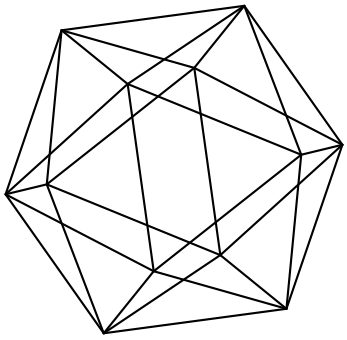
Max-Planck-Institut für Mathematik
Bonn

Computing higher rank primitive root densities

by

Pieter Moree
Peter Stevenhagen



Max-Planck-Institut für Mathematik
Preprint Series 2013 (5)

Computing higher rank primitive root densities

Pieter Moree
Peter Stevenhagen

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands

MPIM 13-5

COMPUTING HIGHER RANK PRIMITIVE ROOT DENSITIES

P. Moree and P. Stevenhagen

Abstract. We extend the "character sum method" for the computation of densities in Artin primitive root problems given by Lenstra and the authors [5] to the situation of radical extensions of arbitrary rank. Our algebraic set-up identifies the key parameters of the situation at hand, and obviates the lengthy analytic multiplicative number theory arguments that used to go into the computation of actual densities. In this way, it leads to dramatic shortenings of existing higher rank proofs, and enables us to extend their range of application in a systematic way.

1. Introduction

Artin's classical 1927 conjecture provides, for an integer $a \neq 0, \pm 1$, a value for the density of the set of primes $q \nmid a$ for which a is a primitive root modulo q. For $q \nmid 2a$, the index $[\mathbf{F}_q^* : \langle a \bmod q \rangle]$ is divisible by n if and only if q splits completely in the splitting field F_n of the polynomial $X^n - a$ over $\mathbf{Q}$, so a is a primitive root modulo q if and only if q does not split completely in any of the fields F_p, with $p < q$ prime. One may therefore expect, with Artin, that a fraction

$$\prod_{p \text{ prime}} \Big(1 - \frac{1}{[F_p : \mathbf{Q}]}\Big) \tag{1.1}$$

of all primes has a as a primitive root. Two problems arise when proving this.

The first problem is of an algebraic nature, and was overlooked for more than 30 years [10]. This problem, which is at the heart of this paper and makes that 1.1 is not in general correct, is the possibility of a *dependency* between the splitting conditions in the various fields F_p. It arises if the Galois group of the compositum of the fields F_p over $\mathbf{Q}$ is a strict subgroup of the product group $\prod_p \mathrm{Gal}(F_p/\mathbf{Q})$, in which it is naturally contained. It leads to the question of how the probability for a prime q to have a certain splitting behavior in the compositum is related to the probabilities of having prescribed splitting behavior in each of the fields F_p.

The second problem is of an analytic nature. It is caused by the fact that the well-known theorem that a 'fraction' $[F_p : \mathbf{Q}]^{-1}$ of all primes splits completely in F_p is an asymptotic statement, and combining these statements for all primes p into a single asymptotic statement is far from trivial, and requires good control of the error terms in the statements involved. Such error terms are only available under assumption of the generalized Riemann hypothesis (GRH) for the fields F_n.

1991 *Mathematics Subject Classification.* Primary 11R45; Secondary 11L03, 11N13.
Key words and phrases. Artin's conjecture, primitive roots.

Hooley [3] showed that, when the algebraic problem is taken into account, the conjectural densities provided by Artin's argument are, under GRH, indeed the correct densities. His argument was extended by Cooke and Weinberger [2] to deal, under GRH, with the case of Artin-type densities over arbitrary number fields.

In the case of Artin's original conjecture, Hooley's argument proves that the density of the set of primes that do not split completely in any of the fields F_n with $n > 1$ equals the inclusion-exclusion value

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{[F_n : \mathbf{Q}]}, \tag{1.2}$$

with μ the Möbius function. For the correct evaluation of this sum, one has to control the algebraic problem that the degree $[F_n : \mathbf{Q}]$ for squarefree values of n may not equal the product of the degrees $[F_p : \mathbf{Q}]$ with $p|n$. If it does so for all squarefree n, then 1.2 equals the Euler product 1.1. In general, one needs to multiply 1.1 by a rational correction factor that takes the entanglement between the fields F_p into account [10].

Well-known variants of Artin's conjecture ask for the density of primes q satisfying more complicated conditions than just having a as a primitive root. One may for instance require that the index of $\langle a \bmod q \rangle$ in $\mathbf{F}_q^*$ be equal to or divisible by some integer, look at $\langle a \bmod q^k \rangle \subset (\mathbf{Z}/q^k\mathbf{Z})^*$ for $k > 1$, or impose an additional congruence condition on q. All these variants can be phrased in terms of the splitting behavior of q in the union $F_\infty = \bigcup_{n \geq 1} F_n$ of all F_n inside some algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. The field F_∞ is obtained by adjoining to $\mathbf{Q}$ the group of radicals

$$R_\infty = \{x \in \overline{\mathbf{Q}}^* : x^k \in \langle a \rangle \quad \text{for some } k > 0\}.$$

The associated Artin-densities can now be given by infinite sums generalizing 1.2 as in [4, formula 2.15], but their explicit evaluation as a rational multiple of the naive Euler product replacing 1.1 tends to lead to nasty calculations, as the field degrees encountered do not always admit an easy description.

The problems arise from the fact that the Galois group of $G = \mathrm{Gal}(\mathbf{Q}(R_\infty)/\mathbf{Q})$ is usually not the product over p of the Galois groups $\mathrm{Gal}(\mathbf{Q}(R_{p^\infty})/\mathbf{Q})$ coming from the adjunction of all p-power roots. It is however shown in [5, Section 2] that G is a closed subgroup of index two of the profinite group

$$A = \mathrm{Aut}_{R_\infty \cap \mathbf{Q}^*}(R_\infty)$$

of group automorphisms of R_∞ fixing the rational numbers in R_∞, and that this larger group A does admit a natural splitting as a product $\prod_p A_p$ of automorphism groups of p-power radicals.

As a profinite group, A naturally comes with a Haar measure ν. The *character sum method* [5, Theorem 3.3] shows that, starting from any reasonable subset

$$S = \prod_p S_p \subset \prod_p A_p = A$$

that characterizes 'good splitting' at each of the p-components, we can *always* decompose the associated Artin-density $\delta(S) = \nu(G \cap S)/\nu(G)$ in a natural way as a product

$$\delta(S) = \frac{\nu(G \cap S)}{\nu(G)} = E \cdot \frac{\nu(S)}{\nu(A)}$$

of the *naive density* $\nu(S)/\nu(A)$ and a rational *entanglement correction factor*

$$E = 1 + \prod_p E_p.$$

Here E_p denotes the average value on S_p of the p-component χ_p of the character

$$\chi = \prod_p \chi_p : A = \prod_p A_p \longrightarrow \{\pm 1\}$$

that has G as its kernel. As we have $\chi_p = 1$ for almost all p, almost all E_p equal 1, and the correction factor $1 + \prod_p E_p$ only involves a finite number of *critical* primes p at which the entanglement of p-power radicals takes place.

When applicable, the method of [5] leads to smooth computations of the densities involved. It is however too restrictive to deal with generalizations of Artin's conjecture that refer to properties of more than a single integer or rational number modulo the prime numbers q under consideration. Already for two rational numbers $a_1, a_2 \in \mathbf{Q}^*$, one may wonder for which fraction of the primes q

1. the subgroup generated by a_1 and a_2 modulo q equals $\mathbf{F}_q^*$;
2. each of a_1 and a_2 is a primitive root modulo q;
3. a_1 and a_2 generate the same subgroup modulo q;
4. a_1 is in the subgroup generated by a_2 modulo q.

The first three problems immediately generalize to $k \geq 2$ rational numbers, and it is clear that many variations of these higher rank primitive root problems exist.

In this paper, we present the extension of our rank-1 result in [5] to arbitrary ranks, and show that it leads to a simple, unified approach to compute higher rank primitive root densities. With minimal effort, we recover the Artin densities for higher rank subgroups due to Cangelmi-Pappalardi [1] in Section 4, and the multiple primitive root densities due to Matthews [6] in Section 5. Our approach explains the structure of the formulas that are found in these papers after cumbersome manipulations of double and triple sums arising from analogues of 1.2. In particular, we see which special cases lead to nice 'multiplicative formulas', and show how a direct application of the method also yields the extension of Matthews result that was recently found by Schinzel [9]. A final section adresses the vanishing problem for primitive root densities, which is more complicated in this higher rank case than it was in the rank-1 case.

2. Radical extensions of the rational number field

Let $\Gamma \subset \mathbf{Q}^*$ be a finitely generated subgroup. We want to explicitly describe the Galois group of the radical extension $\mathbf{Q} \subset \mathbf{Q}(\Gamma_\infty)$ obtained by adjoining to $\mathbf{Q}$ the group

$$\Gamma_\infty = \{x \in \mathbf{C}^* : x^n \in \Gamma \text{ for some } n \in \mathbf{Z}_{\geq 1}\}$$

of complex roots of arbitrary order of the elements in Γ. The group $\Gamma_0 = \Gamma_\infty \cap \mathbf{Q}^*$ is a finitely generated subgroup of $\mathbf{Q}^*$ that contains Γ as a subgroup of finite index. We can choose a $\mathbf{Z}$-basis $\{b_i\}_{i=1}^r$ of positive rational numbers for the subgroup $\Gamma_0^+ = \Gamma_0 \cap \mathbf{Q}_{>0} \subset \mathbf{Q}^*$ of positive elements in Γ_0 and write

$$\Gamma_0 = \Gamma_0^+ \times \langle -1 \rangle = \langle b_1 \rangle \times \langle b_2 \rangle \times \ldots \langle b_r \rangle \times \langle -1 \rangle,$$

with $r \in \mathbf{Z}_{\geq 0}$ the *rank* of Γ. The subgroup of positive real numbers in $\mathbf{C}^*$ naturally forms a $\mathbf{Q}$-vector space, so if we denote by Γ_∞^+ the $\mathbf{Q}$-vector space generated by Γ_0^+, we have

$$\Gamma_\infty = \Gamma_\infty^+ \times \mu_\infty = b_1^{\mathbf{Q}} \times b_2^{\mathbf{Q}} \times \ldots b_r^{\mathbf{Q}} \times \mu_\infty, \tag{2.1}$$

with μ_∞ the group of roots of unity in $\mathbf{C}^*$. As in [5], we analyze the Galois group $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$ in terms of the *Galois representation*

$$G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}) \longrightarrow A = \mathrm{Aut}_{\Gamma_\infty \cap \mathbf{Q}^*}(\Gamma_\infty) = \mathrm{Aut}_{\Gamma_0}(\Gamma_\infty) \tag{2.2}$$

describing the action of G by group automorphisms on the group of radicals Γ_∞. An automorphism $\sigma \in \mathrm{Aut}(\Gamma_\infty)$ that leaves μ_∞ and Γ_0 invariant is determined by the sequences of roots of unity

$$\left\{ \frac{\sigma(b^{1/n})}{b^{1/n}} \right\}_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mu_n$$

by which it multiplies the n-th roots of the elements $b \in \Gamma_0^+$ for $n \in \mathbf{Z}_{\geq 1}$. Here μ_n denotes the group of n-th roots of unity in $\mathbf{C}^*$. We can naturally view such sequences as elements of the Tate module $\widehat{\mu} = \varprojlim_n \mu_n$ of the multiplicative group, and the automorphism σ as a $\widehat{\mu}$-valued homomorphism on Γ_0^+. In this way, we can describe A by the split exact sequence of topological groups forming the lower row of the diagram below:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}(\mu_\infty)) & \longrightarrow & G & \longrightarrow & \mathrm{Gal}(\mathbf{Q}(\mu_\infty)/\mathbf{Q}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle (2.2)} & & \downarrow{\scriptstyle \wr} & & \\
1 & \longrightarrow & \mathrm{Hom}(\Gamma_0^+, \widehat{\mu}) & \longrightarrow & A & \longrightarrow & \mathrm{Aut}(\mu_\infty) & \longrightarrow & 1.
\end{array}$$

In order to describe G as a subgroup of A, we consider the upper row of the diagram, which is exact by Galois theory. As 2.2 induces the familiar isomorphism

$$\mathrm{Gal}(\mathbf{Q}(\mu_\infty)/\mathbf{Q}) \xrightarrow{\sim} \mathrm{Aut}(\mu_\infty) \cong \widehat{\mathbf{Z}}^* = \varprojlim_n (\mathbf{Z}/n\mathbf{Z})^*$$

occurring as the right vertical arrow in the diagram, we can describe $G \subset A$ by identifying the image of $\mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}(\mu_\infty))$ in $\mathrm{Hom}(\Gamma_0^+, \widehat{\mu})$ under the restriction of 2.2, i.e., under the natural left vertical arrow that makes our diagram commute. By Kummer theory, we have an isomorphism

$$\mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}(\mu_\infty)) \xrightarrow{\sim} \mathrm{Hom}(\Gamma_\infty^+/(\Gamma_\infty^+ \cap \mathbf{Q}(\mu_\infty)), \mu_\infty).$$

As in [5, Lemma 2.3], all roots of elements in Γ_0^+ that are in the maximal abelian extension $\mathbf{Q}(\mu_\infty)$ of $\mathbf{Q}$ are *square* roots, so $\Gamma_\infty^+ \cap \mathbf{Q}(\mu_\infty) = (\Gamma_0^+)^{1/2}$ is the group of positive square roots of elements in Γ_0^+. It follows that under 2.2, the subgroup $\mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}(\mu_\infty)) \subset G$ corresponds to the subgroup

$$\mathrm{Hom}(\Gamma_\infty^+/(\Gamma_0^+)^{1/2}, \mu_\infty) = \mathrm{Hom}((\Gamma_0^{1/2})^+, \widehat{\mu}) = 2 \cdot \mathrm{Hom}(\Gamma_0^+, \widehat{\mu}) \subset A.$$

As Γ_0^+ is a free abelian group of rank r, the group $\mathrm{Hom}(\Gamma_0^+, \widehat{\mu}) \cong \bigoplus_{i=1}^r \widehat{\mu}$ is a free $\widehat{\mathbf{Z}}$-module of rank r. It contains $2 \cdot \mathrm{Hom}(\Gamma_0^+, \widehat{\mu})$ as a subgroup of index 2^r. It follows that $G \subset A$ is a subgroup of index 2^r as well.

In field theoretic terms, the index 2^r of G in A reflects the fact that $\mathbf{Q}(\Gamma_\infty)$ is the compositum of $\mathbf{Q}(\Gamma_\infty^+)$ and $\mathbf{Q}(\mu_\infty)$, and that these subfields intersect in the 'multiquadratic' extension $\mathbf{Q}((\Gamma_0^{1/2})^+) = \mathbf{Q}(\{\sqrt{b_i}\}_{i=1}^r)$ of degree 2^r. Thus, if we write an automorphism

$$\alpha \in A = \mathrm{Hom}(\Gamma_0^+, \widehat{\mu}) \rtimes \mathrm{Aut}(\mu_\infty)$$

as $\alpha = (\phi, \sigma)$, and denote the composition of $\phi : \Gamma_0^+ \to \widehat{\mu}$ with the natural map $\widehat{\mu} \to \mu_2$ by ϕ_2, we have

$$\alpha = (\phi, \sigma) \in G \Longleftrightarrow \phi_2(b) = (b^{1/2})^{\sigma - 1} \in \mu_2 \qquad \text{for all } b \in \Gamma_0^+.$$

Here $\sigma \in \mathrm{Aut}(\mu_\infty)$ acts on $b^{1/2} = \sqrt{b} \in \mathbf{Q}(\mu_\infty)$ under the identification $\mathrm{Aut}(\mu_\infty) = \mathrm{Gal}(\mathbf{Q}(\mu_\infty)/\mathbf{Q})$. We find that $G \subset A$ is the subgroup of A that is 'cut out' by quadratic characters $\chi_{[b]} : A \to \mu_2$ coming from elements $b \in \Gamma_0^+$, with

$$\chi_{[b]} : \alpha = (\phi, \sigma) \longmapsto \phi_2(b) \cdot (b^{1/2})^{\sigma - 1}. \tag{2.3}$$

In terms of the generators $b_1, b_2, \ldots, b_r$ of $\Gamma_0^+ = \Gamma_\infty \cap \mathbf{Q}_{>0}$, the injective Galois representation 2.2 fits in an exact sequence

$$1 \to G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}) \xrightarrow{(2.2)} A \xrightarrow{\oplus_{i=1}^r \chi_i} \mu_2^r \to 1, \tag{2.4}$$

where $\chi_i : A \to \mu_2$ denotes the quadratic character corresponding to $b = b_i$ as in 2.3. In words, the exactness of 2.4 means that a group automorphism in $A = \mathrm{Aut}_{\Gamma_0}(\Gamma_\infty)$ is a field automorphism in $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$ if and only if its action on the group

$$(\Gamma_0^+)^{1/2} = \{x \in \overline{\mathbf{Q}}^* : x^2 \in \Gamma_0^+\} = \Gamma_\infty^+ \cap \mathbf{Q}(\mu_\infty)$$

induced by the inclusion map $(\Gamma_0^+)^{1/2} \subset \Gamma_\infty$ coincides with the action via the cyclotomic restriction map $A \to \mathrm{Aut}(\mu_\infty) = \mathrm{Gal}(\mathbf{Q}(\mu_\infty)/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}((\Gamma_0^+)^{1/2}/\mathbf{Q})$. We summarize the discussion in the following way.

2.5. Theorem. *Let $\Gamma \subset \mathbf{Q}^*$ be of rank $r \geq 0$, and define $\Gamma_0^+ = \Gamma_\infty \cap \mathbf{Q}_{>0}$ as above. Then $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$ is a normal subgroup of index 2^r of $A = \mathrm{Aut}_{\Gamma_\infty \cap \mathbf{Q}^*}(\Gamma_\infty)$ under the embedding 2.2, and we have a perfect pairing*

$$\begin{aligned} A/G \times \Gamma_0^+/{\Gamma_0^+}^2 &\longrightarrow \mu_2 \\ (\alpha, b) &\longmapsto \chi_{[b]}(\alpha) \end{aligned}$$

of elementary abelian 2-groups defined by 2.3. □

2.6. Remark. Note that, even though we chose the generating elements $b_i \in \mathbf{Q}^*$ to be positive for the sake of an easy splitting in 2.1, the characters $\chi_{[b]}$ in 2.3 are unchanged if we replace b by $-b$. This is because for $\alpha = (\phi, \sigma) \in A$, definition 2.3 gives us

$$\begin{aligned} \chi_{[-b]}(\alpha) &= \phi_2(-b) \cdot \frac{\sigma(\sqrt{-b})}{\sqrt{-b}} = \phi_2(-1) \cdot \frac{\sigma(\sqrt{-1})}{\sqrt{-1}} \cdot \chi_{[b]}(\alpha) \\ &= \Big(\frac{\alpha(\sqrt{-1})}{\sqrt{-1}}\Big)^2 \cdot \chi_{[b]}(\alpha) = \chi_{[b]}(\alpha). \end{aligned}$$

3. Higher rank entanglement correction

The group μ_∞ of roots of unity is generated by its subgroups μ_{p^∞} of roots of unity of prime power order, for p a prime. In the same way, the radical group Γ_∞, which consists of all roots of arbitrary order of elements in Γ, is generated by its subgroups

$$\Gamma_{p^\infty} = \{x \in \mathbf{C}^* : x^{p^n} \in \Gamma \text{ for some } n \in \mathbf{Z}_{\geq 1}\}$$

of prime power radicals. This gives rise to a natural isomorphism $A \xrightarrow{\sim} \prod_p A_p$, with $A_p = \mathrm{Aut}_{\Gamma_{p^\infty} \cap \mathbf{Q}^*}(\Gamma_{p^\infty})$. In terms of the description of A provided in the previous section, this easily follows from the decompositions $\widehat{\mu} = \prod_p \widehat{\mu}_p$, with $\widehat{\mu}_p = \varprojlim_n \mu_{p^n}$, and $\mathrm{Aut}(\mu_\infty) = \prod_p \mathrm{Aut}(\mu_{p^\infty})$. These yield

$$A \cong \mathrm{Hom}(\Gamma_0^+, \widehat{\mu}) \rtimes \mathrm{Aut}(\mu_\infty) = \prod_p \left[\mathrm{Hom}(\Gamma_0^+, \widehat{\mu}_p) \rtimes \mathrm{Aut}(\mu_{p^\infty})\right].$$

Each of the characters $\chi_{[b]} : A \to \{\pm 1\}$ in 2.3 is continuous, and can uniquely be written as a finite product $\chi_{[b]} = \prod_p \chi_{[b],p}$ of *p-primary* quadratic characters

$$\chi_{[b],p} : A \to A_p \to \{\pm 1\}$$

that factor via a p-component A_p of A for some prime p. This is because $\chi_{[b]}$ is defined as the product of two quadratic characters that each have this property.

The first of these characters maps $\alpha = (\phi, \sigma) \in A$ to $\phi_2(b)$. It describes the action of $\alpha \in A$ on $\sqrt{b} \in \Gamma_{2^\infty} \subset \Gamma_\infty$ and factors via A_2.

The second character maps $\alpha = (\phi, \sigma)$ to $(b^{1/2})^{\sigma - 1} = \sigma(\sqrt{b})/\sqrt{b}$. It factors via the cyclotomic component $\mathrm{Aut}(\mu_\infty) = \mathrm{Gal}(\mathbf{Q}(\mu_\infty)/\mathbf{Q}) \cong \widehat{\mathbf{Z}}^*$ of A, and is the

lift $\chi_K : A \to \widehat{\mathbf{Z}}^* \to \{\pm 1\}$ of the Dirichlet character on $\widehat{\mathbf{Z}}^*$ corresponding to the quadratic field $K = \mathbf{Q}(\sqrt{b})$ of discriminant $d(b)$. We can decompose χ_K as

$$\chi_K = \prod_{p|d(b)} \chi_{K,p}, \tag{3.1}$$

with $\chi_{K,p} : A \to A_p \to \mathbf{Z}_p^* \to \{\pm 1\}$ the lift of a quadratic Dirichlet character of p-power conductor dividing $d(b)$. If $p|d(b)$ is odd, then $\chi_{K,p}$ is the lift of the Legendre symbol at p. If $d(b)$ is even, there are three possibilities for $\chi_{K,2}$. It is the character corresponding to $\mathbf{Q}(i)$ for $d(b) \equiv 4 \bmod 8$, and to one of the fields $\mathbf{Q}(\sqrt{\pm 2})$ for $8|d(b)$.

The profinite groups A_p come with a Haar measure ν_p, and if we normalize these to have $\nu_p(A_p) = 1$ for all p, the product measure $\nu = \prod_p \nu_p$ is a normalized Haar measure on A.

The 'correction factors' occurring in the densities associated to primitive root problems find their origin in the fact that the Galois group $G \subset A$ does not in general decompose as a product $G = \prod_p G_p$, with $G_p = \mathrm{im}[G \to A_p] = \mathrm{Gal}(\mathbf{Q}(\Gamma_{p^\infty})/\mathbf{Q})$. The problem is to determine, for a measurable subset

$$S = \prod_p S_p \subset \prod_p A_p = A$$

that is given as a product of measurable subsets $S_p \subset A_p$, the 'fraction' or density $\delta(S) = \nu(G \cap S)/\nu(G)$ of elements of G that lie in S. It turns out that this density can be written as the product of a *naive density* $\nu(S)/\nu(A)$ that disregards the difference between G and A and a well-structured *entanglement correction factor* E.

3.2. Theorem. *Let $G \subset A$ be the injection from 2.2, and $\nu = \prod_p \nu_p$ the Haar measure on $A = \prod_p A_p$. Take $S = \prod_p S_p \subset A$ a product of ν_p-measurable subsets $S_p \subset A_p$ with $\nu_p(S_p) > 0$. Then we have*

$$\delta(S) = \frac{\nu(G \cap S)}{\nu(G)} = E \cdot \frac{\nu(S)}{\nu(A)},$$

for an entanglement correction factor E given by

$$E = \sum_{\chi \in X} E_\chi = \sum_{\chi \in X} \prod_p E_{\chi,p}.$$

Here $X = \mathrm{Hom}(A/G, \mu_2)$ denotes the dual group of A/G, and the local correction factor

$$E_{\chi,p} = \frac{1}{\nu(S_p)} \int_{S_p} \chi_p d\nu_p$$

of χ at p is the average value on S_p of the p-primary component χ_p of $\chi = \prod_p \chi_p$.

Proof. As A/G is an elementary abelian 2-group of order $[A : G] = 2^r$ by 2.5, we can write the characteristic function of G in A as $1_G = 2^{-r} \sum_{\chi \in X} \chi$.

We can compute $\nu(G \cap S)$ by integrating 1_G over $S \subset A$ with respect to ν. Assume $\nu(S) = \prod_p \nu_p(S_p) > 0$, as the theorem trivially holds in the case $\nu(S) = 0$. Using the equality $\nu(G) = 2^{-r} \cdot \nu(A)$, we easily obtain

$$\frac{\nu(G \cap S)}{\nu(G)} = \frac{2^r}{\nu(A)} \int_S 1_G \, d\nu = \frac{\nu(S)}{\nu(A)} \cdot \sum_{\chi \in X} \left(\frac{1}{\nu(S)} \int_S \chi d\nu \right).$$

Now $\nu(S)$ equals $\prod_p \nu_p(S_p)$, and the integral of $\chi = \prod_p \chi_p$ over $S = \prod_p S_p$ is the product of the values $\int_{S_p} \chi_p d\nu_p$ for all p. The theorem follows. $\square$

We deduce from Theorem 3.2 that the density $\delta(S)$ can vanish for two reasons. The 'obvious' reason for vanishing is that the naive density equals zero, i.e., that the set $S = \prod_p S_p$ we are looking at is a set of measure zero. In Artin-like problems, this trivial reason mostly occurs in cases (excluded in the theorem) where the set S_p is empty for some prime p, and we are trying to impose a kind of splitting behavior that is 'impossible at p'. For instance, a square a will not be a primitive root modulo any odd prime q for the simple reason that every such q splits completely in the field $F_2 = \mathbf{Q}(\sqrt{a}) = \mathbf{Q}$ at $p = 2$. The other, much more subtle reason is that even though S has positive measure, the splitting behavior at p encoded in the sets S_p is incompatible with the entanglement between the fields $\mathbf{Q}(\Gamma_{p^\infty})$ at *different* p. We will discuss this further in Section 6.

4. Artin's conjecture for higher rank subgroups

Let $\Gamma \subset \mathbf{Q}^*$ be a finitely generated subgroup of *positive* rank $r > 0$. Then for all but finitely many primes q, the group Γ consists of q-units, and one may ask for the density of the set of primes q for which the reduction map $\Gamma \to \mathbf{F}_q^*$ is surjective. If $\Gamma = \langle r \rangle$ is cyclic of rank 1, we are in the case of Artin's classical 1927 conjecture, and this generalization is the most obvious higher rank analogue. It may be analyzed in a similar way, as we are now after the density of the set of primes q that do not split completely in any of the fields $M_p = \mathbf{Q}(\Gamma^{1/p})$ generated by

$$\Gamma^{1/p} = \{x \in \mathbf{C}^* : x^p \in \Gamma\},$$

for $p < q$ prime. In this case, the associated set $S = \prod_p S_p \subset A$ of 'good' Frobenius elements is obtained by taking

$$S_p = A_p \setminus \ker \varphi_p \tag{4.1}$$

equal to the complement of the kernel of the natural restriction map

$$\varphi_p : A_p \longrightarrow A(p) = \mathrm{Aut}_{\Gamma^{1/p} \cap \mathbf{Q}^*}(\Gamma^{1/p}). \tag{4.2}$$

The group $A(p) = \mathrm{Aut}_{\Gamma^{1/p} \cap \mathbf{Q}^*}(\Gamma^{1/p})$ is an extension of $\mathrm{Aut}(\mu_p) \cong \mathbf{F}_p^*$ by the dual group $\mathrm{Hom}(\overline{\Gamma}_p, \mu_p)$ of

$$\overline{\Gamma}_p = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*p}].$$

As the natural map $\mathbf{Q}^*/\mathbf{Q}^{*p} \to \mathbf{Q}(\mu_p)^*/\mathbf{Q}(\mu_p)^{*p}$ is injective for all primes p, we have a natural isomorphism

$$\mathrm{Gal}(M_p/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}(\Gamma^{1/p})/\mathbf{Q}) \xrightarrow{\sim} A(p) \tag{4.3}$$

for the Galois group of $M_p = \mathbf{Q}(\Gamma^{1/p})$ over $\mathbf{Q}$ induced by our fundamental map 2.2. In particular, $\ker\varphi_p$ has measure $\nu_p(\ker\varphi_p) = (\#A(p))^{-1} = [M_p : \mathbf{Q}]^{-1}$ for all p. For the measure of S we find the analogue

$$\nu(S) = \frac{\nu(S)}{\nu(A)} = \prod_p \Big(1 - \frac{1}{[M_p : \mathbf{Q}]}\Big) = \prod_p \Big(1 - \frac{1}{(p-1)\#\overline{\Gamma}_p}\Big) \tag{4.4}$$

of the naive density in 1.1. As in the rank-1 case, the density vanishes if and only if $\overline{\Gamma}_2$ is the trivial group, i.e., if and only if Γ consists of squares in $\mathbf{Q}^*$. As $\overline{\Gamma}_p$ has order p^r for almost all primes p, the density in 4.4 is a rational multiple of the *rank-r Artin constant*

$$C_r = \prod_p \left(1 - \frac{1}{(p-1)p^r}\right). \tag{4.5}$$

It is a straightforward application of 3.2 to determine the density of $G \cap S$ in $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$. Under GRH, this is the density of set of the primes q for which $\Gamma \to \mathbf{F}_q^*$ is surjective.

4.6. Theorem. *Let $\Gamma \subset \mathbf{Q}^*$ be finitely generated and of positive rank. Then the density inside A of the subset $S = \prod_p S_p \subset A$ defined by* 4.1 *is given by* 4.4. *If Γ is not contained in $\mathbf{Q}^{*2}$, then S is non-empty, and its density inside the Galois group $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}) \subset A$ from* 2.2 *equals*

$$\frac{\nu(G \cap S)}{\nu(G)} = \left(1 + \sum_{\substack{b \in \overline{\Gamma}_2 \setminus \{1\} \\ d(b) \equiv 1 \bmod 4}} \prod_{p \mid 2 \cdot d(b)} \frac{-1}{[M_p : \mathbf{Q}] - 1}\right) \cdot \frac{\nu(S)}{\nu(A)}.$$

Here we write $M_p = \mathbf{Q}(\Gamma^{1/p})$ and $\overline{\Gamma}_p = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*p}]$ as above, and denote the discriminant of $\mathbf{Q}(\sqrt{b})$ for $b \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ by $d(b)$.

Proof. We computed the density $\nu(S)/\nu(A)$ of S in A in 4.4. For the other statement, which trivially holds for $\nu(S) = 0$, we assume that $\nu(S) = \prod_p \nu_p(S_p)$ is positive. In this case, Theorem 3.2 expresses the density $\nu(G \cap S)/\nu(G)$ of $G \cap S$ in G as the product of $\nu(S)/\nu(A)$ and a correction factor $E = \sum_{\chi \in X} \prod_p E_{\chi,p}$.

To see that the factor E has the form stated, we use the explicit description of $X \cong \Gamma_0^+/\Gamma_0^{+2}$ provided by Theorem 2.5, and compute $E_\chi = \prod_p E_{\chi,p}$ for each of the characters $\chi = \chi_{[b]}$ with $b \in \Gamma_0^+/\Gamma_0^{+2} \subset \mathbf{Q}^*/\mathbf{Q}^{*2}$.

As $S_p = A_p \setminus \ker\varphi_p$ is the set-theoretic difference of a group and a subgroup, the local correction factors

$$E_{\chi,p} = \frac{1}{\nu(S_p)} \left[\int_{A_p} \chi_p \, d\nu_p - \int_{\ker\varphi_p} \chi_p \, d\nu_p\right]$$

at the characters χ come in three different kinds. If χ_p is trivial, we have $E_p = 1$. If χ_p is non-trivial on $\ker\varphi_p$, and consequently on A_p, we have $E_p = 0$ as both integrals vanish, being integrals of a non-trivial character over a group. The most interesting is the remaining third case, in which χ_p is trivial on $\ker\varphi_p$ but not on A_p. It leads to

$$E_{\chi,p} = \frac{-\nu_p(\ker\varphi_p)}{\nu_p(S_p)} = \frac{-[M_p:\mathbf{Q}]^{-1}}{1-[M_p:\mathbf{Q}]^{-1}} = \frac{-1}{[M_p:\mathbf{Q}]-1}. \tag{4.7}$$

For our correction factor $E = \sum_{\chi\in X} E_\chi$, we need to sum over $\chi = \chi_{[b]}$ with $b \in \Gamma_0^+/{\Gamma_0^+}^2$. For $b = \overline{1}$, we have the trivial character and obtain a term $E_\chi = 1$. For $b \neq \overline{1}$, the field $\mathbf{Q}(\sqrt{b})$ is real quadratic, and χ has non-trivial components at the primes dividing $2\cdot d(b)$. For odd primes $p|d(b)$, this component is the lift of the Legendre symbol at p, which is trivial on $\ker\varphi_p$, and $E_{\chi,p}$ is as in 4.7.

For $p = 2$ and $b \neq \overline{1}$ the situation is more involved. Here χ_2 is the product of the character $\psi_{\sqrt{b}} : \alpha = (\phi,\sigma) \mapsto \phi_2(b)$, describing the action of $\alpha \in A$ on $b^{1/2} \in \Gamma_\infty$ as in 2.3, and the lifted Dirichlet character $\chi_{\mathbf{Q}(\sqrt{b}),2}$ of 2-power conductor from 3.1. Note that χ_2 is non-trivial, and that by Remark 2.6, we have

$$\chi_2 = \psi_{\sqrt{b}}\cdot\chi_{\mathbf{Q}(\sqrt{b}),2} = \psi_{\sqrt{-b}}\cdot\chi_{\mathbf{Q}(\sqrt{-b}),2}. \tag{4.8}$$

We find $E_{\chi,2} = 0 = E_\chi$ in case χ_2 is non-trivial on the kernel of

$$\varphi_2 : A \longrightarrow \mathrm{Aut}_{\Gamma^{1/2}\cap\mathbf{Q}^*}(\Gamma^{1/2}) = \mathrm{Hom}(\overline{\Gamma}_2,\mu_2), \tag{4.9}$$

so a non-trivial character $\chi \in X$ only contributes to the sum $E = \sum_\chi E_\chi$, with value

$$E_\chi = \prod_p E_{\chi,p} = \prod_{p|2\cdot d(b)} \frac{-1}{[M_p:\mathbf{Q}]-1},$$

in the cases where its 2-component χ_2 in 4.8 factors via the map φ_2 in 4.9. As the restriction of φ_2 to the subgroup $\mathrm{Aut}(\mu_\infty) = 1\rtimes\mathrm{Aut}(\mu_\infty) \subset A$ factors via $\mathrm{Aut}(\mu_4)$, this does not happen if $d(b)$ (and therefore $d(-b)$) is divisible by 8. If $d(b)$ is not divisible by 8, exactly one of $\chi_{\mathbf{Q}(\sqrt{b}),2}$ and $\chi_{\mathbf{Q}(\sqrt{-b}),2}$ is trivial, and χ_2 factors via φ_2 if and only if the element $b' \in \{b,-b\}$ with $d(b') \equiv 1 \bmod 4$ is contained in $\overline{\Gamma}_2$. Conversely, for $b \in \overline{\Gamma}_2$, either b or $-b$ is in $\Gamma_0^+/{\Gamma_0^+}^2$. This leads to the sum in the statement of the theorem. □

Remark. Theorem 4.6 was originally proved starting from 1.2, with M_p in the place of F_p. Pappalardi [8] first considered a special case, and dealt with the general case together with Cangelmi [1]. Their result looks slightly different, as their "generalized Artin constant" does not include the factor $\nu(S_2)$ that we have in our infinite product 4.4 describing the naive density. To see that 4.6 agrees with Theorem 1 in [1], one can write the entanglement correction factor in 4.6 as

$$\left(1-\frac{1}{[M_2:\mathbf{Q}]}\right)^{-1}\cdot\left(1-\frac{1}{[M_2:\mathbf{Q}]}\sum_{\substack{b\in\overline{\Gamma}_2\\ d(b)\equiv 1 \bmod 4}}\prod_{p|d(b)}\frac{-1}{[M_p:\mathbf{Q}]-1}\right). \tag{4.10}$$

Taking the product with 4.4, the Euler factor at $p = 2$ 'cancels', and one is led to a definition of 4.4 without the factor $\nu(S_2) = 1 - 1/[M_2:\mathbf{Q}]$.

5. Multiple primitive roots

One may generalize Artin's conjecture in a different direction by asking, when given a non-empty finite subset $\{a_1, a_2, \dots, a_n\} \subset \mathbf{Q}^* \setminus \{\pm 1\}$, for the density of the set of primes q for which *each* of the n elements a_i is a primitive root modulo q. This can also be phrased in terms of splitting conditions on q in the field $\mathbf{Q}(\Gamma_\infty)$ of Section 2, with $\Gamma = \langle a_1, a_2, \dots, a_n \rangle \subset \mathbf{Q}^*$ The subgroup generated by the elements a_i. This time, the question does not only depend on Γ, but also on the infinite cyclic subgroups

$$\Gamma_i = \langle a_i \rangle \subset \Gamma$$

generated by each of the a_i. For each Γ_i and prime p, we have restriction maps

$$\varphi_{p,i} : A_p \longrightarrow \mathrm{Aut}_{\Gamma_i^{1/p} \cap \mathbf{Q}^*}(\Gamma_i^{1/p})$$

as in 4.2. As we want to determine the density of the set of primes q that do not split completely in any of the fields $M_{i,p} = \mathbf{Q}(\Gamma_i^{1/p})$, with $p < q$ prime and $i \in \{1, 2, \dots, n\}$, we define the set S_p of good Frobenius elements at p by

$$S_p = A_p \setminus K_p \qquad \text{with} \quad K_p = \bigcup_{i=1}^{n} \ker \varphi_{p,i}, \tag{5.1}$$

and put $S = \prod_p S_p$ in the usual way.

As the subgroups $\ker \varphi_{p,i}$ making up K_p are all contained in the subgroup $\ker[A_p \to \mathrm{Aut}(\mu_p)]$, which has index $p-1$ in A_p, we have $\nu_p(K_p) \leq 1/(p-1)$ for all p. This shows that S_p has positive measure for $p > 2$. For $p = 2$, we have $K_2 = A_2$ and $S_2 = \emptyset$ if and only if there are no elements $\alpha \in A_2$ with $\alpha(\sqrt{a_i}) = -\sqrt{a_i}$ for $i = 1, 2, \dots, n$. This occurs if and only if there is a subset $I \subset \{1, 2, \dots, n\}$ for which

$$\textstyle\prod_{i \in I} a_i \in \mathbf{Q}^* \text{ is a square} \qquad \text{and} \qquad \#I \text{ is odd.} \tag{5.2}$$

If no such I exists, we can uniquely define a homomorphism

$$w_2 : \overline{\Gamma}_2 = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}] \longrightarrow \mu_2 \tag{5.3}$$

by putting $w_2(a_i) = -1$ for all i.

The intersection $\bigcap_{i=1}^n \ker \varphi_{p,i}$ is the subgroup $\ker \varphi_p$ occurring in 4.1. The union $K_p = \bigcup_{i=1}^n \ker \varphi_{p,i}$ is rarely a subgroup for $n \geq 2$, but it is a finite union of a number k_p of cosets of $\ker \varphi_p$. In view of 4.3, the integer $k_p \geq 1$ is the number of elements in $\mathrm{Gal}(M_p/\mathbf{Q})$ that have trivial restriction to at least one of the subfields $M_{i,p} \subset M_p = \mathbf{Q}(\Gamma^{1/p})$. In terms of k_p, the naive density that is the analogue of 4.4 becomes

$$\nu(S) = \frac{\nu(S)}{\nu(A)} = \prod_p \big(1 - \nu_p(K_p)\big) = \prod_p \Big(1 - \frac{k_p}{[M_p : \mathbf{Q}]}\Big). \tag{5.4}$$

The density $\nu(S)$ vanishes if and only if 5.2 holds for some I. In the 'generic' case where Γ is freely generated of rank $r = n \geq 1$ by the a_i, and $\overline{\Gamma}_p = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*p}]$ has order p^r for all p, the integer $k_p = p^r - (p-1)^r$ equals the number of elements in $(\mathbf{Z}/p\mathbf{Z})^r$ having at least one zero-coefficient, and the density 5.4 equals the *Artin constant for r primitive roots*

$$D_r = \prod_p \Big(1 - \frac{p^r - (p-1)^r}{(p-1)p^r}\Big) = \prod_p \Big(1 - \frac{1-(1-1/p)^r}{p-1}\Big). \tag{5.5}$$

For general Γ of free rank $r \geq 1$, the density $\nu(S)$ is a rational multiple of D_r.

As in the previous section, we can apply 3.2 to find the density of $G \cap S$ in $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$. Under GRH, this is the density of set of the primes q for which each of $a_1, a_2, \ldots, a_n$ is a primitive root modulo q.

5.6. Theorem. *Let $\Gamma = \langle a_1, a_2, \ldots, a_n\rangle \subset \mathbf{Q}^*$ be generated by $n \geq 1$ elements $a_i \in \mathbf{Q}^* \setminus \{\pm 1\}$. Then the density inside A of the subset $S = \prod_p S_p$ defined by* 5.1 *is given by* 5.4. *If no subset $I \subset \{1, 2, \ldots, n\}$ satisfies* 5.2, *then S is non-empty, and its density inside the Galois group $G = \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q}) \subset A$ from* 2.2 *equals*

$$\frac{\nu(G \cap S)}{\nu(G)} = \Bigg(\sum_{\substack{a \in \overline{\Gamma}_2 \\ d(a) \equiv 1 \bmod 4}} w_2(a) \prod_{p \mid d(a)} \frac{-k_p}{[M_p : \mathbf{Q}] - k_p} \Bigg) \cdot \frac{\nu(S)}{\nu(A)}.$$

Here w_2 and k_p are as in 5.3 *and* 5.4, *and we use the notation $M_p = \mathbf{Q}(\Gamma^{1/p})$ and $d(a) = \mathrm{disc}(\mathbf{Q}(\sqrt{a}))$ as before.*

Proof. We already computed $\nu(S)$ in 5.4, and we now apply 3.2 to find the correction factor $E = \sum_{\chi \in X} \prod_p E_{\chi,p}$. The analysis is very similar to that in the proof of 4.6, as the only change consists in the replacement of $\ker \varphi_p = A_p \setminus S_p$ in 4.1 by the union $K_p = A_p \setminus S_p$ of k_p cosets of $\ker \varphi_p$ in 5.1.

For characters $\chi \in X$ for which the p-component is trivial on A_p or non-trivial on $\ker \varphi_p$, we find $E_{\chi,p} = 1$ and $E_{\chi,p} = 0$, as before. In particular, the characters contributing to E are of the form $\chi = \chi_{[a]}$ with $a \in \overline{\Gamma}_2$ satisfying $d(a) \equiv 1 \bmod 4$, just as in Theorem 4.6. Let χ be such a character. For primes $p | d(a)$, which are clearly odd, the p-component χ_p of χ is the lift of the Legendre symbol. As χ_p is trivial on $K_p \subset \ker[A_p \to \mathrm{Aut}(\mu_p)]$, we find

$$E_{\chi,p} = \frac{-\nu_p(K_p)}{\nu_p(S_p)} = \frac{-k_p[M_p : \mathbf{Q}]^{-1}}{1 - k_p[M_p : \mathbf{Q}]^{-1}} = \frac{-k_p}{[M_p : \mathbf{Q}] - k_p}.$$

At $p = 2$, the character $\chi_2 = \psi_{\sqrt{a}}$ has, by definition of K_2, the constant value $w_2(a)$ on $S_2 = A_2 \setminus K_2$, so we find $E_{\chi,2} = w_2(a)$. The result follows. $\square$

Theorem 5.6 was originally proved by Matthews [6], who phrases his result in terms of the density

$$c(p) = \frac{k_p}{[M_p : \mathbf{Q}]} = \nu_p(K_p)$$

of the set of primes $q \equiv 1 \bmod p$ with the property that at least one of the generators a_i of Γ is a p-th power modulo q.

In the case where the set $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$ consists of n different prime numbers congruent to 1 mod 4, we have $c(p) = (1 - (1 - 1/p)^r)/(p - 1)$, and the sum of 2^n terms in the correction factor

$$E = \sum_{\substack{a \in \overline{\Gamma}_2 \\ d(a) \equiv 1 \bmod 4}} w_2(a) \prod_{p \mid d(a)} \frac{-k_p}{[M_p : \mathbf{Q}] - k_p} \tag{5.7}$$

in Theorem 5.6 can be rewritten in terms of $D(a) = c(a)/(1 - c(a))$ as a product

$$E = \prod_{a \in \mathcal{A}} \big(1 + D(a)\big) = \prod_{a \in \mathcal{A}} \big(1 + \frac{c(a)}{1 - c(a)}\big). \tag{5.8}$$

For $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$ an arbitrary set of n odd prime numbers, one can adapt 5.8 to 'filter out' only the terms with discriminant $d(a) \equiv 1 \bmod 4$ required in 5.7 by putting

$$E = \frac{1}{2}\Big[\prod_{a \in \mathcal{A}} \big(1 + D(a)\big) + \prod_{a \in \mathcal{A}} \big(1 + \big(\tfrac{-1}{a}\big) D(a)\big)\Big].$$

Similar remarks apply to Theorem 4.6, provided that one uses the formula 4.10 or pays some attention in 4.6 to the factor at $p = 2$. It yields the formulation of the special case of Theorem 4.6 found in [8].

Schinzel [9] extends the particular case of Theorem 5.6 for $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$ a set of odd primes by additionally imposing that the primes q for which each of the primes a_i is a primitive root split in $\mathbf{Q}(\sqrt{2})$ and in m additional quadratic fields of prime conductor $b \in \mathcal{B}$, with $\mathcal{B}$ a set of primes disjoint from $\mathcal{A}$. The $m+1$ additional quadratic conditions change the naive density by a factor $2^{-(m+1)}$, and the proof of his main theorem goes through extensive calculations to obtain the correction factor

$$E = \frac{1}{2}\Big[\prod_{a \in \mathcal{A}} \big(1 + D(a)\big) \prod_{b \in \mathcal{B}} \big(1 - D(b)\big) + \prod_{a \in \mathcal{A}} \big(1 + \big(\tfrac{-1}{a}\big) D(a)\big) \prod_{a \in \mathcal{A}} \big(1 - \big(\tfrac{-1}{b}\big) D(b)\big)\Big].$$

For us, it is an almost trivial modification of the previous result. We take Γ generated by $\mathcal{A} \cup \mathcal{B} \cup \{2\}$, redefine S_2 in the obvious way, and note that the homomorphism $w_2 : \overline{\Gamma}_2 = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}] \longrightarrow \mu_2$ from 5.3, which is now defined by $w_2(a) = -1$ for $a \in \mathcal{A}$ and $w_2(b) = 1$ for $b \in \mathcal{B} \cup \{2\}$, yields again the constant value on S_2 of the character $\psi_{\sqrt{x}}$ for $x \in \overline{\Gamma}_2$.

6. Vanishing criteria

As we observed at the end of Section 3, the density $\delta(S)$ can vanish for the simple reason that S is a zero-set, or for the more subtle reason that, even though S itself has positive density, the entanglement correction factor E vanishes. The occurrence of the simple reason, which amounts to the vanishing of the naive density, is usually easily established. The vanishing of E is only uncomplicated in the rank-1 case, where $E = 1 + E_\chi = 0$ implies that we have

$$E_\chi = \prod_p E_{\chi,p} = -1$$

for the unique non-trivial character $\chi \in X$ in Theorem 3.2. As all $E_{\chi,p}$ are average values of characters χ_p on S_p, and therefore bounded in absolute value by 1, these extreme cases are easily found [5, Corollary 3.4]. For rank $r \geq 2$ however, the vanishing of the correction factor

$$E = 1 + \sum_{\chi \in X \setminus \{1\}} E_\chi$$

with $2^r - 1$ non-trivial terms is not so easily established.

In the case of the higher rank Artin conjecture in Section 4, the naive density vanishes if and only if $\Gamma \subset \mathbf{Q}^{*2}$ consists of squares, making S_2 into the empty set. If the naive density is positive, then so is the actual density, as the correction factor E *never* vanishes in this case. This is immediately obvious in the rank-1 case, when we have $E = 1 + E_\chi$ and $|E_\chi| < 1$ is readily checked. In higher rank cases, this is less immediate, but we know *a priori* that the density will increase if we enlarge Γ from a rank-1 to a higher rank subgroup of $\mathbf{Q}^*$, so there is an easy way out that bypasses an exact analysis of E.

For the multiple primitive root densities in Section 5, the vanishing of the naive density is almost as simple: it vanishes if and only if S_2 is empty, and this is the case where 5.2 applies for some subset $I \subset \{1, 2, \ldots, n\}$. For the vanishing of the density in cases where the naive density is positive, we are dealing with a rather complicated correction factor in Theorem 5.6, and in this case the density *decreases* if we add elements a_i.

In such cases, a promising way to proceed is often to *not* directly use the formula itself, but the structural idea giving rise to it. What Theorem 2.5 expresses is that the nature of the entanglement lies in the relation the splitting behavior at 2 bears to the splitting behavior at the *finitely many* odd primes p at which the elements of Γ can have non-zero valuation. In cases where the splitting condition $S_p \subset A_p$ at p factors through a finite quotient $A_p \to \bar{A}_p$, in the sense that S_p is the inverse image of a subset $\bar{S}_p \subset \bar{A}_p$, it suffices to find a single element of G for which the p-component at $p = 2$ and at the finitely many odd critical primes projects into $\bar{S}_p$ under $A_p \to \bar{A}_p$. This is essentially an explicit version of the observation in [4, Theorem 4.1] that the density can only vanish due to obstructions 'at a finite level' that can be made precise in terms of the input data. In the examples we have in Sections 4 and 5, the map $\varphi_p : A_p \to A(p) \cong \mathrm{Gal}(M_p/\mathbf{Q})$ from 4.2 and 4.3 is such a finite quotient map on A_p that is used to define S_p.

As an illustration, let us derive the vanishing conditions for the entanglement correction factor E in Theorem 5.6 without directly considering the expression for E that is given in the theorem. We only use the fact that the 'splitting condition' S_p that is imposed reflects an actual splitting condition in the field M_p: the set S_p consists of Frobenius classes of primes that do not split completely in any of the subfields $M_{i,p} = \mathbf{Q}(\Gamma_i^{1/p})$.

The assumption that S_2 and therefore S be non-empty amounts to saying that there exist primes q that are inert in all n quadratic fields $\mathbf{Q}(\sqrt{a_i})$, thus satisfying the necessary splitting condition in $M_2 = \mathbf{Q}(\Gamma^{1/2})$. By Theorem 2.5, the only possible implication this can have for the splitting behavior of q in fields $M_p =$

$\mathbf{Q}(\Gamma^{1/p})$ for primes $p > 2$ is that possibly, the splitting behavior of q in the quadratic subfield $\mathbf{Q}(\sqrt{\pm p}) \subset \mathbf{Q}(\mu_p) \subset M_p$ can no longer be freely prescribed at the critical primes p. For primes $p \geq 5$, this will not lead to an incompatibility of local splitting behaviors, as there will be primes q with Frobenius in S_2 (or even with prescribed Frobenius in $\mathrm{Gal}(M_2/\mathbf{Q})$) that satisfy $q \not\equiv 1 \bmod p$ for all critical primes $p \geq 5$. Such q trivially have Frobenius in S_p.

For $p = 3$, where we have $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\mu_3)$, it may however happen that $-3 \in \mathbf{Q}^*/(\mathbf{Q}^*)^2$ is in $\overline{\Gamma}_2$, and that we have $w_2(-3) = 1$. Then *every* q with Frobenius in S_2 is congruent to 1 mod 3, and it can only have Frobenius class in S_3 if there exists a character

$$\chi : \overline{\Gamma}_3 = \mathrm{im}[\Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*3}] \longrightarrow \mu_3 \tag{6.1}$$

that is non-trivial on $a_i \bmod \mathbf{Q}^{*3}$ for $i = 1, 2, \ldots n$. This yields the following algebraic (and more precise) version of the vanishing result for multiple primitive roots. Its derivation in [6, p. 114–118 and p. 138–145] takes a dozen pages.

6.2. Theorem. *Let* $\Gamma = \langle a_1, a_2, \ldots, a_n \rangle \subset \mathbf{Q}^*$ *and* S *be as in Theorem* 5.6*, and suppose no subset* $I \subset \{1, 2, \ldots, n\}$ *satisfies* 5.2*. Then* $S \cap \mathrm{Gal}(\mathbf{Q}(\Gamma_\infty)/\mathbf{Q})$ *has zero density if and only if the following conditions are satisfied:*

(a) *the kernel of the map* $w_2 : \overline{\Gamma}_2 \to \mu_2$ *in* 5.3 *contains* $-3 \bmod \mathbf{Q}^{*2}$;
(b) *the kernel of every character* $\chi : \overline{\Gamma}_3 \to \mu_3$ *contains at least one element* $a_i \bmod \mathbf{Q}^{*3}$.

If none of the a_i *is a cube in* $\mathbf{Q}^*$*, then condition* (b) *does not hold if we have* $n \leq 3$*, or if the* $\mathbf{F}_3$*-rank of* $\overline{\Gamma}_3$ *is either* 1 *or at least* $n - 1$*.*

Proof. The hypothesis concerning 5.2 means that S itself has positive density. As explained above, $\nu(S \cap G) = 0$ in 5.6 can then only occur in the case where condition (a) is satisfied, and the splitting condition S_2 implies that we have primes $q \equiv 1 \bmod 3$ only. For such q, the condition at 3 that q needs to satisfy is that no Frobenius element over q in $\mathrm{Gal}(M_3/\mathbf{Q}(\mu_3))$ fixes a cube root $a_i^{1/3}$, as this is equivalent to a_i being a cube modulo q. The group of characters $\chi : \overline{\Gamma}_3 \to \mu_3$ in 6.1 may be identified, by Kummer theory and the injectivity of the map $\mathbf{Q}^*/\mathbf{Q}^{*3} \to \mathbf{Q}(\mu_3)^*/\mathbf{Q}(\mu_3)^{*3}$, with the Galois group $\mathrm{Gal}(M_3/\mathbf{Q}(\mu_3))$. Condition (b) therefore amounts to saying that every element of $\mathrm{Gal}(M_3/\mathbf{Q}(\mu_3))$ fixes a cube root $a_i^{1/3}$, and we obtain the first half of our theorem.

We finally have to deal with the question whether there exists a character $\chi : \overline{\Gamma}_3 \to \mu_3$ that is non-trivial on each of the generators $\overline{a}_i = a_i \bmod \mathbf{Q}^{*3}$ of $\overline{\Gamma}_3$. For this, it is clearly necessary that each $\overline{a}_i$ is not the trivial element, i.e., none of the a_i is a rational cube. This is also sufficient if the $\mathbf{F}_3$-rank of $\overline{\Gamma}_3$ is n, since then a suitable character χ can simply be defined by choosing non-trivial values $\chi(\overline{a}_i)$. If the $\mathbf{F}_3$-rank equals $n-1 > 0$, there is a single relation expressing one generator, say $\overline{a}_n$, as a product of some other generators $\overline{a}_i$ with exponents ± 1. We now choose the values $\chi(\overline{a}_i) \in \mu_3 \setminus \{1\}$ for $1 \leq i < n$ such that we have $\chi(\overline{a}_n) \neq 1$. For Γ_3 of $\mathbf{F}_3$-rank 1, any isomorphism $\chi : \overline{\Gamma}_3 \xrightarrow{\sim} \mu_3$ does what we want.

For $n \leq 3$, we are automatically in one of the three cases we just dealt with. □

For $n = 4$ and $\overline{\Gamma}_3$ of rank 2, it is possible that both conditions of the theorem hold without any a_i being a cube. This follows from the fact that if a_1 and a_2 are arbitrary and a_3 and a_4 are chosen to satisfy $\overline{a}_3 = \overline{a}_1\overline{a}_2$ and $\overline{a}_4 = \overline{a}_1\overline{a}_2^{-1} \in \overline{\Gamma}_3$, condition (b) will always be satisfied,

Appendix: numerical values

The rank-r Artin constant C_r from (4.5) and the Artin constant for r primitive roots D_r from (5.5) are defined by Euler-products that converge slowly, especially for small values of r. However, there are techniques for rapidly obtaining accurate approximations, see [7].

The table below provides 20 digit decimal approximations of C_r and D_r for $1 \le r \le 7$.

r	C_r	D_r
1	0.37395 58136 19202 28805	0.37395 58136 19202 28805
2	0.69750 13584 96365 90328	0.14734 94000 02001 45807
3	0.85654 04448 53542 17442	0.06082 16551 20305 08600
4	0.93126 51841 60004 33438	0.02610 74463 14917 70808
5	0.96666 88685 96777 51274	0.01156 58420 47143 35542
6	0.98368 26363 12342 05850	0.00525 17580 26977 39754
7	0.99195 72807 75518 31567	0.00243 02267 63032 72703

References

1. L. Cangelmi, F. Pappalardi, *On the r-rank Artin conjecture, II*, J. Number Theory **75** (1999), 120–132.
2. G. Cooke, P.J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to SL2*, Comm. Algebra **3** (1975), 481–524.
3. C. Hooley, *On Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), 209–220.
4. H. W. Lenstra, Jr, *On Artin's conjecture and Euclid's algorithm in global fields*, Inv. Math. **42** (1977), 201–224.
5. H. W. Lenstra, Jr, P. Moree, P. Stevenhagen, *Character sums for primitive root densities*, arXiv:1112.4816 (2011).
6. K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith. **29** (1976), 113–146.
7. P. Moree, *Approximation of singular series and automata*, Manuscripta Math. **101** (2000), no. 3, 385–399.
8. F. Pappalardi, *On the r-rank Artin conjecture*, Math. Comp. **66** (1997), 853–868.
9. A. Schinzel, *Primitive roots and quadratic non-residues*, Acta Arith. **149** (2011), 161-170.
10. P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), 383–391.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

E-mail address: psh@math.leidenuniv.nl

Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany

E-mail address: moree@mpim-bonn.mpg.de