

AperTO - Archivio Istituzionale Open Access dell'Università di Torino

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

### **This is the author's manuscript**

*Original Citation:*

*Availability:*

This version is available <http://hdl.handle.net/2318/1944869> since 2023-11-28T14:42:27Z

*Published version:*

DOI:10.1016/j.crma.2005.12.023

*Terms of use:*

Open Access

Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)

authorlabel1]Francesco Amoroso amoroso@math.unicaen.fr  
 [authorlabel1]Laboratoire N. Oresme, CNRS UMR 6139 – Université de  
 Caen, BP 5186 – 14032 Caen Cédex, France

### Abstract

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 ??? (200?).*

### 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 ??? (200?).*

## Abridged English version

### 1 Introduction

For a natural number  $m \not\equiv 2 \pmod{4}$  we denote by  $\zeta_m$  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  $\Gamma_m$  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  $\sigma_{-1}$  and by  $Cl_m^-$  the minus part of the ideal class group of  $K_m$ . Finally, for

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

we let  $\|\psi\|_1 = \sum_a |\psi_a|$ . We prove:

**Théorème 1.1** *Let  $\psi \in \mathbb{Z}[\Gamma_m]$  and assume  $(1 - J)\psi \neq 0$  and  $\psi \in \text{Ann}(Cl_m^-)$ . Then*

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

where  $L$  is Linnik's constant<sup>1</sup>.

Let now

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

---

1. i.e. the smallest  $L > 0$  such that for all integer  $m \geq 2$  there exists a prime number  $l \equiv 1 \pmod{m}$  such that  $l \leq m^L$ .

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

$$I_m^- \subseteq \text{Ann}(Cl_m^-)^-$$

and (see [?])

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

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

$$\log [\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)^-] \leq \log [\mathbb{Z}[\Gamma_m]^- : I_m^-] = a(m) \log 2 + \log h_m^-.$$

We deduce from theorem (??) the following lower bound for the index of the annihilator.

### **Théorème 1.2**

$$\log [\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)^-] \geq \left( \frac{c\varphi(m)}{4 \log m} - 1 \right) \log \left( \frac{2 \log m}{c} \right) \gg \frac{\varphi(m) \log \log m}{\log m},$$

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

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

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

## **2 Proofs**

**Proof of theorem ??:** We generalize the proof, sketched in the introduction of [?], of the lower bound for the exponent of the class group of  $K_m$ . Let

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

and assume that  $\psi$  satisfies the hypothesis of theorem ???. Then, by a theorem of Linnik, there exists a prime number  $l \equiv 1 \pmod{m}$  bounded by

$$l \leq m^L$$

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  $\alpha$  is not a root of unity, since  $P^{\psi(1-J)} \neq \mathbb{Z}[\zeta_m]$ . By the main result of [?], we have the following lower bound for the Weil height of  $\alpha$ :

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

Let now  $P_a = \sigma_a P$ ; then

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

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,

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

Theorem ?? follows from (??) and (??), since

$$(1-J)\psi = \sum_{\substack{1 \leq a \leq m-1 \\ \gcd(a,m)=1}} (\psi_a - \psi_{m-a})\sigma_a.$$

□

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

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

Let also remark that

$$\text{Card}((1-J)\Lambda_m) = \text{Card}(\Lambda_m). \quad (4)$$

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

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

By theorem ??,  $\psi - \psi' \notin \text{Ann}(Cl_m^-)$ ; thus

$$[\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)] \geq \text{Card}((1-J)\Lambda_m). \quad (5)$$

Theorem ?? follows from (??), (??) and (??). □

## Version française

### 1 Introduction

Soit  $m$  un entier,  $m \not\equiv 2 \pmod{4}$  et soit  $\zeta_m$  une racine primitive  $m$ -ième de l'unité. Notons  $K_m = \mathbb{Q}(\zeta_m)$  et posons  $\Gamma_m = \text{Gal}(K_m/\mathbb{Q})$ . Pour tout  $a \in \mathbb{Z}$ ,

$\text{pgcd}(a, m) = 1$ , on note  $\sigma_a$  l'élément de  $\Gamma_m$  tel que  $\sigma_a(\zeta_m) = \zeta_m^a$ . Notons également  $J = \sigma_{-1}$  et  $Cl_m^-$  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

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

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  $\psi \in \text{Ann}(Cl_m^-)$ . Alors*

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

où  $L > 0$  est la constante de Linnik<sup>2</sup>.

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. [?], theorem 6.10) :

$$I_m^- \subseteq \text{Ann}(Cl_m^-)^-$$

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

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

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

$$\log [\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)^-] \leq \log [\mathbb{Z}[\Gamma_m]^- : I_m^-] = a(m) \log 2 + \log h_m^-.$$

Nous déduirons du théorème ?? la minoration suivante pour l'indice de l'annulateur :

**Théorème 1.2**

$$\log [\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)^-] \geq \left( \frac{c\varphi(m)}{4 \log m} - 1 \right) \log \left( \frac{2 \log m}{c} \right) \gg \frac{\varphi(m) \log \log m}{\log m},$$

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

Remarquons que (cf. [?], theorem 4.20) :

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

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

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

---

2. *i.e.* le plus petit  $L$  tel que pour tout entier  $m \geq 2$  il existe un nombre premier  $l \leq m^L$  avec  $l \equiv 1 \pmod{m}$ .

## 2 Preuves

**Démonstration du théorème ?? :** On généralise la preuve de la minoration de l'exposant du groupe de classes de  $K_m$  esquissée dans l'introduction de [?]. Soit

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

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

$$l \leq m^L$$

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  $\alpha$  n'est pas une racine de l'unité (car  $P^{\psi(1-J)} \neq \mathbb{Z}[\zeta_m]$ ). Le théorème principal de [?] (op. cit., p. 2) montre que

$$h(\alpha) \geq \frac{\log 5}{12}. \quad (6)$$

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

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

et

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

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 :

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

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

$$(1 - J)\psi = \sum_{\substack{1 \leq a \leq m-1 \\ \text{pgcd}(a, m) = 1}} (\psi_a - \psi_{m-a})\sigma_a .$$

□

**Démonstration du théorème ??.** 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

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

est de cardinal

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

Remarquons aussi que

$$\text{Card}((1 - J)\Lambda_m) = \text{Card}(\Lambda_m). \quad (9)$$

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

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

Le théorème ?? nous assure donc :  $\psi - \psi' \notin \text{Ann}(Cl_m^-)$ , ce qui montre que :

$$[\mathbb{Z}[\Gamma_m]^- : \text{Ann}(Cl_m^-)] \geq \text{Card}((1 - J)\Lambda_m). \quad (10)$$

Les relations (??), (??) et (??) donnent la conclusion cherchée. □

Si l'on admet l'hypothèse de Riemann généralisée, le théorème ?? peut être généralisé à des extensions abéliennes imaginaires et même CM, (en utilisant, comme on l'a fait dans [?] pour minorer l'exposant du groupe de classes d'un corps CM, le résultat principal de [?] à la place de la minoration de la hauteur de [?]). 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 [?].

## 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.

## References

- [1] F. Amoroso. Groupes de classes de corps de « type CM ». Rapport de Recherche LMNO 2005-17.
- [2] F. Amoroso and S. David. Le problème de Lehmer en dimension supérieure. *J. reine angew. Math.* 513, 145–179 (1999).
- [3] F. Amoroso and R. Dvornicich. A Lower Bound for the Height in Abelian Extensions, *J. Number Theory* 80, no. 2, 260–272 (2000).
- [4] F. Amoroso and R. Dvornicich. Lower bounds for the height and size of the ideal class group in CM fields. *Monatsh. Math.* 138, No.2, 85-94 (2003).
- [5] W. Sinnott. On the Stickelberger ideal and the circular units of a cyclotomic field. *Ann. Math. (2)* 108, 107-134 (1978).
- [6] L.C. Washington. *Introduction to Cyclotomic Fields*. Springer–Verlag, New York (1982).