1. Moreover we have $\Delta_{L,m^A} = 0$ if $a_f = 0$. So we get

$$\sum_{A:a_f>0} \Delta_{K,m^A} = [L:K]^{-1} \cdot \sum_{A:a_f>0} \Delta_{L,m^A} = \frac{D_{L,m}}{[L:K]}\,.$$

Write $A = (B, a_f)$ where $B = (a_1, \ldots, a_{f-1})$, and call Γ_B the set of primes $\mathfrak{p}$ of K that split completely in $K_{n^B}(\sqrt[n^B]{G})$ and for every $i = 1, \ldots, f-1$ do not split completely in $K_{n^{S_i B}}$. The set Γ_B has natural density Δ_{K,n^B}. The primes in Γ_B which split completely in L have density $[L:K]^{-1} \cdot \Delta_{L,n^B}$ by Proposition 1. The primes in Γ_B which do not split completely in L have density $\Delta_{K,m^{(B,0)}}$, because having ℓ^0-th roots is an empty condition. So we get

$$D_{K,n} = \sum_B \Delta_{K,n^B} = \sum_B \Big(\frac{\Delta_{L,n^B}}{[L:K]} + \Delta_{K,m^{(B,0)}} \Big) = \frac{D_{L,n}}{[L:K]} + \sum_{a_f=0} \Delta_{K,m^A}$$

and we may easily recover the formula in the statement. □

Theorem 15. *Let $m = \ell_1 \cdots \ell_f$ be a product of distinct prime numbers. If $f \geqslant 2$ we have*

$$D_{K,m} = \sum_{i=1}^{f} \Big(\varepsilon_{i-1} \cdot D_{L_{i-1}, \frac{m}{\ell_i}} - \varepsilon_i \cdot D_{L_i, \frac{m}{\ell_i}} \Big) + \varepsilon_f \cdot \prod_{i=1}^{f} D_{L_f, \ell_i}$$

where the notations are as follows: we write $\varepsilon_0 := 1$, $L_0 := K$ and for $i = 1, \ldots, f$ we set

$$\varepsilon_i := \prod_{1 \leqslant j \leqslant i} [K_{\ell_j} : K]^{-1} \qquad \text{and} \qquad L_i := \prod_{1 \leqslant j \leqslant i} K_{\ell_j}\,.$$

Proof. By Corollary 12 we have $D_{L_f,m} = \prod_{i=1}^{f} D_{L_f,\ell_i}$. We then prove that for $1 \leqslant n \leqslant f$ we have

$$D_{K,m} = \sum_{i=1}^{n} \Big(\varepsilon_{i-1} \cdot D_{L_{i-1}, \frac{m}{\ell_i}} - \varepsilon_i \cdot D_{L_i, \frac{m}{\ell_i}} \Big) + \varepsilon_n \cdot D_{L_n,m}\,.$$

We prove this formula by induction on n. The case $n = 1$ can be obtained by applying Theorem 14 to ℓ_1:

$$D_{K,m} = D_{K,\frac{m}{\ell_1}} + \varepsilon_1 \cdot D_{L_1,m} - \varepsilon_1 \cdot D_{L_1,\frac{m}{\ell_1}} = \Big(\varepsilon_0 \cdot D_{L_0,\frac{m}{\ell_1}} - \varepsilon_1 \cdot D_{L_1,\frac{m}{\ell_1}} \Big) + \varepsilon_1 \cdot D_{L_1,m}\,.$$

Now suppose that we know the inductive assumption

$$D_{K,m} = \sum_{i=1}^{n-1} \Big(\varepsilon_{i-1} \cdot D_{L_{i-1}, \frac{m}{\ell_i}} - \varepsilon_i \cdot D_{L_i, \frac{m}{\ell_i}} \Big) + \varepsilon_{n-1} \cdot D_{L_{n-1},m}\,.$$

We can achieve the induction step by applying Theorem 14 to ℓ_n, which gives:

$$\varepsilon_{n-1} \cdot D_{L_{n-1},m} = \varepsilon_{n-1} \cdot D_{L_{n-1},\frac{m}{\ell_n}} + \varepsilon_n \cdot D_{L_n,m} - \varepsilon_n \cdot D_{L_n,\frac{m}{\ell_n}}\,.$$

□

By the above result we can reduce to computing densities which involve one prime factor less. With finitely many applications of this result we have reduced to the case of exactly one prime number, and we can make use of the formulas of [4, 1].

7. EXAMPLES

Example 16. Let $K = \mathbb{Q}$ and $m = 6$. By Corollary 12 we know $D_{\mathbb{Q}(\zeta_3),6} = D_{\mathbb{Q}(\zeta_3),2} \cdot D_{\mathbb{Q}(\zeta_3),3}$ and by Theorem 14 applied to $\ell = 3$ we have

$$D_{\mathbb{Q},6} = D_{\mathbb{Q},2} + [\mathbb{Q}(\zeta_3) : \mathbb{Q}]^{-1} \cdot (D_{\mathbb{Q}(\zeta_3),6} - D_{\mathbb{Q}(\zeta_3),2}) .$$

We evaluate the right-hand side of this expression (with [4, Theorems 16 and 17] for rank 1 and [1, Theorems 3 and 4] otherwise) in some explicit examples, which are listed in the following table. We also compute $D_{\mathbb{Q},3}$, so that one can easily see that the formula $D_{\mathbb{Q},6} = D_{\mathbb{Q},2} D_{\mathbb{Q},3}$ holds for the examples in the upper part of the table (and in general it does not hold). Notice that the field $\mathbb{Q}(\zeta_3)$ contains $\sqrt{-3}$.

G	$D_{\mathbb{Q},6}$	$D_{\mathbb{Q},2}$	$D_{\mathbb{Q},3}$	$D_{\mathbb{Q}(\zeta_3),2}$	$D_{\mathbb{Q}(\zeta_3),3}$
$\langle 2 \rangle$	$35/192$	$7/24$	$5/8$	$7/24$	$1/4$
$\langle 5 \rangle$	$5/24$	$1/3$	$5/8$	$1/3$	$1/4$
$\langle 2, 5 \rangle$	$29/416$	$29/224$	$7/13$	$29/224$	$1/13$
$\langle -3 \rangle$	$1/12$	$1/3$	$5/8$	$2/3$	$1/4$
$\langle 3 \rangle$	$13/48$	$1/3$	$5/8$	$1/6$	$1/4$
$\langle 9 \rangle$	$17/48$	$2/3$	$5/8$	$5/6$	$1/4$
$\langle -9 \rangle$	$13/96$	$1/6$	$5/8$	$1/12$	$1/4$
$\langle -27 \rangle$	$1/4$	$1/3$	$7/8$	$2/3$	$3/4$
$\langle 27 \rangle$	$5/16$	$1/3$	$7/8$	$1/6$	$3/4$
$\langle 2, 3 \rangle$	$365/2912$	$29/224$	$7/13$	$1/112$	$1/13$
$\langle 2, -3 \rangle$	$29/2912$	$29/224$	$7/13$	$29/112$	$1/13$

All examples in the table have been tested with Sage [6].

Example 17. Let $K = \mathbb{Q}$ and $m = 15$. If we apply Theorem 14 for $\ell = 3$ we have

$$D_{\mathbb{Q},15} = D_{\mathbb{Q},5} + [\mathbb{Q}(\zeta_3) : \mathbb{Q}]^{-1} \cdot (D_{\mathbb{Q}(\zeta_3),15} - D_{\mathbb{Q}(\zeta_3),5})$$

and by Theorem 14 for $\ell = 5$ we can write

$$D_{\mathbb{Q}(\zeta_3),15} = D_{\mathbb{Q}(\zeta_3),3} + [\mathbb{Q}(\zeta_{15}) : \mathbb{Q}(\zeta_3)]^{-1} \cdot (D_{\mathbb{Q}(\zeta_{15}),15} - D_{\mathbb{Q}(\zeta_{15}),3})$$

so by recalling $D_{\mathbb{Q}(\zeta_{15}),15} = D_{\mathbb{Q}(\zeta_{15}),3} \cdot D_{\mathbb{Q}(\zeta_{15}),5}$ we get

$$D_{\mathbb{Q},15} = D_{\mathbb{Q},5} + \frac{1}{2} \cdot (D_{\mathbb{Q}(\zeta_3),3} - D_{\mathbb{Q}(\zeta_3),5}) - \frac{1}{8} D_{\mathbb{Q}(\zeta_{15}),3} + \frac{1}{8} \cdot D_{\mathbb{Q}(\zeta_{15}),3} \cdot D_{\mathbb{Q}(\zeta_{15}),5} .$$

If we apply Theorem 14 for for $\ell = 5$ and then expand $D_{\mathbb{Q}(\zeta_5),15}$ (by Theorem 14 for $\ell = 3$) we similarly get

$$D_{\mathbb{Q},15} = D_{\mathbb{Q},3} + \frac{1}{4}(D_{\mathbb{Q}(\zeta_5),5} - D_{\mathbb{Q}(\zeta_5),3}) - \frac{1}{8} D_{\mathbb{Q}(\zeta_{15}),5} + \frac{1}{8} \cdot D_{\mathbb{Q}(\zeta_{15}),3} \cdot D_{\mathbb{Q}(\zeta_{15}),5} .$$

Both methods give of course the same value for $D_{\mathbb{Q},15}$ (tested with Sage [6] for the following examples):

G	$D_{\mathbb{Q},15}$	$D_{\mathbb{Q},3}$	$D_{\mathbb{Q},5}$	$D_{\mathbb{Q}_3,3}$	$D_{\mathbb{Q}_3,5}$	$D_{\mathbb{Q}_5,3}$	$D_{\mathbb{Q}_5,5}$	$D_{\mathbb{Q}_{15},3}$	$D_{\mathbb{Q}_{15},5}$
$\langle 2\rangle$	$95/192$	$5/8$	$19/24$	$1/4$	$19/24$	$5/8$	$1/6$	$1/4$	$1/6$
$\langle 2^9\rangle$	$437/576$	$23/24$	$19/24$	$11/12$	$19/24$	$23/24$	$1/6$	$11/12$	$1/6$
$\langle 2^{15}\rangle$	$161/192$	$7/8$	$23/24$	$3/4$	$23/24$	$7/8$	$5/6$	$3/4$	$5/6$

Example 18. This example is in particular a counterexample to (1) with m odd. Let $K = \mathbb{Q}(\zeta_3)$ and $m = 21$. If C denotes the cyclic subextension of $\mathbb{Q}(\zeta_7)$ of degree 3 then $C(\zeta_3)$ is a Kummer extension of $\mathbb{Q}(\zeta_3)$ and we can write it as $\mathbb{Q}(\zeta_3, \sqrt[3]{g})$ for some $g \in \mathbb{Q}(\zeta_3)^\times$. We claim that for the group $G = \langle g\rangle$ we have

$$D_{\mathbb{Q}(\zeta_3),21} \neq D_{\mathbb{Q}(\zeta_3),3} \cdot D_{\mathbb{Q}(\zeta_3),7}\,.$$

We may suppose that g is strongly 7-indivisible in $\mathbb{Q}(\zeta_3)$ and hence also in $\mathbb{Q}(\zeta_{21})$. We know that it is strongly 3-indivisible in $\mathbb{Q}(\zeta_3)$. We deduce that $\sqrt[3]{g}$ is strongly 3-indivisible in $\mathbb{Q}(\zeta_{21})$. We have $D_{\mathbb{Q}(\zeta_3),3} = 1/4$ and $D_{\mathbb{Q}(\zeta_3),7} = 41/48$. By Theorem 14 applied to $\ell = 7$ we get

$$D_{\mathbb{Q}(\zeta_3),21} = D_{\mathbb{Q}(\zeta_3),3} + [\mathbb{Q}(\zeta_{21}) : \mathbb{Q}(\zeta_3)]^{-1} \cdot (D_{\mathbb{Q}(\zeta_{21}),21} - D_{\mathbb{Q}(\zeta_{21}),3})\,.$$

We have $D_{\mathbb{Q}(\zeta_{21}),3} = 3/4$ and $D_{\mathbb{Q}(\zeta_{21}),7} = 1/8$ and hence $D_{\mathbb{Q}(\zeta_{21}),21} = 3/32$. We deduce $D_{\mathbb{Q}(\zeta_3),21} = 9/64$ and the claim follows.

ACKNOWLEDGEMENTS

The author would like to thank Christophe Debry, Franziska Schneider and Franziska Wutz for their support, and the referee for their careful reading of the paper. The project originated as a mentor/mentee collaboration in the WIN style (the mentees left academia).

REFERENCES

[1] C. Debry and A. Perucca, *Reductions of algebraic integers*, J. Number Theory, **167** (2016), 259–283.
[2] M. Hindry and J. Silverman, *Diophantine geometry. An Introduction.* Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2000, xiv+558 pp.
[3] H. W. Jr. Lenstra, *Commentary on H: Divisibility and congruences*. Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 901–902.
[4] A. Perucca, *The order of the reductions of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.
[5] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980),101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.
[6] W. A. Stein et al., Sage Mathematics Software (Version 5.7). The Sage Development Team, 2013, http://www.sagemath.org.
[7] J. Wójcik, *Criterion for a field to be abelian*, Colloq. Math. **68** (1995), no. 2, 187–191.

FAKULTÄT MATHEMATIK, UNIVERSITÄT REGENSBURG, 93040 REGENSBURG, GERMANY

E-mail address: antonella.perucca@mathematik.uni-regensburg.de