Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 342 (2006) 289–294
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Théorie des nombres

Une remarque sur l'annulateur du groupe des classes d'idéaux

Francesco Amoroso

Laboratoire N. Oresme, CNRS UMR 6139, université de Caen, BP 5186, 14032 Caen cedex, France

Reçu le 10 septembre 2005 ; accepté après révision le 21 décembre 2005

Disponible sur Internet le 20 janvier 2006

Présenté par Jean-Pierre Serre

Résumé

En utilisant une inégalité pour la hauteur de Weil dans une extension abélienne de $\mathbb{Q}$ ainsi qu'un théorème de Linnik, nous démontrons une minoration de l'indice de l'annulateur du groupe des classes d'idéaux d'un corps cyclotomique, qui est exponentielle en le degré du corps. ***Pour citer cet article : F. Amoroso, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Abstract

A remark on the annihilator of the ideal class group. Using an inequality for the Weil height on an Abelian extension of the rationals and a theorem of Linnik, we prove a lower bound for the index of the annihilator of the ideal class group of a cyclotomic field. This lower bound is exponential in the degree of the field. ***To cite this article: F. Amoroso, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Abridged English version

Introduction

For a natural number $m \not\equiv 2 \bmod 4$ we denote by ζ_m a primitive m-root of unity and we let $K_m = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field of degree $\varphi(m)$ over $\mathbb{Q}$. Let also Γ_m be the Galois group of K_m over $\mathbb{Q}$, whose elements are the maps $\sigma_a : \zeta_m \mapsto \zeta_m^a$, for a integer with $\gcd(a, m) = 1$. We also denote by J the complex conjugation σ_{-1} and by Cl_m^- the minus part of the ideal class group of K_m. Finally, for

$$\psi = \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \gcd(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[\Gamma_m];$$

we let $\|\psi\|_1 = \sum_a |\psi_a|$.

We prove:

Adresse e-mail : amoroso@math.unicaen.fr (F. Amoroso).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2005.12.023

Theorem 0.1. *Let $\psi \in \mathbb{Z}[\Gamma_m]$ and assume $(1-J)\psi \neq 0$ and $\psi \in \mathrm{Ann}(\mathrm{C}l_m^-)$. Then*

$$\|\psi\|_1 \geqslant \frac{1}{2}\big\|(1-J)\psi\big\|_1 \geqslant \frac{\log 5}{12L} \times \frac{\varphi(m)}{\log m},$$

where L is Linnik's constant.[1]

Let now

$$\mathbb{Z}[\Gamma_m]^- = \big\{\psi \in \mathbb{Z}[\Gamma_m] \text{ s.t. } (1+J)\psi = 0\big\} = (1-J)\mathbb{Z}[\Gamma_m],$$

I_m be the Stickelberger ideal and $I_m^- = I_m \cap \mathbb{Z}[\Gamma_m]^-$ its minus part. Then (see [6], Theorem 6.10)

$$I_m^- \subseteq \mathrm{Ann}\big(\mathrm{C}l_m^-\big)^-$$

and (see [5])

$$\big[\mathbb{Z}[\Gamma_m]^- : I_m^-\big] = 2^{a(m)} h_m^-,$$

where $\mathrm{Ann}(\mathrm{C}l_m^-)^- = \mathrm{Ann}(\mathrm{C}l_m^-) \cap \mathbb{Z}[\Gamma_m]^-$ and $a(m) = 0$ if m is a prime power and $a(m) = 2^{k-2} - 1$ if m has $k \geqslant 2$ distinct prime factors. Therefore

$$\log\big[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}\big(\mathrm{C}l_m^-\big)^-\big] \leqslant \log\big[\mathbb{Z}[\Gamma_m]^- : I_m^-\big] = a(m)\log 2 + \log h_m^-.$$

We deduce from Theorem 0.1 the following lower bound for the index of the annihilator.

Theorem 0.2.

$$\log\big[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}\big(\mathrm{C}l_m^-\big)^-\big] \geqslant \left(\frac{c\varphi(m)}{4\log m} - 1\right)\log\left(\frac{2\log m}{c}\right) \gg \frac{\varphi(m)\log\log m}{\log m},$$

where $c = \frac{\log 5}{12L}$ and L is Linnik's constant.

Let us remark that (see [6], Theorem 4.20) $\log h_m^- \sim \frac{1}{4}\varphi(m)\log m$, for $m \to +\infty$; therefore, at least for a prime power m,

$$\log\big[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}\big(\mathrm{C}l_m^-\big)^-\big] \ll \varphi(m)\log m.$$

Proof of Theorem 0.1. We generalize the proof, sketched in the introduction of [4], of the lower bound for the exponent of the class group of K_m. Let

$$\psi = \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \mathrm{pgcd}(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[G]$$

and assume that ψ satisfies the hypothesis of Theorem 0.1. Then, by a theorem of Linnik, there exists a prime number $l \equiv 1 \pmod m$ bounded by

$$l \leqslant m^L$$

for some absolute constant $L > 0$. This prime splits completely in $\mathbb{Z}[\zeta_m]$; let $P \subseteq \mathbb{Z}[\zeta_m]$ be a prime ideal over l. Then $P^\psi = (\gamma)I$ for some $\gamma \in K_m^*$ and for a fractional ideal I which is an extension of a fractional ideal of $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. Let $\alpha = \gamma^{1-J}$ and remark that α is not a root of unity, since $P^{\psi(1-J)} \neq \mathbb{Z}[\zeta_m]$. By the main result of [3], we have the following lower bound for the Weil height of α:

$$h(\alpha) \geqslant \frac{\log 5}{12}. \tag{1}$$

Let now $P_a = \sigma_a P$; then

[1] I.e. the smallest $L > 0$ such that for all integer $m \geqslant 2$ there exists a prime number $l \equiv 1 \bmod m$ such that $l \leqslant m^L$.

$$(\alpha) = (\gamma)^{1-J} = \prod_{\substack{1 \leqslant a \leqslant m-1 \\ \gcd(a,m)=1}} P_a^{\psi_a - \psi_{m-a}}.$$

For the place v_a of K_m corresponding to the prime P_a we have

$$|\alpha|_{v_a}^{n_{v_a}} = l^{\psi_{m-a} - \psi_a}.$$

For all the other places, $|\alpha|_v = 1$. Therefore,

$$\varphi(m)h(\alpha) = \frac{\log l}{2} \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \gcd(a,m)=1}} |\psi_a - \psi_{m-a}| \leqslant \frac{L \log m}{2} \left\| (1-J)\psi \right\|_1. \tag{2}$$

Theorem 0.1 follows from (1) and (2), since

$$(1-J)\psi = \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \mathrm{pgcd}(a,m)=1}} (\psi_a - \psi_{m-a})\sigma_a. \qquad \square$$

Proof of Theorem 0.2. Let $c = \frac{\log 5}{12L}$ and put $N = \frac{\varphi(m)}{2}$ and $n = \frac{c\varphi(m)}{4\log m}$. The set Λ_m of $\psi = \sum_{\substack{1 \leqslant a \leqslant (m-1)/2 \\ \gcd(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[\Gamma_m]$ with $\psi_a \geqslant 0$ and $\|\psi\|_1 \leqslant [n]$ has cardinality

$$\binom{N+[n]}{[n]} \geqslant \left(\frac{N}{n}\right)^{n-1} \geqslant \left(\frac{2\log m}{c}\right)^{\frac{c\varphi(m)}{4\log m} - 1}. \tag{3}$$

Let also remark that

$$\mathrm{Card}\big((1-J)\Lambda_m\big) = \mathrm{Card}(\Lambda_m). \tag{4}$$

Let now ψ and ψ' two distinct elements of $(1-J)\Lambda_m$. Then $(1-J)(\psi - \psi') = 2(\psi - \psi') \neq 0$ and

$$\|\psi - \psi'\|_1 \leqslant 4[n] < \frac{c\varphi(m)}{\log m}.$$

By Theorem 0.1, $\psi - \psi' \notin \mathrm{Ann}(\mathrm{C}l_m^-)$; thus

$$\big[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}\big(\mathrm{C}l_m^-\big)\big] \geqslant \mathrm{Card}\big((1-J)\Lambda_m\big). \tag{5}$$

Theorem 0.2 follows from (3), (4) and (5). $\square$

1. Introduction

Soit m un entier, $m \not\equiv 2 \bmod 4$ et soit ζ_m une racine primitive m-ième de l'unité. Notons $K_m = \mathbb{Q}(\zeta_m)$ et posons $\Gamma_m = \mathrm{Gal}(K_m/\mathbb{Q})$. Pour tout $a \in \mathbb{Z}$, $\mathrm{pgcd}(a,m) = 1$, on note σ_a l'élément de Γ_m tel que $\sigma_a(\zeta_m) = \zeta_m^a$. Notons également $J = \sigma_{-1}$ et $\mathrm{C}l_m^-$ la « partie moins » du groupe des classes d'idéaux de K_m, i.e. le quotient du groupe des classes d'idéaux de K_m par celui de son sous-corps réel maximal $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Soit

$$\psi = \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \mathrm{pgcd}(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[\Gamma_m]\,;$$

on pose : $\|\psi\|_1 = \sum_a |\psi_a|$. Nous démontrons le résultat suivant :

Théorème 1.1. *Soit $\psi \in \mathbb{Z}[\Gamma_m]$. Supposons $(1-J)\psi \neq 0$ et $\psi \in \mathrm{Ann}(\mathrm{C}l_m^-)$. Alors*

$$\|\psi\|_1 \geqslant \frac{1}{2} \left\| \psi(1-J) \right\|_1 \geqslant \frac{\log 5}{12L} \times \frac{\varphi(m)}{\log m},$$

où $L > 0$ est la constante de Linnik.[2]

[2] I.e. le plus petit L tel que pour tout entier $m \geqslant 2$ il existe un nombre premier $l \leqslant m^L$ avec $l \equiv 1 \bmod m$.

Notons

$$\mathbb{Z}[\Gamma_m]^- = \{\psi \in \mathbb{Z}[\Gamma_m] \text{ t.q. } (1+J)\psi = 0\} = (1-J)\mathbb{Z}[\Gamma_m]$$

et soit I_m l'idéal de Stickelberger et $I_m^- = I_m \cap \mathbb{Z}[\Gamma_m]^-$. Alors (cf. [6], Theorem 6.10) :

$$I_m^- \subseteq \mathrm{Ann}(\mathrm{C}l_m^-)^-$$

et, par un théorème de Sinnott (voir [5]) :

$$[\mathbb{Z}[\Gamma_m]^- : I_m^-] = 2^{a(m)} h_m^-,$$

où $\mathrm{Ann}(\mathrm{C}l_m^-)^- = \mathrm{Ann}(\mathrm{C}l_m^-) \cap \mathbb{Z}[\Gamma_m]^-$ et où $a(m) = 0$ si m est une puissance d'un nombre premier et $a(m) = 2^{k-2} - 1$ si m possède $k \geqslant 2$ facteurs premiers distincts. Donc

$$\log[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathrm{C}l_m^-)^-] \leqslant \log[\mathbb{Z}[\Gamma_m]^- : I_m^-] = a(m)\log 2 + \log h_m^-.$$

Nous déduirons du Théorème 1.1 la minoration suivante pour l'indice de l'annulateur :

Théorème 1.2.

$$\log[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathrm{C}l_m^-)^-] \geqslant \left(\frac{c\varphi(m)}{4\log m} - 1\right)\log\left(\frac{2\log m}{c}\right) \gg \frac{\varphi(m)\log\log m}{\log m},$$

où $c = \frac{\log 5}{12L}$ et L est la constante de Linnik.

Remarquons que (cf. [6], Theorem 4.20) :

$$\log h_m^- \sim \frac{1}{4}\varphi(m)\log m,$$

pour $m \to +\infty$ et donc, au moins pour une puissance m d'un nombre premier,

$$\log[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathrm{C}l_m^-)^-] \ll \varphi(m)\log m.$$

2. Preuves

Démonstration du Théorème 1.1. On généralise la preuve de la minoration de l'exposant du groupe de classes de K_m esquissée dans l'introduction de [4]. Soit

$$\psi = \sum_{\substack{1 \leqslant a \leqslant m-1 \\ \mathrm{pgcd}(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[G]$$

qui satisfait aux hypothèses du théorème. Le théorème de Linnik montre qu'il existe un nombre premier $l \equiv 1 \bmod m$ et tel que

$$l \leqslant m^L$$

pour une certaine constante $L > 0$. Le nombre premier l est totalement décomposé dans $\mathbb{Z}[\zeta_m]$; soit P un idéal premier au-dessus de l. Alors : $P^\psi = (\gamma)I$ pour un certain $\gamma \in K_m^*$ et pour un idéal I extension d'un idéal de $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. Notons $\alpha = \gamma^{1-J}$ et remarquons que α n'est pas une racine de l'unité (car $P^{\psi(1-J)} \neq \mathbb{Z}[\zeta_m]$). Le théorème principal de [3] (op. cit., p. 2) montre que

$$h(\alpha) \geqslant \frac{\log 5}{12}. \tag{6}$$

Notons $P_a = \sigma_a P$ ($a = 1, \ldots, m-1$, $\mathrm{pgcd}(a,m) = 1$). On a donc :

$$(\gamma)I = \prod_{\substack{1 \leqslant a \leqslant m-1 \\ \mathrm{gcd}(a,m)=1}} P_a^{\psi_a}$$

et

$$(\alpha)=\prod_{\substack{1\leqslant a\leqslant m-1\\ \gcd(a,m)=1}} P_a^{\psi_a-\psi_{m-a}}.$$

Notons v_a la place finie de K_m correspondant à P_a ; on a alors

$$|\alpha|_{v_a}^{n_{v_a}}=l^{\psi_{m-a}-\psi_a}.$$

Par ailleurs, si v est une place de K_m et $v\neq v_a$, alors $|\alpha|_v=1$. Donc :

$$\begin{aligned}
\varphi(m)h(\alpha)&=\sum_{\substack{1\leqslant a\leqslant m-1\\ \gcd(a,m)=1}}\log\max\bigl\{|\alpha|_{v_a}^{n_{v_a}},1\bigr\}\\
&=\sum_{\substack{1\leqslant a\leqslant m-1\\ \gcd(a,m)=1}}\max(\psi_{m-a}-\psi_a,0)\log l\\
&=\frac{\log l}{2}\sum_{\substack{1\leqslant a\leqslant m-1\\ \gcd(a,m)=1}}|\psi_a-\psi_{m-a}|\\
&\leqslant\frac{L\log m}{2}\bigl\|(1-J)\psi\bigr\|_1.
\end{aligned}\tag{7}$$

La conclusion désirée découle des formules (6) et (7) en remarquant que

$$(1-J)\psi=\sum_{\substack{1\leqslant a\leqslant m-1\\ \mathrm{pgcd}(a,m)=1}}(\psi_a-\psi_{m-a})\sigma_a.\qquad\Box$$

Démonstration du Théorème 1.2. On pose

$$N:=\frac{\varphi(m)}{2}\quad\text{et}\quad n:=\frac{c\varphi(m)}{4\log m},$$

où $c=\frac{\log 5}{12L}$. L'ensemble

$$\Lambda_m:=\Biggl\{\psi=\sum_{\substack{1\leqslant a\leqslant (m-1)/2\\ \mathrm{pgcd}(a,m)=1}}\psi_a\sigma_a\in\mathbb{Z}[\Gamma_m]\text{ t.q. }\psi_a\geqslant 0,\ \|\psi\|_1\leqslant[n]\Biggr\}$$

est de cardinal

$$\binom{N+[n]}{[n]}\geqslant\left(\frac{N}{n}\right)^{n-1}\geqslant\left(\frac{2\log m}{c}\right)^{\frac{c\varphi(m)}{4\log m}-1}.\tag{8}$$

Remarquons aussi que

$$\mathrm{Card}\bigl((1-J)\Lambda_m\bigr)=\mathrm{Card}(\Lambda_m).\tag{9}$$

Soient $\psi,\psi'\in(1-J)\Lambda_m$ avec $\psi\neq\psi'$. Alors $(1-J)(\psi-\psi')=2(\psi-\psi')\neq 0$ et

$$\|\psi-\psi'\|_1\leqslant 4[n]<\frac{c\varphi(m)}{\log m}.$$

Le Théorème 1.1 nous assure donc : $\psi-\psi'\notin\mathrm{Ann}(\mathrm{C}l_m^-)$, ce qui montre que :

$$\bigl[\mathbb{Z}[\Gamma_m]^-:\mathrm{Ann}\bigl(\mathrm{C}l_m^-\bigr)\bigr]\geqslant\mathrm{Card}\bigl((1-J)\Lambda_m\bigr).\tag{10}$$

Les relations (8), (9) et (10) donnent la conclusion cherchée. $\Box$

Si l'on admet l'hypothèse de Riemann généralisée, le Théorème 1.1 peut être généralisé à des extensions abéliennes imaginaires et même CM, (en utilisant, comme on l'a fait dans [4] pour minorer l'exposant du groupe de classes d'un corps CM, le résultat principal de [2] à la place de la minoration de la hauteur de [3]). Plus généralement, en utilisant des techniques additionnelles de géométrie des nombres, on peut traiter également des corps « proche » d'un corps CM, par exemple les corps engendrés par un petit nombre de Salem. Tous ces résultats font l'objet de l'article [1].

Remerciements

Je tiens à remercier B. Anglès pour plusieurs discussions qui ont motivé ce travail et pour avoir bien voulu me faire part de ses commentaires sur une version initiale de cet article.

Références

[1] F. Amoroso, Groupes de classes de corps de « type CM », Rapport de Recherche LMNO 2005-17.
[2] F. Amoroso, S. David, Le problème de Lehmer en dimension supérieure, J. Reine Angew. Math. 513 (1999) 145–179.
[3] F. Amoroso, R. Dvornicich, A lower bound for the height in Abelian extensions, J. Number Theory 80 (2) (2000) 260–272.
[4] F. Amoroso, R. Dvornicich, Lower bounds for the height and size of the ideal class group in CM fields, Monatsh. Math. 138 (2) (2003) 85–94.
[5] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. Math. (2) 108 (1978) 107–134.
[6] L.C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.