ISSN 0012-9593

quatrième série - tome 49 *fascicule 3* *mai-juin 2016*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Joël BELLAÏCHE

Théorème de Chebotarev et complexité de Littlewood

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

Rédaction / *Editor*

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.
Tél. : (33) 1 44 32 20 88. Fax : (33) 1 44 32 20 80.
annales@ens.fr

Édition / *Publication*

Société Mathématique de France
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 Paris Cedex 05
Tél. : (33) 01 44 27 67 99
Fax : (33) 01 40 46 90 96

Abonnements / *Subscriptions*

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 09
Fax : (33) 04 91 41 17 51
email : smf@smf.univ-mrs.fr

Tarifs

Europe : 515 €. Hors Europe : 545 €. Vente au numéro : 77 €.

ISSN 0012-9593

Directeur de la publication : Stéphane Seuret
Périodicité : 6 nos / an

Ann. Scient. Éc. Norm. Sup.
4 e série, t. 49, 2016, p. 579 à 632

THÉORÈME DE CHEBOTAREV ET COMPLEXITÉ DE LITTLEWOOD

PAR JOËL BELLAÏCHE

RÉSUMÉ. – Dans la version effective du théorème de Chebotarev sous l'hypothèse de Riemann généralisée et la conjecture d'Artin (voir le livre d'Iwaniec et Kowalski, *Analytic Number Theory*, § 5.13) apparaît un invariant numérique d'un sous-ensemble D d'un groupe fini G, que nous appelons la *complexité de Littlewood* de D. Nous étudions en détail cet invariant. À l'aide de cette étude, et d'une application du grand crible, nous traitons de manière améliorée deux questions classiques liées à Chebotarev: celle de prouver une majoration du plus petit nombre premier d'un ensemble frobénien, et celle de donner une estimation asymptotique du nombre de nombres premiers ayant des Frobénius donnés dans une famille d'extensions galoisiennes. Nous donnons ensuite des applications concrètes de ces résultats au problème de la factorisation des polynômes à coefficients entiers modulo un nombre premier p, à la conjecture de Lang-Trotter pour les surfaces abéliennes, et à la conjecture de Koblitz, obtenant dans chacun de ces cas des estimations meilleures que celles qu'on trouve dans la littérature.

ABSTRACT. – The effective version of Chebotarev's density theorem under the Generalized Riemann Hypothesis and the Artin conjecture (cf. Iwaniec and Kowalski's *Analytic Number Theory*, § 5.13) involves a numerical invariant of a subset D of a finite group G that we call the Littlewood Complexity of D. We study this invariant in detail. Using this study, and an application of the large sieve, we give improved versions of two standard problems related to Chebotarev: the bound on the first prime in a Frobenian set, and the asymptotics of the set of primes with given Frobenius in an infinite family of Galois extensions. We then give concrete applications to the problem of the factorization of an integral polynomial modulo primes, to the Lang-Trotter conjecture for abelian surfaces, and to the conjecture of Koblitz, with in all three cases better bounds that previously known.

1. Introduction

1.1. Objectifs

Sous l'hypothèse de Riemann généralisée pour les fonctions L d'Artin, que nous noterons comme d'habitude GRH, et sous la conjecture d'Artin, le théorème de Chebotarev admet

une preuve simple et naturelle et une forme effective élégante et forte (cf. [11, page 143]) [(1)], mais qui n'a semble-t-il jamais encore été utilisée. Cette forme effective fait apparaître un invariant d'un sous-ensemble invariant par conjugaison D d'un groupe fini G que nous appelons sa *complexité de Littlewood* $\lambda_G(D)$. Le but de cet article est de commencer une étude détaillée de cet invariant, de prouver un certain nombre de corollaires de ce théorème de Chebotarev et de donner des applications arithmétiques « concrètes » de ces résultats concernant le plus petit nombre premier modulo lequel un polynôme $P \in \mathbb{Z}[X]$ irréductible fixé a une racine (ou bien a au moins deux racines, ou n'en a aucune, ou encore reste irréductible... On pourrait multiplier les variantes, la méthode étant très générale) et la conjecture de Lang-Trotter pour les courbes elliptiques et ses généralisations, notamment aux courbes de genre $g > 1$ et aux variétés abéliennes (cette seconde application combinant l'emploi du théorème de Chebotarev effectif et du grand crible).

Ces résultats se divisent en trois familles, qui sont les suivantes : premièrement le théorème de Chebotarev proprement dit (i.e., concernant la densité des nombres premiers dont le Frobenius dans une extension finie de $\mathbb{Q}$ de groupe de Galois G est dans un certain ensemble invariant par conjugaison $D \subset G$) et les propriétés de la complexité de Littlewood $\lambda_G(D)$; deuxièmement les théorèmes permettant de majorer le plus petit nombre premier dont le Frobenius dans G appartient à D ; troisièmement, les généralisations du théorème de Chebotarev au cas d'une extension infinie, ou d'un système infini d'extensions — ce sont ces généralisations qui sont utiles pour la conjecture de Lang-Trotter par exemple. Dans le reste de cette introduction, nous discutons en détail ces trois familles de résultats et les idées qui les sous-tendent.

1.2. Le théorème de Chebotarev et la complexité de Littlewood

Soit L une extension finie galoisienne [(2)] de $\mathbb{Q}$ de groupe de Galois G. Soit M le produit des nombres premiers ramifiés dans L. Pour p un nombre premier ne divisant pas M, on note Frob_p, (ou $\mathrm{Frob}_{p,G}$ quand il y a une ambiguïté sur l'extension considérée) la classe de conjugaison de l'élément de Frobenius associé à p dans G. Pour f une fonction centrale (i.e., invariante par conjugaison) sur G à valeurs complexes, posons

$$\pi(f,x) = \sum_{p<x, p\nmid M} f(\mathrm{Frob}_p).$$

Associons à f deux invariants : le premier,

$$\mu(f) = \mu_G(f) = \frac{1}{|G|}\sum_{g\in G} f(g)$$

(1) La preuve de cette forme du théorème de Chebotarev apparaît pour la première fois dans l'article [19] de Murty, Murty, et Saradha, et est reprise dans le livre [18] de Murty et Murty mais dans les deux cas le résultat n'est énoncé que sous une forme affaiblie. La forme forte du théorème est énoncée et prouvée par Iwaniec et Kowalski dans leur livre [11]. Il y est également affirmé qu'on peut prouver le même résultat sans supposer la conjecture d'Artin, mais cette affirmation est erronée, comme E. Kowalski me l'a confirmé.

(2) Pour ne pas alourdir les notations, nous ne considérons dans cet article que des extensions de corps de nombres dont le corps de base est $\mathbb{Q}$. Il est en principe toujours possible de se ramener à ce cas.

est simplement la valeur moyenne de f. Le second est

$$\lambda(f) = \lambda_G(f) = \sum_{\pi} |\hat{f}(\pi)| \dim \pi, \tag{1}$$

où π parcourt l'ensemble $\widehat{G}$ des classes d'équivalences de représentations complexes irréductibles de G, et $\hat{f} : \widehat{G} \to \mathbb{C}$ est la *transformée de Fourier* de f, définie par $\hat{f}(\pi) = \frac{1}{|G|} \sum_g \operatorname{tr} f(g)\pi(g^{-1})$. Nous appellerons $\lambda(f)$ la *norme de Littlewood* de f.

L'ensemble des représentations irréductibles π de G telles que $\hat{f}(\pi) \neq 0$ est appelé *support spectral* de f. Comme d'habitude $\mathrm{Li}(x)$ est le logarithme intégral : $\mathrm{Li}(x) = \int_2^x \frac{1}{\log t} dt$.

THÉORÈME 1 (Chebotarev effectif). – *Supposons vraies GRH et la conjecture d'Artin pour les fonctions L d'Artin associées aux représentations irréductibles de* $\mathrm{Gal}(L/\mathbb{Q})$ *qui appartiennent au support spectral de* f. *Il existe une constante absolue* $c_1 > 0$ *telle que pour* $x \geq 3$, *on ait :*

$$|\pi(f, x) - \mu(f)\mathrm{Li}(x)| < c_1 x^{1/2} \lambda(f)(\log x + \log M + \log |G|). \tag{2}$$

Comme cet énoncé diffère, quoique très légèrement, de la forme donnée dans [11], nous expliquons comment le déduire en § 4.1.

Le cas le plus important est celui où f est la fonction indicatrice $\mathbf{1}_D$ d'un sous-ensemble D de G invariant par conjugaison. On note alors $\pi(D, x)$ pour $\pi(f, x)$, et ce nombre est le nombre d'éléments plus petits que x de l'ensemble $\tilde{D}$ des nombres premiers p ne divisant pas M tels que $\mathrm{Frob}_p \in D$. Un ensemble de la forme $\tilde{D}$ sera appelé un ensemble *frobénien*. Nous noterons $\lambda(D)$ pour $\lambda(\mathbf{1}_D)$, et nous appellerons ce nombre réel positif la *complexité de Littlewood* de D. De la même façon, on appellera *support spectral* de D le support spectral de $\mathbf{1}_D$. On a évidemment $\mu(D) = \frac{|D|}{|G|}$ si bien que le théorème de Chebotarev effectif ci-dessus prend la forme :

THÉORÈME 2. – *Supposons vraies GRH et la conjecture d'Artin pour les fonctions L d'Artin associées aux représentations irréductibles de* $\mathrm{Gal}(L/\mathbb{Q})$ *qui appartiennent au support spectral de D. Pour* $x \geq 3$,

$$\left|\pi(D, x) - \frac{|D|}{|G|}\mathrm{Li}(x)\right| < c_1 x^{1/2} \lambda(D)(\log x + \log M + \log |G|). \tag{3}$$

Comme nous l'avons dit, cette forme précise du théorème de Chebotarev effectif n'a à notre connaissance pas été utilisée jusqu'ici (mentionnons tout de même que dans le livre [14] de Kowalski, une variante pour $L/\mathbb{Q}$ remplacée par une extension de corps de fonctions l'est). En revanche, des formes affaiblies de ce résultat ont souvent été utilisées, à savoir celles qu'on obtient en remplaçant $\lambda(D)$ par $|D|$, ce qui revient à appliquer la majoration triviale $\lambda(D) \leq |D|$ — c'est le théorème employé par exemple dans [23], qui est une légère amélioration du théorème de Lagarias et Odlyzko, [15], que nous appellerons ici *la version de Lagarias-Odlyzko-Serre*, ou bien $\lambda(D)$ par $\sqrt{|D|}$ (ce qui revient à appliquer la majoration dite « de Cauchy-Schwarz » $\lambda(D) \leq \sqrt{|D|}$) — c'est le théorème employé par exemple dans [19] et [18], que nous appellerons *la version de Murty-Murty-Saradha*.

Pour obtenir une application du théorème de Chebotarev effectif ci-dessus qui ne soit pas directement conséquence de la version de Murty-Murty-Saradha, il faut donc, dans des cas particuliers intéressants, prouver une meilleure majoration de $\lambda(D)$ que la borne