Journal of Number Theory **75**, 120–132 (1999)
Article ID jnth.1998.2319, available online at http://www.idealibrary.com on IDEAL®

On the r-rank Artin Conjecture, II*

Leonardo Cangelmi

Dipartimento di Metodi e Modelli Matematici per le Scienze Applicate,
Università di Roma La Sapienza,
Via Scarpa, 16, 00161 Rome, Italy
E-mail: cangelmi@dmmm.uniroma1.it

and

Francesco Pappalardi

Dipartimento di Matematica, Università Roma TRE,

Communicated by A. Hildebrand

Received March 24, 1998; revised June 12, 1998

For any finitely generated subgroup Γ of $\mathbf{Q}^*$ we compute a formula for the density of the primes for which the reduction modulo p of Γ contains a primitive root modulo p. We use this to conjecture a characterization of "optimal" subgroups (i.e., subgroups that have maximal density). We also improve the error term in the asymptotic formula of Pappalardi's Theorem 1.1 (*Math. Comp.* **66** (1997), 853–868).

1. INTRODUCTION AND STATEMENT OF THE MAIN RESULTS

Let Γ be a finitely generated multiplicative subgroup of $\mathbf{Q}^*$. We denote by supp(Γ) the (finite) set of those primes p such that $v_p(a) \neq 0$ for some $a \in \Gamma$. For all primes p not in supp(Γ), we consider the reduction Γ_p of Γ. Precisely, γ_p is the subgroup of $\mathbf{F}_p^*$ obtained by reducing modulo p all the elements of Γ. We let

$$N_\Gamma(x) = \#\{p \leqslant x,\ p \notin \operatorname{supp}(\Gamma) \mid \Gamma_p = \mathbf{F}_p^*\}. \tag{1}$$

The statement that $N_{\langle a \rangle}(x) \to \infty$ as $x \to \infty$ (when a is an integer $\neq 0$, ± 1 and not a perfect square) is known as the Artin Conjecture for primitive roots. In 1967, Hooley [3] proved that the Generalized Riemann

* Both authors are members of GNSAGA or CNR.

0022-314X/99 $30.00

Hypothesis (GRH) for the Dedekind zeta functions of certain Kummer extensions implies the strong form of the Artin Conjecture:

$$N_{\langle a\rangle}(x) \sim \delta_{\langle a\rangle} \frac{x}{\log x}. \tag{2}$$

Furthermore, Hooley proved that if $a=b^h$ with $b\in\mathbf{Z}$ not a power, then

$$\delta_{\langle a\rangle} = c_a \prod_{\ell\mid h}\left(1-\frac{1}{\ell-1}\right)\prod_{\ell\nmid h}\left(1-\frac{1}{\ell(\ell-1)}\right), \tag{3}$$

where, if $b=b_1b_2^2$ with b_1 square-free, then

$$c_a = \begin{cases} 1 & \text{if} \quad b_1 \not\equiv 1 \pmod 4 \\ 1-\mu(|b_1|)\left(\prod\limits_{\ell\mid h,\,\ell\mid b_1}\dfrac{1}{\ell-2}\prod\limits_{\ell\nmid h,\,\ell\mid b_1}\dfrac{1}{\ell^2-\ell-1}\right) & \\ \qquad \text{if} \quad b_1\equiv 1 \pmod 4. \end{cases} \tag{4}$$

We also recall the very important unconditional theorems in 1984 by Gupta and Murty [1] and in 1986 by Heath-Brown [2]. We summarize their results in the following.

Let a_1, a_2, a_3 be non-zero multiplicatively independent integers such that none of a_1, a_2, a_3, $-3a_1a_2$, $-3a_1a_3$, $-3a_2a_3$, and $a_1a_2a_3$ is a square. Then for at least one $i\in\{1, 2, 3\}$, we have

$$N_{\langle a_i\rangle}(x) \gg \frac{x}{\log^2 x}. \tag{5}$$

As a consequence, the Artin Conjecture is true for almost all integers. More recently, Murty [8], under an hypothesis weaker than GRH, proved that for at least one $i\in\{1, 2, 3\}$ the function $N_{\langle a_i\rangle}(x)$ has a positive density.

The second author proved in [9] that, when $\operatorname{rank}(\Gamma)>1$, the GRH for the Dedekind zeta function of $\mathbf{Q}(\zeta_m, \Gamma^{1/m})$ implies

$$N_\Gamma(x) = \delta_\Gamma \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right), \tag{6}$$

where the implied O-constant can be expressed in terms of Γ, and

$$\delta_\Gamma = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbf{Q}(\zeta_m, \Gamma^{1/m}) : \mathbf{Q}]}. \tag{7}$$

Here $\Gamma^{1/m}$ denotes the set of mth roots of the elements of Γ, and $\zeta_m = \exp(2\pi i/m)$. Furthermore, he proved that, if $p_1, ..., p_r$ are odd primes, then

$$\delta_{\langle p_1, ..., p_r \rangle} = A_r \left(1 - \frac{1}{2^{r+1}} \left(\prod_{i=1}^{r} \left(1 - \frac{(-1/p_i)}{p_i^{r+1} - p_i^r - 1}\right)\right.\right.$$
$$\left.\left.+ \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^{r+1} - p_i^r - 1}\right)\right)\right), \tag{8}$$

where

$$A_r = \prod_{\ell > 2} \left(1 - \frac{1}{\ell^2(\ell - 1)}\right) \tag{9}$$

is called the *r-dimensional Artin Constant*.

The main goal of this note is to extend formulas (3) and (8) to every finitely generated subgroup of $\mathbf{Q}^*$. We let

$$A_\Gamma = \prod_{\ell > 2} \left(1 - \frac{1}{|\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|\,(\ell - 1)}\right) \tag{10}$$

be the *Generalized Artin Constant* of Γ. Moreover, for any $\xi \in \mathbf{Q}^*/\mathbf{Q}^{*2}$, let $s(\xi)$ denote the unique square-free integer such that $\xi = s(\xi)\,\mathbf{Q}^{*2}$.

THEOREM 1. *Let Γ be a finitely generated subgroup of $\mathbf{Q}^*$ of rank r. With the above notation, we have*

$$\delta_\Gamma = A_\Gamma \left(1 - \frac{1}{|\Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2}|} \sum_{\xi \in \tilde{\Gamma}} \mu(|s(\xi)|) \prod_{\ell \mid s(\xi)} \frac{1}{|\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|\,(\ell - 1) - 1}\right), \tag{11}$$

where

$$\tilde{\Gamma} = \{\xi \in \Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2} \mid s(\xi) \equiv 1 \ (\mathrm{mod}\ 4)\}. \tag{12}$$

In Section 2, we prove Theorem 1. In Section 3, we develop some technical results that will be used for the computation of $|\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|$. Using these results, in Section 4 we improve the estimate for the error term of (6).

THEOREM 2. *Let Γ be a finitely generated subgroup of $\mathbf{Q}^*$ of rank $r > 1$. If the GRH holds for the Dedekind zeta function of $\mathbf{Q}(\zeta_m, \Gamma^{1/m})$, then*

$$N_\Gamma(x) = \delta_\Gamma \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{(\log x)^{r+1} (\log \log x)^r}\right), \tag{13}$$

where the implied constant depends only on Γ.

We shall give more precise statements of Theorem 2 in (57), (60), and (61) of Section 4. We point out that (as in Theorem 3.1 of [9]) it is possible to prove unconditionally that

$$N_\Gamma(x) \leqslant (\delta_\Gamma + \mathrm{o}(1)) \frac{x}{\log x}. \tag{14}$$

It is easy to see from (11) that if $\Gamma \subseteq \mathbf{Q}^{*h}$, with $h \in \mathbf{N}$, then

$$\delta_\Gamma \ll \prod_{\substack{\ell > 2 \\ \ell \mid h}} \left(1 - \frac{1}{\ell - 1}\right) \ll \frac{1}{\log \log h}, \tag{15}$$

which shows that there exist infinitely many subgroups of any given rank whose density is arbitrarily small. On the other hand, it was first observed by Lehmer and Lehmer [7] that some integers have higher chances than others to be primitive roots. Indeed, they noticed that -3 is primitive root for about 45% of the primes, while 2 just for about 38% of them. This phenomenon appears also in the higher rank case.

We say that a free subgroup Γ of $\mathbf{Q}^*$ of rank r is *r-optimal* if its density δ_Γ is maximal in the set of all possible densities of free subgroups of $\mathbf{Q}^*$ of rank r. Analogously, we say that a torsion subgroup Γ of $\mathbf{Q}^*$ of rank r is *r-optimal with torsion* if its density δ_Γ is maximal in the set of all possible densities of torsion subgroups of $\mathbf{Q}^*$ of rank r.

It is easy to see by (3) that $\langle -3 \rangle$ is 1-optimal with $\delta_{\langle -3 \rangle} = 3/5 \cdot A_1 \simeq$ 0.44875, and by (11) that $\langle -1, 3 \rangle$ is 1-optimal with torsion with $\delta_{\langle -1, 3 \rangle}$ $= 4/5 \cdot A_1 \simeq 0.59833$. By a careful analysis of (11) and by some evidence given by numerical computations, we are led to state the following.

Claim. Let r be a positive integer, and let $(\ell_i)_{i \geqslant 1}$ be the increasing sequence of all the odd primes.

(1) The subgroup $\langle (-1/\ell_i)\, \ell_i \mid i = 1, ..., r \rangle$ is r-optimal. Its density is

$$A_r \left(1 - \frac{1}{2^r} \prod_{i=1}^{r} \left(1 - \frac{1}{\ell_i^r(\ell_i - 1) - 1}\right)\right). \tag{16}$$

Moreover, a subgroup Γ of $\mathbf{Q}^*$ is r-optimal if and only if $\tilde{\Gamma} = \langle (-1/\ell_i)\, \ell_i \mathbf{Q}^2 \mid i = 1, ..., r \rangle$ and $\Delta_r(\Gamma) = 1$ (the invariant $\Delta_r(\Gamma)$ will be defined in (34)).

(2) The subgroup $\langle -1, \ell_1, ..., \ell_r \rangle$ is r-optimal with torsion. Its density is

$$A_r \left(1 - \frac{1}{2^{r+1}} \prod_{i=1}^{r} \left(1 - \frac{1}{\ell_i^r(\ell_i - 1) - 1}\right)\right). \tag{17}$$

Moreover, a subgroup Γ of $\mathbf{Q}^*$ is r-optimal with torsion if and only if $\tilde{\Gamma} = \langle -\mathbf{Q}^{*2}, \ell_1 \mathbf{Q}^{*2}, ..., \ell_r \mathbf{Q}^{*2} \rangle$ and $\Delta_r(\Gamma) = 1$.

We plan to deal with this claim and some other related problems in a future paper.

2. EVALUATION OF THE DENSITY (PROOF OF THEOREM 1)

Let us rewrite the sum in (7) as

$$\delta_\Gamma = \sum_{j=1}^{\infty} \frac{\mu(j)}{\varphi(j)\, n_j}, \tag{18}$$

where $n_j = [K_j(\Gamma^{1/j}) : K_j]$, with $K_j = \mathbf{Q}(\zeta_j)$.

Henceforth m will denote an odd positive square-free integer, and ℓ an odd positive prime.

We have (see, e.g., [6, Chapter VIII, Section 8])

$$n_m = \prod_{\ell \mid m} [K_m(\Gamma^{1/\ell}) : K_m] = \prod_{\ell \mid m} |\Gamma K_m^{*\ell} / K_m^{*\ell}| = \prod_{\ell \mid m} |\Gamma \mathbf{Q}^{*\ell} / \mathbf{Q}^{*\ell}|, \tag{19}$$

since $\Gamma \cap K_m^{*\ell} = \Gamma \cap \mathbf{Q}^{*\ell}$, while

$$n_{2m} = [K_m(\Gamma^{1/2}) : K_m] \prod_{\ell \mid m} [K_m(\Gamma^{1/\ell}) : K_m] = |\Gamma K_m^{*2} / K_m^{*2}|\, n_m. \tag{20}$$

Furthermore,

$$\frac{\Gamma K_m^{*2}}{K_m^{*2}} \cong \frac{\Gamma}{\Gamma \cap K_m^{*2}} \cong \frac{\Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2}}{(\Gamma \cap K_m^{*2})\, \mathbf{Q}^{*2}/\mathbf{Q}^{*2}}. \tag{21}$$

We set

$$\mathscr{H}_m = (\Gamma \cap K_m^{*2})\, \mathbf{Q}^{*2}/\mathbf{Q}^{*2}, \tag{22}$$

so that

$$n_{2m} = |\Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2}|\, |\mathscr{H}_m|^{-1} \prod_{\ell \mid m} |\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|. \tag{23}$$

We also note that

$$\mathscr{H}_m = \{ \xi \in \Gamma \mathbf{Q}^{*1}/\mathbf{Q}^{*2} \mid s(\xi) \mid m,\ s(\xi) \equiv 1 \pmod 4 \}. \tag{24}$$

Let us split the above sum as the sum $\mathbf{\Sigma_o}$ over odd j's plus the sum $\mathbf{\Sigma_e}$ over even j's. It is immediate to see that

$$\mathbf{\Sigma_o} = \prod_{\ell > 2} \left(1 - \frac{1}{|\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|\,(\ell - 1)}\right) = A_\Gamma. \tag{25}$$

Let us deal with the second sum. We have

$$\mathbf{\Sigma_e} = \sum_{\substack{m=1 \\ (m,2)=1}}^{\infty} \frac{\mu(2m)}{\varphi(2m)\, n_{2m}} = \frac{-1}{|\Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2}|} \sum_{\substack{m=1 \\ (m,2)=1}}^{\infty} \frac{\mu(m)\, |\mathscr{H}_m|}{\varphi(m)\, n_m}. \tag{26}$$

For conciseness, we set $f(m) = \mu(m)/(\varphi(m)\, n_m)$. The function $f(m)$ is multiplicative on odd m's and it is zero on non square-free integers. Then we have

$$\mathbf{\Sigma_e} = \frac{-1}{|\Gamma \mathbf{Q}^{*2}/\mathbf{Q}^{*2}|} \sum_{\substack{m=1 \\ (m,2)=1}}^{\infty} f(m)\, |\mathscr{H}_m|. \tag{27}$$

Note that $\mathscr{H}_m \leqslant \tilde{\Gamma}$ for any m (where $\tilde{\Gamma}$ is defined in (12)). Then

$$\begin{aligned}
&\sum_{\substack{m=1 \\ (m,2)=1}}^{\infty} f(m)\, |\mathscr{H}_m| \\
&\quad = \sum_{\substack{m=1 \\ (m,2)=1}}^{\infty} f(m) \sum_{\xi \in \mathscr{H}_m} 1 && (28)\\
&\quad = \sum_{\xi \in \tilde{\Gamma}} \sum_{\substack{m=1 \\ (m,2)=1,\ \mathscr{H}_m \ni \xi}}^{\infty} f(m) = \sum_{\xi \in \tilde{\Gamma}} f(|s(\xi)|) \sum_{\substack{m=1 \\ (m,2s(\xi))=1}}^{\infty} f(m) && (29)\\
&\quad = \sum_{\xi \in \tilde{\Gamma}} f(|s(\xi)|) \prod_{\substack{\ell > 2 \\ \ell \nmid s(\xi)}} (1 + f(\ell)) \\
&\quad = \prod_{\ell > 2} (1 + f(\ell)) \sum_{\xi \in \tilde{\Gamma}} f(|s(\xi)|) \prod_{\substack{\ell > 2 \\ \ell \mid s(\xi)}} (1 + f(\ell))^{-1}. && (30)
\end{aligned}$$

Finally, using the definition of f and (19), the last expression equals

$$\begin{aligned}
&A_\Gamma \sum_{\xi \in \tilde{\Gamma}} \mu(|s(\xi)|) \prod_{\substack{\ell > 2 \\ \ell \mid s(\xi)}} \frac{1}{n_\ell(\ell - 1)} \left(1 - \frac{1}{n_\ell(\ell - 1)}\right)^{-1} \\
&\quad = A_\Gamma \sum_{\xi \in \tilde{\Gamma}} \mu(|s(\xi)|) \prod_{\substack{\ell > 2 \\ \ell \mid s(\xi)}} \frac{1}{|\Gamma \mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|\,(\ell - 1) - 1}. && (31)
\end{aligned}$$

Substituting (31) into (27) and adding (25) to (27) we obtain (11). This completes the proof. ∎

3. EFFECTIVE COMPUTATION OF THE DENSITY

The purpose of this section is to provide some explicit tools to compute the quantities $\operatorname{rank}(\Gamma)$ and $|\Gamma\mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell}|$, which are necessary for a practical computation of δ_Γ. For simplicity we shall start with the case when Γ is free (i.e., when $-1\notin\Gamma$) and is contained in the group $\mathbf{Q}^+$ of positive rational numbers.

3.1. *The Case $\Gamma\subseteq\mathbf{Q}^+$*

Let Γ be subgroup of $\mathbf{Q}^+$ of rank r, $\{a_1, ..., a_r\}$ be a $\mathbf{Z}$-basis of Γ and $\operatorname{supp}(\Gamma)=\{p_1, ..., p_s\}$. Fix an ordering for the basis and the support, say $(a_1, ..., a_r)$ and $(p_1, ..., p_s)$. Then we can construct the matrix in $\mathrm{M}(s\times r, \mathbf{Z})$

$$M(a_1, ..., a_r)=\begin{pmatrix}\alpha_{1,1} & \cdots & \alpha_{1,r}\\ \vdots & & \vdots\\ \alpha_{s,1} & \cdots & \alpha_{s,r}\end{pmatrix}, \tag{32}$$

where $a_i=p_1^{\alpha_{1,i}}\cdots p_s^{\alpha_{s,i}}$. Indeed, $M(a_1, ..., a_r)$ is the *relations matrix* of $(a_1, ..., a_r)$ with respect to $(p_1, ..., p_s)$ (see [4, Chapter 3]). It is obvious that $\operatorname{rank}(M(a_1, ..., a_r))=r$ (this of course implies $r\leqslant s$) If $(b_1, ..., b_r)$ is another ordered $\mathbf{Z}$-basis of Γ then there exists a matrix $U\in\mathrm{SL}_r(\mathbf{Z})$ such that

$$M(a_1, ..., a_r)=M(b_1, ..., b_r)\cdot U. \tag{33}$$

For any matrix of integers $M\in\mathrm{M}(h\times k, \mathbf{Z})$ and for $i=1, ..., \min(h, k)$, let $\Delta_i(M)$ be the greatest common divisor of the minors of size i of M, while $\Delta_0(M)=1$. For any $i=0, ..., r$, we define

$$\Delta_i(\Gamma)=\Delta_i(M(a_1, ..., a_r)), \tag{34}$$

which is well defined by (33), and does not depend on the ordering of the basis $\{a_1, ..., a_r\}$ or of the support $\{p_1, ..., p_s\}$.

For any positive prime ℓ (including $\ell=2$), we may consider the matrix $M(a_1, ..., a_r)_\ell\in\mathrm{M}(s\times r, \mathbf{F}_\ell)$ obtained by reducing modulo ℓ each entry of $M(a_1, ..., a_r)$. The rank of $M(a_1, ..., a_r)_\ell$ (over $\mathbf{F}_\ell$) equals $\dim_{\mathbf{F}_\ell}(\Gamma\mathbf{Q}^{*\ell}/\mathbf{Q}^{*\ell})$, so it does not depend on the basis, but only on Γ; we shall denote it by $r_\ell(\Gamma)$. Furthermore, $r_\ell(\Gamma)$ is the greatest integer h such that

$\Delta_h(\Gamma) \not\equiv 0 \pmod{\ell}$ (we have $r_\ell(\Gamma)=0$ in case $\Delta_1(\Gamma) \equiv 0 \pmod{\ell}$). Finally $r_\ell(\Gamma)=r$ if and only if $\ell \nmid \Delta_r(\Gamma)$. Hence

$$A_\Gamma = A_r \prod_{\substack{\ell > 2 \\ \ell \mid \Delta_r(\Gamma)}} \left(1 - \frac{\ell^{r-r_\ell} - 1}{\ell^r(\ell-1) - 1}\right), \tag{35}$$

and

$$\delta_\Gamma = A_\Gamma \left(1 - \frac{1}{2^{r_2}} \sum_{\xi \in \tilde{\Gamma}} \mu(|s(\xi)|) \prod_{\ell \mid s(\xi)} \frac{1}{\ell^{r_\ell}(\ell-1) - 1}\right), \tag{36}$$

where $r_\ell = r_\ell(\Gamma)$ for all ℓ's.

3.2. *The General Case* $\Gamma \subseteq \mathbf{Q}^*$

In the general case we let

$$\|\Gamma\| = \{|a| \mid a \in \Gamma\}. \tag{37}$$

It is clear that $\operatorname{rank}(\Gamma) = \operatorname{rank}(\|\Gamma\|)$. The relation between $r_\ell(\Gamma)$ and $r_\ell(\|\Gamma\|)$ is as follows.

Proposition 1. *For $\ell > 2$, $r_\ell(\Gamma) = r_\ell(\|\Gamma\|)$. Moreover,*

$$r_2(\Gamma) = \begin{cases} r_2(\|\Gamma\|) + 1 & \textit{if} \quad -1 \in \Gamma \mathbf{Q}^{*2} \\ r_2(\|\Gamma\|) & \textit{otherwise.} \end{cases} \tag{38}$$

Proof. We consider the epimorphism

$$\begin{gathered} \Gamma \mathbf{Q}^{*\ell} / \mathbf{Q}^{*\ell} \to \|\Gamma\| \, \mathbf{Q}^{*\ell} / \mathbf{Q}^{*\ell} \\ a \mathbf{Q}^{*\ell} \mapsto |a| \, \mathbf{Q}^{*\ell}. \end{gathered} \tag{39}$$

If $\ell > 2$, the kernel is trivial. If $\ell = 2$, the kernel is $(\pm \mathbf{Q}^{*2} \cap \Gamma \mathbf{Q}^{*2}) / \mathbf{Q}^{*2}$. Hence the claim. ∎

If Γ is free of rank r and $\Gamma = \langle a_1, ..., a_r \rangle$, we associate to Γ the matrix in $\mathrm{M}((s+1) \times r, \mathbf{Z})$

$$\tilde{M}(a_1, ..., a_r) = \begin{pmatrix} \alpha_{0,1} & \cdots & \alpha_{0,r} \\ \alpha_{1,1} & \cdots & \alpha_{1,r} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \alpha_{s,1} & \cdots & \alpha_{s,r} \end{pmatrix}, \tag{40}$$

where $\alpha_{0,i} \in \{0, 1\}$ and $a_i = (-1)^{\alpha_{0,i}} p_1^{\alpha_{1,i}} \cdots p_s^{\alpha_{s,i}}$. Note that the matrix $M(|a_1|, ..., |a_r|)$ associated to $\|\Gamma\|$ equals $\tilde{M}(a_1, ..., a_r)$ with the first row removed. Therefore, if we let $M = M(|a_1|, ..., |a_r|)$ and $\tilde{M} = \tilde{M}(a_1, ..., a_r)$ by Proposition 1 we always have that $\mathrm{rank}(\Gamma) = \mathrm{rank}(M)$ and $r_\ell(\Gamma) = \mathrm{rank}(M_\ell)$, for $\ell \neq 2$. On the other hand, it is easy to prove that

$$r_2(\Gamma) = \mathrm{rank}(\tilde{M}_2), \tag{41}$$

where $\tilde{M}_2$ is the reduction modulo 2 of $\tilde{M}$. Then, we let $\Delta_i(\Gamma) = \Delta_i(\|\Gamma\|)$, for $i = 1, ..., r$. Finally, it is clear that formulas (35) and (36) hold also in this case.

Example. Let

$$\Gamma = \langle -3^3 \cdot 11^{15}, 3^3 \cdot 11^3, -3^7 \cdot 13^7, 2^2 \cdot 5^2 \cdot 11 \cdot 13 \rangle. \tag{42}$$

Then $\mathrm{supp}(\Gamma) = (2, 3, 5, 11, 13)$ and the matrix associated to $\|\Gamma\|$ is

$$M = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 3 & 3 & 7 & 0 \\ 0 & 0 & 0 & 2 \\ 15 & 3 & 0 & 1 \\ 0 & 0 & 7 & 1 \end{pmatrix}. \tag{43}$$

So $\Delta_4(\Gamma) = 2^3 \cdot 3^2 \cdot 7$, $r_3(\Gamma) = 2$, and $r_7(\Gamma) = 3$. The matrix associated to Γ is

$$\tilde{M} = \begin{pmatrix} 1 \ 0 \ 1 \ 0 \\ M \end{pmatrix}. \tag{44}$$

Hence $r_2(\Gamma) = 3$ (note that $\mathrm{rank}(M_2) = 2$). Finally

$$\tilde{\Gamma} = \{\mathbf{Q}^{*2}, 33\mathbf{Q}^{*2}, -39\mathbf{Q}^{*2}, -143\mathbf{Q}^{*2}\}. \tag{45}$$

So $A_\Gamma = (314721/331315)\, A_4$ and $c_\Gamma = 746411120668/853041350643$. Hence

$$\delta_\Gamma = \frac{4606103025642228}{5541674413495795} A_4 \simeq 0.831175 \cdot 0.993350 \simeq 0.82565.$$

Note that the density of our claimed optimal free subgroup of rank 4 is about 0.93792 (see (16)).

When Γ is torsion of rank r, then $\Gamma = \langle -1 \rangle \oplus \|\Gamma\|$, and we may assume that $\Gamma = \langle -1, a_1, ..., a_r \rangle$, with $\|\Gamma\| = \langle a_1, ..., a_r \rangle$. By Proposition 1 we have $r_\ell(\Gamma) = r_\ell(\|\Gamma\|)$ for $\ell \neq 2$, and $r_2(\Gamma) = r_2(\|\Gamma\|) + 1$.

3.3. *An Estimate for* $[K_m(\Gamma^{1/m})\colon \mathbf{Q}]$

We do not know whether the formula of the following proposition is known. Since we have not been able to find it in the literature, we give a proof here.

PROPOSITION 2. *Let m be an odd positive integer, Γ a finitely generated subgroup of $\mathbf{Q}^*$, and r the rank of Γ. Then*

$$[K_m(\Gamma^{1/m}) : K_m] = \frac{m^r}{\gcd(m^r, m^{r-1}\Delta_1(\Gamma), ..., m\Delta_{r-1}(\Gamma), \Delta_r(\Gamma))}. \tag{47}$$

Proof. By the same argument that led to (19) we have (see, e.g., [6, Chapter VIII, Section 8])

$$[K_m(\Gamma^{1/m}) : K_m] = \left|\frac{\Gamma\mathbf{Q}^{*m}}{\mathbf{Q}^{*m}}\right|. \tag{48}$$

Now suppose that $\|\Gamma\| = \langle a_1, ..., a_r\rangle$ and $\operatorname{supp}(\Gamma) = \{p_1, ..., p_s\}$. Note that, since m is odd,

$$\begin{aligned}\frac{\Gamma\mathbf{Q}^{*m}}{\mathbf{Q}^{*m}} &\cong \frac{\|\Gamma\|\ \mathbf{Q}^{*m}}{\mathbf{Q}^{*m}} \cong \frac{\langle a_1, ..., a_r, p_1^m, ..., p_s^m\rangle}{\langle p_1^m, ..., p_s^m\rangle}\\ &\cong \frac{\langle p_1, ..., p_s\rangle}{\langle p_1^m, ..., p_s^m\rangle}\Big/\frac{\langle p_1, ..., p_s\rangle}{\langle a_1, ..., a_r, p_1^m, ..., p_s^m\rangle}.\end{aligned} \tag{49}$$

It is clear that $\langle p_1, ..., p_s\rangle/\langle p_1^m, ..., p_s^m\rangle$ has m^s elements. As for $\langle p_1, ..., p_s\rangle/\langle a_1, ..., a_r, p_1^m, ..., p_s^m\rangle$, we consider the relations matrix N of $(a_1, ..., a_r, p_1^m, ..., p_s^m)$ with respect to $(p_1, ..., p_s)$. Letting $M = M(a_1, ..., a_r)$, then $N = (M\ \ mI_s)$. By the theory of finitely generated modules over principal ideal domains (see [4, Chapter 3]), since $N \in \mathrm{M}(s \times (r+s), \mathbf{Z})$, we know that $\langle p_1, ..., p_s\rangle/\langle a_1, ..., a_r, p_1^m, ..., p_s^m\rangle$ has $\Delta_s(N)$ elements (provided that $\Delta_s(N) \neq 0$). Indeed, we can explicitly compute it, observing that

$$\Delta_h(N) = \begin{cases}\gcd(m^{h-i}\Delta_i(M) \mid i = 0, ..., h), & \text{for}\quad h = 1, ..., r\\ m^{h-r}\Delta_r(N), & \text{for}\quad h = r+1, ..., s.\end{cases} \tag{50}$$

It follows that

$$\left|\frac{\langle p_1, ..., p_s\rangle}{\langle a_1, ..., a_r, p_1^m, ..., p_s^m\rangle}\right| = m^{s-r}\gcd(m^r, m^{r-1}\Delta_1(\Gamma), ..., m\Delta_{r-1}(\Gamma), \Delta_r(\Gamma)), \tag{51}$$

hence the claim. ∎

Corollary 1. *Let m be a square-free positive integer, Γ be a finitely generated subgroup of $\mathbf{Q}^*$ of rank r. Then*

$$[K_m(\Gamma^{1/m}):\mathbf{Q}] \geqslant \varphi(m)\,\frac{m^r}{\Delta_r(\Gamma)}\,\frac{1}{2^{r-r_2+\min(r_2,\,\nu(m)-1)}}, \tag{52}$$

where $\nu(m)$ is the number of distinct prime divisors of m.

4. ESTIMATE OF THE ERROR TERM (SKETCH OF THE PROOF OF THEOREM 2)

The proof of Theorem 2 follows the lines of [9, Section 2]. We refer to it for details.

Set $L=\mathbf{Q}(\zeta_m, \Gamma^{1/m})$, n_L its degree over $\mathbf{Q}$, d_L the discriminant of L, and

$$\pi_p(x) = \#\{p \leqslant x \mid p \text{ is unramified and splits completely in } L\}. \tag{53}$$

We use the Hensel inequality (see [10, p. 128, Prop. 5]),

$$\log|d_L| \leqslant n_L\left(\sum_{p\mid d_L} \log p + \log n_L\right), \tag{54}$$

and the effective version of the Chebotarev Density Theorem due to Lagarias and Odlyzko under GRH [5],

$$\pi_m(x) = \frac{1}{n_L}\frac{x}{\log x} + \mathrm{O}(x^{1/2}\log(x d_L^{1/n_L})). \tag{55}$$

Thus we deduce

$$\pi_m(x) = \frac{1}{n_L}\frac{x}{\log x} + \mathrm{O}(x^{1/2}\log(x m^{r+2}\mathscr{P})), \tag{56}$$

where $\mathscr{P} = \prod\{p \mid p \in \operatorname{supp}(\Gamma)\}$.

By an argument similar to that in [9], we obtain from Corollary 1 that

$$\begin{aligned} N_\Gamma(x) = \delta_\Gamma \frac{x}{\log x} + \mathrm{O}\Bigg(&\frac{2^r\Delta_r}{y^r}\frac{x}{\log x} + 2^{\pi(y)} x^{1/2}\log(x e^{(r+2)\vartheta(y)}\mathscr{P}) \\ &+ \pi(z)\,x^{1/2}\log(x z^{r+2}\mathscr{P}) + \left(\frac{x}{z}\right)^{(r+1)/r}\frac{r2^r\log A}{\log(x/z)}\Bigg), \end{aligned} \tag{57}$$

where y and z are parameters, and A equals the product $a_1, ..., a_r$, for some fixed $\mathbf{Z}$-basis $\{a_1, ..., a_r\}$ of Γ.

Now we choose the parameters

$$2^{\pi(y)}=\frac{x^{1/2}}{\log^{r+4} x}, \qquad \pi(z)=\frac{x^{1/2}}{\log^{r+4} x}, \tag{58}$$

which requires us to assume the bound

$$r\leqslant\left(\frac{1}{2}-\delta\right)\frac{\log x}{\log\log x}, \tag{59}$$

for some $\delta\in(0, 1/2)$. Hence

$$N_\Gamma(x)=\delta_\Gamma\frac{x}{\log x}+\mathrm{O}\left(\frac{x}{\log^{r+1} x}\left(\frac{1}{\log x}+\left(\frac{2\log 2}{\delta\log\log x}\right)^r\Delta_r\right.\right.$$
$$\left.\left.+\frac{\log\mathscr{P}}{\log^3 x}+\frac{(\log x)^{2r+6}}{x^{1/2(1-1/r)}}\,r2^r\log A\right)\right), \tag{60}$$

where the implied constant does not depend on Γ, but only on δ.

Furthermore, if $r\leqslant(1/5)(\log x/\log\log x)$ we can simplify this estimate to

$$N_\Gamma(x)=\delta_\Gamma\frac{x}{\log x}+\mathrm{O}\left(\Delta_r\log(A\mathscr{P})\frac{x}{\log^{r+1} x(\log\log x)^{r/2}}\right), \tag{61}$$

where the implied constant does not depend on Γ, nor on r.

On the other hand, we also gather from (60) that, for any fixed Γ of rank r,

$$N_\Gamma(x)=\delta_\Gamma\frac{x}{\log x}+\mathrm{O}\left(\frac{x}{(\log x)^{r+1}\,(\log\log x)^r}\right), \tag{62}$$

where the implied constant depends on Γ.

Corrigendum to "On the r-rank Artin Conjecture" [9]. We point out a mistake in the proof of Theorem 1.1. The Hensel inequality in (2.12) is wrongly stated; it has to be replaced by inequality (54) of the present paper. However, this mistake does not affect the validity of the theorem, since only some minor adjustement is to be done: $m\cdot a_1\cdots a_r$ in (2.13), (2.14), and (2.15) should be replaced by $m^{r+2}a_1\cdots a_r$. The same replacement is to be done in the proof of Theorem 3.1; as a consequence, the upper bound of (3.10) must be replaced by $(\log x)^{1/(3r+5)}$.

ACKNOWLEDGMENT

We thank Paola Cellini for suggesting to us the proof of Proposition 2.

REFERENCES

1. R. Gupta and R. Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984), 127–130.
2. D. R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford (2)* **37** (1986), 27–38.
3. C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
4. N. Jacobson, "Basic Algebra I," 2nd edition, Freeman, New York, 1985.
5. J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), pp. 409–464, Academic Press, London, 1977.
6. S. Lang, "Algebra," 2nd edition, Addison–Wesley, Reading, MA, 1984.
7. D. H. Lehmer and E. Lehmer, Heuristics, anyone?, *in* "Studies in Mathematical Analysis and Related Topics," pp. 202–210, Stanford Univ. Press, Stanford, CA, 1962.
8. R. Murty, Artin's conjecture and elliptic analogues, *in* "Sieve Methods, Exponential Sums, and Their Applications in Number Theory" (G. R. H. Greaves, G. Harman, and M. N. Huxley, Eds.), pp. 325–344, Cambridge Univ. Press, Cambridge, UK, 1996.
9. F. Pappalardi, On the r-rank Artin Conjecture, *Math. Comp.* **66** (1997), 853–868.
10. J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. Inst. Hautes Études Sci.* **54** (1981), 123–201.