MULTIPLICATIVE ORDER AND FROBENIUS SYMBOL FOR THE REDUCTIONS OF NUMBER FIELDS

ANTONELLA PERUCCA

ABSTRACT. Let L/K be a finite Galois extension of number fields, and let G be a finitely generated subgroup of $K^\times$. We study the natural density of the set of primes of K having some prescribed Frobenius symbol in $\mathrm{Gal}(L/K)$, and for which the reduction of G has multiplicative order with some prescribed ℓ-adic valuation for finitely many prime numbers ℓ. This extends in several directions results by Moree and Sury (2009) and by Chinen and Tamura (2012), and has to be compared with the very general result of Ziegler (2006).

1. INTRODUCTION

Consider a Lucas sequence $a^k + b^k$ where $a, b \in \mathbb{Z}$. A prime divisor for the sequence is a prime number that divides at least one term in the sequence. Apart from some trivial cases, counting the prime divisors for the above sequence means counting the prime numbers p such that the multiplicative order of a/b modulo p is even (we may count instead the reductions for which the order is odd). The set of prime divisors admits a natural density, which has been computed by Hasse [3, 4]. There are many related questions, see for example the survey by Moree [5].

The following refined question has also been considered: if $L/\mathbb{Q}$ is a finite Galois extension and $\mathfrak{c}$ is a conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$, how many prime numbers p (unramified in L) are prime divisors for a given Lucas sequence and also fulfill the condition $\mathrm{Frob}_{L/\mathbb{Q}}(p) \subseteq \mathfrak{c}$ for their Frobenius symbol? If L is either quadratic or cyclotomic, the corresponding density has been worked out by Chinen and Tamura [1] and by Moree and Sury [6].

We work in much greater generality. Indeed, we let L/K be any finite Galois extension of number fields and let $\mathfrak{c}$ be a conjugacy-stable subset of the Galois group $\mathrm{Gal}(L/K)$. We also work with any finitely generated subgroup G of $K^\times$. We test coprimality of the order with respect to finitely many prime numbers ℓ and in fact we can also arbitrarily prescribe the ℓ-adic valuation of the order.

Up to excluding finitely many primes $\mathfrak{p}$ of K, we may assume that $\mathfrak{p}$ is unramified in L and that the reduction of G modulo $\mathfrak{p}$ is well-defined.

For simplicity, we now fix one prime number ℓ and count the primes $\mathfrak{p}$ of K that satisfy the following two conditions: firstly, for the Frobenius symbol we must have $\mathrm{Frob}_{L/K}(\mathfrak{p}) \subseteq \mathfrak{c}$; secondly, the order of the group $(G \bmod \mathfrak{p})$ must be coprime to ℓ. Since G only affects the second condition, we may assume w.l.o.g. that G is torsion-free and non-trivial. The general result involves cyclotomic and Kummer extensions (we refer to Section 2 for the definitions and the notation) and it is as follows:

Theorem 1. *Let K be a number field, and fix some non-trivial, finitely generated and torsion-free subgroup G of $K^\times$. Let L be a finite Galois extension of K, and fix some conjugacy-stable subset $\mathfrak{c}$ of $\mathrm{Gal}(L/K)$. Let ℓ be a prime number.*
The set of primes $\mathfrak{p}$ of K satisfying $\mathrm{Frob}_{L/K}(\mathfrak{p}) \subseteq \mathfrak{c}$ and $\ell \nmid \mathrm{ord}(G \bmod \mathfrak{p})$ admits a natural density, which is given by

$$\mathrm{dens}_K(G, \mathfrak{c}, \ell) = \sum_{n=0}^{\infty} \Big(\frac{c(n,n)}{[L(n,n):K]} - \frac{c(n+1,n)}{[L(n+1,n):K]} \Big), \tag{1}$$

where we set $K(m,n) := K(\ell^{-m}1, \ell^{-n}G)$ and $L(m,n) := L \cdot K(m,n)$, and where $c(m,n)$ is the number of elements in $\mathfrak{c}$ that are the identity on $L \cap K(m,n)$.

In the special case $\mathfrak{c} = \mathrm{Gal}(L/K)$, the condition on the Frobenius symbol is trivial and we become the density considered by Debry and Perucca in [2], namely

$$\mathrm{dens}_K(G, \ell) = \sum_{n=0}^{\infty} \Big(\frac{1}{[K(n,n):K]} - \frac{1}{[K(n+1,n):K]} \Big). \tag{2}$$

We also extend Theorem 1 by requiring coprimality of the order with respect to finitely many prime numbers i.e. the order of the reduction of G must be coprime to some given integer $m > 1$. We call the corresponding density $\mathrm{dens}_K(G, \mathfrak{c}, m)$. The density $\mathrm{dens}_K(G, m)$ without the condition on the Frobenius symbol has been considered in [7]. We prove in general that $\mathrm{dens}_K(G, \mathfrak{c}, m)$ is an explicitly computable rational number, see Theorem 17. Finally, rather than considering only the case of valuation 0, for each prime divisor ℓ of m we may arbitrarily prescribe the ℓ-adic valuation of the order of the reduction of G, see Theorem 18.

We conclude by justifying our work in view of the elegant and very general result of Ziegler [8, Theorem 1]. The advantages of our approach are that we work unconditionally, we consider a finitely generated group of any rank, and we show that the density is computable and it is a rational number.

Acknowledgements: The author sincerely thanks Pieter Moree for inviting her to visit the MPIM Bonn in April 2017 and for suggesting the problem which has been solved in this paper.

2. PRELIMINARIES

The Frobenius symbol: If L/K is a finite Galois extension of number fields, we define the Frobenius symbol $\mathrm{Frob}_{L/K}(\mathfrak{p})$ of a prime $\mathfrak{p}$ of K that does not ramify in L. Write $\mathcal{O}_K$ and $\mathcal{O}_L$ for the ring of integers of K and L respectively. The Frobenius symbol of $\mathfrak{p}$ is the conjugacy class in $\mathrm{Gal}(L/K)$ consisting of those σ satisfying the following condition: there exists some prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$ such that for all $\alpha \in \mathcal{O}_L$ we have

$$\sigma(\alpha) \equiv \alpha^{\#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)} (\mathrm{mod}\ \mathfrak{q})\,.$$

The m-adic valuation (and tuples): We let $m > 1$ be a square-free integer and we consider its prime factorization $m = \ell_1 \cdots \ell_f$. Set $I = \{1, \ldots, f\}$. We define the *m-adic valuation* as the f-tuple of the ℓ_i-adic valuations where $i \in I$.

If n is a non-negative integer, to ease notation we also write n for the f-tuple with all entries equal to n.

Let A, B be f-tuples. We write $A \leqslant B$ if each entry of A is smaller than or equal to the corresponding entry of B. We write $A < B$ if $A \leqslant B$ and $A \neq B$ hold.

Let A be any f-tuple of non-negative integers, and write A_i for the i-th entry of A. We define

$$m^A := \prod_{i \in I} \ell_i^{A_i}\,.$$

Torsion and Kummer extensions: Let K be a number field. If n is a positive integer, the n-th cyclotomic extension of K will be denoted by $K(n^{-1}1)$. If G is a finitely generated subgroup of $K^\times$ we consider the Kummer extension $K(n^{-1}G)$, which is the smallest extension of K over which all n-th roots of G (namely all algebraic numbers x such that $x^n \in G$) are defined. When we are interested in powers of some fixed prime number ℓ, we use the following compact notation:

$$K(m, n) := K(\ell^{-m}1, \ell^{-n}G)\,.$$

The union of these fields is usually denoted by $K(\ell^{-\infty}G)$. We will work with some positive square-free number $m > 1$ and then consider $K(m^{-\infty}G)$ i.e. the compositum of the fields $K(\ell^{-\infty}G)$ for ℓ varying among the prime divisors of m.

Lemma 2. *Let K'/K be a finite Galois extension of number fields. Let S (resp. S') be a set of primes of K (resp. K') admitting a Dirichlet density. If S consists only of primes splitting completely in K', and if S' is the set of primes of K' lying above the primes in S, then we have* $\mathrm{dens}_K(S) = [K' : K]^{-1} \cdot \mathrm{dens}_{K'}(S')$.

Proof. This fact is well known, see e.g. [7, Proposition 1] for a proof. □

3. The density as an infinite sum

Theorem 3. *Let K be a number field, and fix some non-trivial, finitely generated and torsion-free subgroup G of $K^\times$. Let L be a finite Galois extension of K, and fix some conjugacy-stable subset $\mathfrak{c}$ of $\mathrm{Gal}(L/K)$. Let m be the product of f distinct prime numbers. The set of primes $\mathfrak{p}$ of K satisfying $\mathrm{Frob}_{L/K}(\mathfrak{p}) \subseteq \mathfrak{c}$ and such that $\mathrm{ord}(G \bmod \mathfrak{p})$ is coprime to m admits a natural density, which is given by*

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \sum_A \mathrm{dens}_K(G, \mathfrak{c}, m, A) \tag{3}$$

where A varies over the f-tuples of non-negative integers and where $\mathrm{dens}_K(G, \mathfrak{c}, m, A)$ is the natural density of the set of primes $\mathfrak{p}$ of K that split completely in $K(m^{-A}G)$, do not split completely in $K(m^{-B}1)$ for any $B > A$, and satisfy $\mathrm{Frob}_{L/K}(\mathfrak{p}) \subseteq \mathfrak{c}$.

Proof. Up to excluding finitely many primes of K, we may suppose them to be unramified in L and in $K(m^{-\infty}G)$. The natural density $\mathrm{dens}_K(G, \mathfrak{c}, m, A)$ is well-defined by the Chebotarev Density Theorem. The set of primes considered for $\mathrm{dens}_K(G, \mathfrak{c}, m)$ is the disjoint union over A of those considered for $\mathrm{dens}_K(G, \mathfrak{c}, m, A)$, see [7, Theorem 9]. The natural density $\mathrm{dens}_K(G, \mathfrak{c}, m)$ then exists because the tail of the sum is contained in the set of primes splitting completely in $K(m^{-n}G)$ for some $n \geqslant 1$, and this set has a natural density going to zero for n going to infinity. □

Proof of Theorem 1. By Theorem 3 we only need evaluating $\mathrm{dens}_K(G, \mathfrak{c}, n)$ i.e. consider the set of primes of K that split completely in $K(n, n)$, do not split in $K(n+1, n)$ and satisfy the condition on the Frobenius symbol. We first count the primes $\mathfrak{p}$ of K whose Frobenius symbol is in $\mathfrak{c}$ and split completely in $K(n, n)$ and then remove those whose Frobenius symbol is in $\mathfrak{c}$ and split completely in $K(n + 1, n)$. Let $N \in \{n, n + 1\}$. By the Chebotarev Density Theorem, we only have to evaluate the relative size of the conjugacy-stable subset of $\mathrm{Gal}(L(N, n)/K)$ consisting of those elements that map to $\mathfrak{c}$ in $\mathrm{Gal}(L/K)$ and map to the identity on $K(N, n)$. The fields L and $K(N, n)$ are linearly disjoint over their intersection and their compositum is $L(N, n)$. Up to considering a factor $[L(N, n) : L]^{-1}$ it is then equivalent to compute the relative size of the conjugacy class in $\mathrm{Gal}(L/K)$ consisting of those elements in $\mathfrak{c}$ that are the identity on $L \cap K(N, n)$. The latter is $c(N, n)/[L : K]$ and we conclude. □

4. General remarks

We keep the notation of Theorem 3 and investigate $\mathrm{dens}_K(G, \mathfrak{c}, m)$. Recall that we write $\mathrm{dens}_K(G, m)$ for the density analogous to $\mathrm{dens}_K(G, \mathfrak{c}, m)$ where we neglect the condition on the Frobenius symbol.

Lemma 4. *The following assertions hold:*

(a): *We may replace the field L by L' and $\mathfrak{c}$ by $\mathfrak{c}'$, where L'/L is any finite Galois extension and $\mathfrak{c}'$ is the preimage of $\mathfrak{c}$ in $\mathrm{Gal}(L'/K)$ because we have*

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \mathrm{dens}_K(G, \mathfrak{c}', m)\,.$$

(b): *We may partition $\mathfrak{c}$ into sets which are the union of conjugacy classes and add together the densities calculated with respect to each element in the partition.*

(c): *If two conjugacy-stable subsets $\mathfrak{c}$ and $\mathfrak{c}'$ give a partition of $\mathrm{Gal}(L/K)$ then we may compute $\mathrm{dens}_K(G, \mathfrak{c}, m)$ from $\mathrm{dens}_K(G, \mathfrak{c}', m)$.*

(d): *We may reduce w.l.o.g. to the following special case: for every Galois subextension F/K of L/K either all elements of $\mathfrak{c}$ are the identity on F, or none is (which possibility applies depends on F).*

Proof. **(a)** The Frobenius symbol w.r.t L/K lies in $\mathfrak{c}$ if and only if the Frobenius symbol w.r.t L'/K lies in $\mathfrak{c}'$. **(b)** Obvious. **(c)** We have

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \mathrm{dens}_K(G, m) - \mathrm{dens}_K(G, \mathfrak{c}', m)$$

where $\mathrm{dens}_K(G, m)$ is the density without considering the Frobenius condition, which can be explicitly computed by the results in [7]. **(d)** The kernel of the quotient map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ and its complement induce a partition on $\mathfrak{c}$, and we may apply (b). Since L/K has only finitely many Galois subextensions, we may repeat this procedure and get the assertion for every F. □

Remark 5. *We may always reduce to the case $L \subset K(m^{-\infty}G)$ by combining Lemma 4(b) with the following result.*

Proposition 6. *Let $L' = L \cap K(m^{-\infty}G)$ and let $\mathfrak{c}'$ be the projection of $\mathfrak{c}$ in $\mathrm{Gal}(L'/K)$.*

(a): *If each element in $\mathfrak{c}'$ has the same amount of preimages in $\mathfrak{c}$, then we have*

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \frac{\#\mathfrak{c}}{\#\mathfrak{c}' \cdot [L : L']} \cdot \mathrm{dens}_K(G, \mathfrak{c}', m)\,. \tag{4}$$

In particular, if $\mathfrak{c}$ is the inverse image of $\mathfrak{c}'$ in $\mathrm{Gal}(L/K)$, then we have

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \mathrm{dens}_K(G, \mathfrak{c}', m)\,. \tag{5}$$

(b): *We may partition $\mathfrak{c}$ into conjugacy classes for which part (a) applies, and whose images in $\mathrm{Gal}(L'/K)$ give a partition of $\mathfrak{c}'$.*

Proof. **(a)** Call $\mathfrak{c}'' \supseteq \mathfrak{c}$ the inverse image of $\mathfrak{c}'$ in $\mathrm{Gal}(L/K)$. By Lemma 4(a) we have to prove

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \frac{\#\mathfrak{c}}{\#\mathfrak{c}''} \cdot \mathrm{dens}_K(G, \mathfrak{c}'', m)\,.$$

By Theorem 3 it then suffices to fix any f-tuple A of nonnegative integers and show that

$$\mathrm{dens}_K(G, \mathfrak{c}, m, A) = \frac{\#\mathfrak{c}}{\#\mathfrak{c}''} \cdot \mathrm{dens}_K(G, \mathfrak{c}'', m, A)$$

holds. Whether a prime of K has to be counted or not for these two densities only depends on its Frobenius class in the extension $L(m^{-A+1}G)/K$, therefore we may apply the Chebotarev Density Theorem to this finite Galois extension. By the assumption on $\mathfrak{c}'$, the sizes of the conjugacy-stable sets corresponding to the two densities have ratio $\#\mathfrak{c}/\#\mathfrak{c}''$, and we conclude. **(b)** It suffices to remark that two elements of $\mathrm{Gal}(L/K)$ having the same restriction to L' are mapped under conjugation to two elements with the same property. □

The following corollary deals with the generic case, in which the extensions L and $K(m^{-\infty}G)$ are linearly disjoint. The condition on the Frobenius symbol provides the term $\frac{\#\mathfrak{c}}{[L:K]}$ and the condition on the order gives the remaining term (the two conditions are here independent).

Corollary 7. *If $L \cap K(m^{-\infty}G) = K$, then we have*

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \frac{\#\mathfrak{c}}{[L:K]} \cdot \mathrm{dens}_K(G, m)\,. \tag{6}$$

Proof. This is Proposition 6(a) where we set $L' = K$. □

Lemma 8. *We may reduce w.l.o.g. to the special case $K = K(m^{-1}1)$ (because if ℓ is a prime divisor of m we may either recover $\mathrm{dens}_K(G, \mathfrak{c}, m)$ from the analogue density computed over $K(\ell^{-1}1)$ or we may replace m by $\frac{m}{\ell}$). In particular, if ℓ varies over the prime divisors of m, we may reduce w.l.o.g. to the case where the extensions $K(\ell^{-\infty}G)$ are linearly disjoint over K.*

Proof. By Lemma 4(a) we may suppose that L contains $K(m^{-1}1)$. By Lemma 4(d), for each prime divisor ℓ of m we may suppose that either $\mathfrak{c} \subseteq \mathrm{Gal}(L/K(\ell^{-1}1))$ or that $\mathfrak{c} \cap \mathrm{Gal}(L/K(\ell^{-1}1)) = \emptyset$. In the first case we have

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = [K(\ell^{-1}1) : K]^{-1} \cdot \mathrm{dens}_{K(\ell^{-1}1)}(G, \mathfrak{c}, m)$$

by Lemma 2. In the second case the coprimality condition w.r.t. ℓ is trivial (being a consequence of the condition on the Frobenius symbol) so we may replace m by $\frac{m}{\ell}$. For the second assertion notice that the Galois group of $K(\ell^{-\infty}G)$ over K is a pro-ℓ-group if $K = K(m^{-1}1)$. □

5. Examples and special cases

Proposition 9 (Intermediate Galois groups; the identity)**.** *Suppose that $\mathfrak{c} = \mathrm{Gal}(L/K')$ holds for some intermediate extension $K \subseteq K' \subseteq L$ which is Galois over K. Then we*

have

$$\mathrm{dens}_K(G,\mathfrak{c},m)=\frac{1}{[K':K]}\cdot\mathrm{dens}_{K'}(G,m)\,, \tag{7}$$

In particular, we have:

$$\mathrm{dens}_K(G,\{\mathrm{id}_L\},m)=\frac{1}{[L:K]}\cdot\mathrm{dens}_L(G,m)\,. \tag{8}$$

Proof. We are interested in the primes $\mathfrak{p}$ of K that split completely in K' and for which the order of $(G \bmod \mathfrak{p})$ is coprime to m. This amounts to counting the primes $\mathfrak{q}$ of K' such that the order of $(G \bmod \mathfrak{q})$ is coprime to m. Finally, we can apply Lemma 2. The second assertion is the special case $K'=L$. □

Remark 10 (Abelian extensions)**.** *If the extension L/K is abelian, then by Lemma 4(b) we may suppose that $\mathfrak{c}$ consists of one element. More generally, we may consider $\mathfrak{c}=\{\sigma\}$ for any σ in the center of $\mathrm{Gal}(L/K)$. By Proposition 9 we may suppose that σ is not the identity.*

Remark 11 (Quadratic extensions)**.** *If L/K is a quadratic extension, there are three possibilities for $\mathfrak{c}$:*

(1) *If $\mathfrak{c}=\mathrm{Gal}(L/K)$, then we have $\mathrm{dens}_K(G,\mathfrak{c},m)=\mathrm{dens}_K(G,m)$.*

(2) *If $\mathfrak{c}=\{\mathrm{id}_L\}$, Proposition 9 gives $\mathrm{dens}_K(G,\mathfrak{c},m)=\frac{1}{2}\,\mathrm{dens}_L(G,m)$.*

(3) *If $\mathfrak{c}=\mathrm{Gal}(L/K)\setminus\{\mathrm{id}_L\}$, then Lemma 4(c) and the previous assertions give*

$$\mathrm{dens}_K(G,\mathfrak{c},m)=\mathrm{dens}_K(G,m)-\frac{1}{2}\,\mathrm{dens}_L(G,m)\,.$$

Remark 12 (Cyclotomic extensions)**.** *If L/K is a cyclotomic extension, i.e. if $L=K(n^{-1}1)$ for some $n\geqslant 1$, then in particular we have an abelian Galois extension. We may then suppose by Lemma 4(b) and Proposition 9 that $\mathfrak{c}=\{\sigma\}$ where σ is not the identity: if ζ_n is a primitive n-th root of unity, we have $\sigma(\zeta_n)=\zeta_n^s$ for some integer $1\leqslant s<n$ coprime to n. Thus the condition on the Frobenius symbol means considering the primes of K lying above the prime numbers congruent to s modulo n.*

Proposition 13 (Trivial coprimality condition)**.** *Let ℓ vary over the prime divisors of m. If, for every ℓ, no element of $\mathfrak{c}$ is the identity on $L\cap K(\ell^{-1}1)$, then we have:*

$$\mathrm{dens}_K(G,\mathfrak{c},m)=\frac{\#\mathfrak{c}}{[L:K]}\,. \tag{9}$$

Proof. The primes $\mathfrak{p}$ of K satisfying $\mathrm{Frob}_{L/K}(\mathfrak{p})\subseteq\mathfrak{c}$ are such that ℓ does not divide the order of the multiplicative group of the residue field at $\mathfrak{p}$. In particular, the order of $(G \bmod \mathfrak{p})$ is coprime to ℓ. The assertion is then a consequence of the Chebotarev Density Theorem. □

We now investigate the formula of Theorem 1 by choosing the field L and the conjugacy-stable set $\mathfrak{c}$ in different ways with respect to the involved cyclotomic/Kummer extensions. Remark that the summands of (1) are non-negative.

Example 14. Let ℓ be a prime number. Taking $L = K(\ell^{-t}1)$ and $\mathfrak{c} = \{\mathrm{id}_L\}$ for some integer $t \geqslant 1$ gives a density $D(t) := \mathrm{dens}_K(G, \mathfrak{c}, \ell)$ which is non-increasing with t, and that eventually is decreasing with t. We can write

$$D(t) = \sum_{n=t}^{\infty} \Big(\frac{1}{[L(n,n) : K]} - \frac{1}{[L(n+1,n) : K]} \Big) . \tag{10}$$

Set $\ell = 3$. Let us fix K such that $K \cap \mathbb{Q}(3^{-\infty}1) = \mathbb{Q}$, and choose G of positive rank r such that $K(3^{-\infty}G)$ has maximal degree over $K(3^{-\infty}1)$. Notice that this choice of K and G corresponds to the generic case. We then have

$$D(t) = \sum_{n=t}^{\infty} \frac{1}{2 \cdot 3^{(n-1)+nr}} - \frac{1}{2 \cdot 3^{n+nr}} = \sum_{n=t}^{\infty} 3^{-n(r+1)} = \frac{1}{3^{(t-1)(r+1)}(3^{r+1} - 1)} .$$

Clearly we could have done similar calculations for a different choice of ℓ.

Example 15. Let ℓ be a prime number, and consider $L = K(\ell^{-t}1)$ for some $t \geqslant 1$. Since the Galois extension L/K is abelian (and because of the previous example) we may fix without loss of generality some integer $0 \leqslant s \leqslant t-1$ and consider $\mathfrak{c} = \{\sigma\}$, where σ fixes all ℓ^s-th roots of unity and does not fix the primitive ℓ^{s+1}-th roots of unity. We write $D(t,s) := \mathrm{dens}_K(G, \mathfrak{c}, \ell)$. The only contribution to the density in (1) is the summand $n = s$. In the generic case, for G of rank r we obtain

$$D(t,s) = \frac{1}{[L(s,s) : K]} = \frac{1}{[K(\ell^{-t}1) : K] \cdot \ell^{rs}} . \tag{11}$$

For $\ell = 3$, $K = \mathbb{Q}$ and $s = t-1$ the formula gives the density $\frac{1}{2} \cdot 3^{-(r+1)s}$.

6. On the computability of the density

We keep the notation of Theorem 3 and investigate the computability and the rationality of the density $\mathrm{dens}_K(G, \mathfrak{c}, m)$. We write $\mathrm{dens}_K(G, m)$ if we neglect the condition on the Frobenius symbol.

• By Remark 5 we may suppose $L \subseteq K(m^{-\infty}G)$.

• We assume w.l.o.g. the uniformity on the subfields provided by Lemma 4(d).

• By Lemma 8 we may suppose that $K = K(m^{-1}1)$ and hence that for ℓ varying in the prime divisors of m the extensions $K(\ell^{-\infty}G)$ are linearly disjoint over K.

Definition (free primes, bounded primes): Let us fix a conjugacy-stable subset of the Galois group $\mathrm{Gal}(L/K)$, and some square-free integer $m \geqslant 2$. We call a prime divisor ℓ of m *free* if all elements of $\mathfrak{c}$ are the identity on $L \cap K(\ell^{-\infty}G)$, and *bounded* otherwise. We write $m = m_B \cdot m_F$ where m_B is the product of the bounded primes and m_F the product of the free primes. By definition, there is some positive integer n_0 (which we call the *bound*) such that for all bounded primes ℓ all elements of $\mathfrak{c}$ are not the identity on $L \cap K(\ell^{-n_0}G)$.

• By Lemma 2 for each free prime ℓ we may extend the base field to $L \cap K(\ell^{-\infty}G)$ i.e. suppose that $K = L \cap K(\ell^{-\infty}G)$. Then the free primes do not appear in the Frobenius symbol condition.

From Theorem 3 we know

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \sum_A \mathrm{dens}_K(G, \mathfrak{c}, m, A)\,. \tag{12}$$

We write $A = (X, Y)$ by sorting the indexes for the bounded primes and for the free primes respectively.

• We may suppose $A \neq Y$ because if $A = Y$ then we have $\mathrm{dens}_K(G, \mathfrak{c}, m) = \mathrm{dens}_K(G, m)$ and the latter density is rational and computable by the results in [2, 7].

• We may suppose $A \neq X$ because if $A = X$ then the density reduces to a finite sum of computable rational numbers. Indeed, we have $\mathrm{dens}_K(G, \mathfrak{c}, m, A) = 0$ if $A \leqslant n_0$ does not hold and hence (12) becomes

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \sum_{A \leqslant n_0} \mathrm{dens}_K(G, \mathfrak{c}, m, A)\,.$$

• We may then suppose that the decomposition $A = (X, Y)$ is non-trivial.

As an aside remark, notice that by [7, Corollary 12] the density $\mathrm{dens}_K(G, m_F)$ is the product of $\mathrm{dens}_K(G, \ell)$ where ℓ varies over the prime divisors of m_F.

Theorem 16. *With the above restrictions (all of which were made without loss of generality) we can write*

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \Big(\sum_{X \leqslant n_0} \mathrm{dens}_K(G, \mathfrak{c}, m_B, X) \Big) \cdot \mathrm{dens}_K(G, m_F)\,. \tag{13}$$

Proof. Consider the notation introduced in this section. If $A = (X, Y)$ and $X \leqslant n_0$ does not hold, then we have $\mathrm{dens}_K(G, \mathfrak{c}, m, A) = 0$. Thus (12) becomes

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \sum_{X \leqslant n_0} \sum_{Y} \mathrm{dens}_K(G, \mathfrak{c}, m, (X, Y)) \,. \tag{14}$$

Fix $A = (X, Y)$ and work in $F = L(m^{-A+1}G)$, which is the compositum of the extensions $F_1 = L(m_B^{-(X+1)}G)$ and $F_2 = K(m_F^{-(Y+1)}G)$. By the restrictions that we made, the fields F_1 and F_2 are linearly disjoint over K.

The density $\mathrm{dens}_K(G, \mathfrak{c}, m, (X, Y))$ can be computed by the Chebotarev Density Theorem because it corresponds to some conjugacy-stable subset $\mathfrak{c}_A$ of $\mathrm{Gal}(F/K)$. We can write $\mathfrak{c}_A = \mathfrak{c}_{A,X} \times \mathfrak{c}_{A,Y}$ by identifying $\mathrm{Gal}(F/K)$ and $\mathrm{Gal}(F_1/K) \times \mathrm{Gal}(F_2/K)$. Considering $\mathfrak{c}_{A,Y}$ in $\mathrm{Gal}(F_2/K)$ gives $\mathrm{dens}_K(G, m_F, Y)$ because by our restrictions the original condition on the Frobenius symbol does not affect the free primes. Considering $\mathfrak{c}_{A,X}$ in $\mathrm{Gal}(F_1/K)$ gives $\mathrm{dens}_K(G, \mathfrak{c}, m_B, X)$. We then deduce

$$\mathrm{dens}_K(G, \mathfrak{c}, m) = \sum_{X \leqslant n_0} \mathrm{dens}_K(G, \mathfrak{c}, m_B, X) \cdot \sum_{Y} \mathrm{dens}_K(G, m_F, Y) \,,$$

which gives the statement. □

We also have the following result:

Theorem 17. *The density* $\mathrm{dens}_K(G, \mathfrak{c}, m)$ *is a computable rational number.*

Proof. The finite sum in (13) is computable and gives a rational number because each summand has these properties. The density $\mathrm{dens}_K(G, m_F)$ is an explicitly computable rational number by the results in [2, 7] because there is no Frobenius condition involved in the density. □

Theorem 18. *Let* $m > 1$ *be a square-free integer. Consider the set of primes* $\mathfrak{p}$ *of* K *such that the multiplicative order of* $(G \bmod \mathfrak{p})$ *has some prescribed* m*-adic valuation and such that* $\mathfrak{p}$ *has some prescribed Frobenius symbol in* L/K*. The natural density of this set is well-defined, and it is a computable rational number.*

Proof. We have already proven the theorem for the special case where the m-adic valuation is the tuple 0 because that means requiring the order of $(G \bmod \mathfrak{p})$ to be coprime to m. If V is some m-adic valuation, then we can apply the statement for the above known case to $m^V G$ and obtain that the multiplicative order of $(G \bmod \mathfrak{p})$ has m-adic valuation at most V. We may then conclude with the help of the inclusion-exclusion principle. □

REFERENCES

[1] K. Chinen and C. Tamura, On a distribution property of the residual order of $a(\mathrm{mod}\, p)$ with a quadratic residue condition, *Tokyo J. Math.* **35** (2012), 441–459.

[2] C. Debry and A. Perucca, *Reductions of algebraic integers*, J. Number Theory, **167** (2016), 259–283.
[3] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist*, Math. Ann. **162** (1965/1966), 74–76.
[4] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist*, Math. Ann. **166** (1966), 19–23.
[5] P. Moree, Artin's primitive root conjecture – a survey, *Integers* **12A** (2012), No. 6, 1305–1416.
[6] P. Moree and B. Sury, Primes in a prescribed arithmetic progression dividing the sequence $\{a^k + b^k\}_{k=1}^{\infty}$, *Int. J. Number Theory* **5** (2009), 641–665.
[7] A. Perucca, *Reductions of algebraic integers II*, to appear in the Proceedings of WINE2, 2018.
[8] V. Ziegler, *On the distribution of the order of number field elements modulo prime ideals.* Unif. Distrib. Theory 1 (2006), no. 1, 65–85.