Une remarque sur les facteurs de h_p^+

Gabriele Ranieri

Une remarque sur les facteurs de h_p^+.

Gabriele Ranieri

1 Introduction.

Soit p un nombre premier tel que $m = (p-1)/2$ soit une puissance d'un nombre premier impair ou deux fois une puissance d'un nombre premier impair, de telle sorte que $(\mathbb{Z}/m\mathbb{Z})^*$ soit cyclique. Dans ce travail nous déterminons une majoration pour les nombres premiers l divisant l'ordre h_p^+ du groupe des classes d'idéaux du corps $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ et tels que l est une racine primitive modulo m. Notre preuve repose sur une minoration de la hauteur due à Schinzel (paragraphe 2), et sur des propriétés bien connues des anneaux de groupe (paragraphe 3). Plus précisément, grâce au résultat de Schinzel et à la relation $[E_p^+ : C_p^+] = h_p^+$ entre le groupe E_p^+ des unités de $\mathbb{Z}[\zeta_p + \overline{\zeta_p}]$ et le sous-groupe C_p^+ des unités cyclotomiques, nous prouvons qu'il existe une unité $\beta \in E_p^+ \backslash C_p^+$ telle que $\beta^l \in C_p^+$, et telle que la hauteur de Weil de β est $\geq Cl$, où C est une certaine constante. Ensuite, en utilisant les propriétés démontrées dans le troisième paragraphe, nous prouvons qu'on peut choisir l'élément β, de telle sorte que la valeur absolue des coefficients de β^l dans une base bien déterminée de C_p^+ soit majorée par $\phi(m)$. En remarquant que la hauteur de Weil des éléments de cette base déterminée de C_p^+ est elle-même majorée par $\log(2)$, nous montrons (paragraphe 4) le théorème suivant :

Théorème 1 *Soit p un nombre premier, soit $m = (p-1)/2$ et soit l un nombre premier divisant le cardinal h_p^+ du groupe des classes d'idéaux du corps $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ et tel que sa classe modulo m engendre $(\mathbb{Z}/m\mathbb{Z})^*$. Alors p et l satisfont la relation suivante :*

$$l \leq \frac{2\log(2)}{\log\left((1+\sqrt{5})/2\right)}\, m\, \phi(m).$$

Remerciements. Je tiens à remercier F. Amoroso, B. Anglès et R. Dvornicich qui ont bien voulu m'aider pendant la réalisation de ce travail. Je tiens également à remercier D. Simon pour avoir relu une version préliminaire de cet article.

2 Une Minoration pour la hauteur.

Le premier lemme, appelé Lemme de Schinzel, nous donne une minoration pour la hauteur de Weil h d'un nombre algébrique qui appartient à un corps totalement réel ou CM.

Lemme 1 *Soit K un corps de nombres totalement réel ou CM, et soit $\alpha \in K^*$ un nombre entier algébrique tel que α n'est pas une racine de l'unité. Alors :*

$$h(\alpha) \geq C = \log\left(\sqrt{\frac{1+\sqrt{5}}{2}}\right).$$

Preuve. Voir [Sch 1973]. □

Soit p un nombre premier, et soient E_p^+, C_p^+ respectivement le groupe des unités et le groupe des unités cyclotomiques de $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Il est bien connu (voir par exemple [Was 1997], Theorem 8.2) que l'indice $[E_p^+ : C_p^+]$ est égal au cardinal h_p^+ du groupe des classes d'idéaux de $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$, et donc, pour tout premier l divisant h_p^+, il existe un élément $\beta \in E_p^+$, dont la classe dans E_p^+/C_p^+ soit exactement d'ordre l. Notre but est déterminer une fonction f telle que, pour tout premier l divisant h_p^+, il existe $\beta \in E_p^+$ tel que :

$$h(\beta^l) \leq f(p)$$

et telle que, si p tend vers $+\infty$, alors $f(p) \leq p^n$ où n est un entier fixé. Grâce au Lemme 1, une telle fonction fournit alors la majoration suivante :

$$l \leq \frac{f(p)}{C}.$$

3 Quelques propriétés des anneaux de groupes.

Nous rappelons ici quelques propriétés bien connues des anneaux de groupes. Soit G un groupe abélien fini, et F un corps commutatif dont la caractéristique ne divise pas l'ordre de G. Soit aussi $\hat{G}$ le groupe des caractères de G à valeur dans une clôture algébrique $\overline{F}$ fixée de F. Les groupes G et $\hat{G}$ sont isomorphes (voir [Was 1997], Lemme 3.1) et donc ils sont du même ordre. Soit $\omega \in \overline{F}$ une racine primitive de l'unité d'ordre $|G|$. Alors, pour tout caractère $\chi \in \hat{G}$, l'image de χ est contenue dans le corps $F(\omega)$. Soit Γ le groupe $\mathrm{Gal}(F(\omega)/F)$ et posons :

$$\varepsilon_\chi = \frac{1}{|G|}\sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in F(\omega)[G].$$

Les éléments ε_χ, qui sont bien définis car par hypothèse la caractéristique de F ne divise pas $|G|$, satisfont les propriétés suivantes :
(1) $\varepsilon_\chi \varepsilon_\psi = \delta_{\chi,\psi}$ pour tout $\chi, \psi \in \hat{G}$.
(2) $\sum_{\chi \in \hat{G}} \varepsilon_\chi = 1$.
(3) $\sigma \varepsilon_\chi = \chi(\sigma)\varepsilon_\chi$ pour tout $\sigma \in G$.
Par ces propriétés, on obtient tout de suite que :

$$F(\omega)[G] \simeq \bigoplus_{\chi \in \hat{G}} \varepsilon_\chi F(\omega)[G].$$

Mais pour tout $\chi \in \hat{G}$, par la propriété (3), l'anneau $\varepsilon_\chi F(\omega)[G]$ est isomorphe au corps $F(\omega)$, et donc l'anneau $F(\omega)[G]$ est semi-simple puisqu'il est isomorphe à une somme directe de corps. Les éléments ε_χ sont appelés idempotents de l'anneau $F(\omega)[G]$.

Nous pouvons maintenant étudier l'anneau $F[G]$. Soit X l'ensemble des classes d'équivalence de $\hat{G}$ pour la relation $\chi \sim \chi' \Leftrightarrow$ il existe $\gamma \in \Gamma$ tel que $\chi^\gamma = \chi'$ (où l'on a noté $\chi^\gamma(\sigma) = \gamma(\chi(\sigma))$ pour tout $\sigma \in G$). Les éléments

$$\varepsilon_{\overline{\chi}} = \frac{1}{|G|} \sum_{\sigma \in G} \sum_{\chi' \in \overline{\chi}} \chi'(\sigma)\sigma^{-1}$$

(où $\overline{\chi}$ est la classe d'équivalence du caractère χ) satisfont les propriétés (1) et (2), et ils appartienent à $F[G]$ car les coefficients de tels éléments sont invariants par l'action de Γ. Mais alors, comme dans le cas précédent, on obtient :

$$F[G] \simeq \bigoplus_{\overline{\chi} \in X} \varepsilon_{\overline{\chi}} F[G].$$

Soit F_χ la plus petite extension de F contenant l'image du caractère χ. Le corps F_χ est un G-module via $\sigma x = \chi(\sigma)x$ où $x \in F_\chi$, et il est isomorphe à $\varepsilon_{\overline{\chi}} F[G]$, où l'isomorphisme est l'extension de la fonction qui envoie $\sigma \in G$ sur $\chi(\sigma) \in F_\chi$. En particulier, nous avons ainsi montré que $F[G]$ est isomorphe à une somme directe de corps et donc qu'il est semi-simple.

4 Détermination de la majoration pour l.

Dans ce paragraphe, en utilisant les résultats des paragraphes 2 et 3, nous déterminons une majoration pour le nombre premier l. D'abord, nous appliquons les remarques du paragraphe 3 au cas où $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p + \overline{\zeta_p})/\mathbb{Q})$, et $F = \mathbb{F}_l$ (on remarquera que l engendre $(\mathbb{Z}/m\mathbb{Z})^*$ et donc, *a fortiori* ne divise pas m). Donc, en utilisant les notations du troisième paragraphe, on a que $\mathbb{F}_l[G]$ est semi-simple, et :

$$\mathbb{F}_l[G] \simeq \bigoplus_{\overline{\chi} \in X} \varepsilon_{\overline{\chi}} \mathbb{F}_l[G].$$

Ici, les caractères χ sont à valeur dans le corps $\mathbb{F}_l(\omega)$ où ω est une racine m-ième primitive de l'unité (dans une clôture algébrique fixée de $\mathbb{F}_l$).

Lemme 2 *Soient p, m, l et $\overline{\chi} \in X$ comme auparavant et supposons que la classe de l modulo m engendre $(\mathbb{Z}/m\mathbb{Z})^*$. Alors, pour tout $\sigma \in G$, il existe $b_\sigma \in \mathbb{Z}$ tel que :*

$$\varepsilon_{\overline{\chi}} = \frac{1}{|G|} \sum_{\sigma \in G} \overline{b_\sigma} \sigma^{-1},$$

où $\overline{b_\sigma}$ est la classe de b_σ modulo l, et $|b_\sigma| \leq \phi(m)$, où ϕ est la fonction d'Euler.

Preuve. Fixons un élément χ de $\hat{G}$ et soit F_χ la plus petite extension de $\mathbb{F}_l$ contenant l'image de χ. Notons :

$$\varepsilon_{\overline{\chi}} = \frac{1}{|G|} \sum_{\sigma \in G} c_\sigma \sigma^{-1}.$$

Par définition de $\varepsilon_{\overline{\chi}}$, pour tout $\sigma \in G$ on a :

$$c_\sigma = Tr_{F_\chi/\mathbb{F}_l}(\chi(\sigma)),$$

car le sous-groupe H_χ de Γ qui fixe le caractère χ, est le groupe qui fixe le corps F_χ et donc $\mathrm{Gal}(F_\chi/\mathbb{F}_l)$ est isomorphe à Γ/H_χ. Par les propriétés de la trace, on a

$$\forall \sigma \in G,\ c_\sigma = [F_\chi : \mathbb{F}_l(\chi(\sigma))] Tr_{\mathbb{F}_l(\chi(\sigma))/\mathbb{F}_l}(\chi(\sigma)).$$

Puisque la classe de l modulo m engendre $(\mathbb{Z}/m\mathbb{Z})^*$, pour tout d divisant m le polynôme minimal des racines d-ième de l'unité dans $\mathbb{F}_l$ est la réduction modulo l du d-ième polynôme cyclotomique. Mais alors, puisque $\chi(\sigma)$ est une racine de l'unité d'ordre divisant m, on a :

$$Tr_{\mathbb{F}_l(\chi(\sigma))/\mathbb{F}_l}(\chi(\sigma)) = \overline{Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)},$$

où $\alpha \in \mathbb{C}$ est une racine de l'unité du même ordre que $\chi(\sigma)$. Par notre hypothèse sur l, le groupe $(\mathbb{Z}/m\mathbb{Z})^*$ est cyclique et donc m est soit de la forme q^k, soit de la forme $2q^k$, où q est un nombre premier impair et k un entier positif. Donc, pour terminer la preuve, il suffit de déterminer la valeur $Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ où α est une racine de l'unité d'ordre q^k ou $2q^k$, où $k \in \mathbb{N}$. Si l'ordre de α est égal à q^k alors $Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ est égal à $-a_1$, où a_1 est le coefficient de degré $q^k - q^{k-1} - 1$ du polynôme :

$$\frac{X^{q^k} - 1}{X^{q^{k-1}} - 1}$$

et donc :

$$Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = -1 \text{ si } \ k = 1$$
$$Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 0 \text{ si } \ k > 1.$$

Si par contre, l'ordre de α est égal à $2q^k$ alors $Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ est égal à $-a'_1$, où a'_1 est le coefficient de degré $q^k - q^{k-1} - 1$ du polynôme :

$$\frac{X^{q^k}+1}{X^{q^{k-1}}+1}$$

et donc on obtient :

$$Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 1 \text{ si } \ k = 1$$
$$Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 0 \text{ si } \ k > 1.$$

Mais alors, puisque

$$\begin{aligned} Tr_{F_\chi/\mathbb{F}_l}(\chi(\sigma)) &= [F_\chi : \mathbb{F}_l(\chi(\sigma))] Tr_{\mathbb{F}_l(\chi(\sigma))/\mathbb{F}_l}(\chi(\sigma)) \\ &= [F_\chi : \mathbb{F}_l(\chi(\sigma))] \overline{Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)} \end{aligned}$$

on a :

$$\left| \, [F_\chi : \mathbb{F}_l(\chi(\sigma))] Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \, \right| \leq \phi(m),$$

car $[F_\chi : \mathbb{F}_l(\chi(\sigma)]$ divise $\phi(m)$. En posant :

$$b_\sigma = [F_\chi : \mathbb{F}_l(\chi(\sigma))] Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

on a bien $|b_\sigma| \leq \phi(m)$ et $\overline{b_\sigma} = c_\sigma$. □

Preuve du Théorème 1. La relation $[E_p^+ : C_p^+] = h_p^+$ montre qu'il existe un élément $\beta \in E_p^+$ tel que la classe de β est d'ordre exactement l dans E_p^+/C_p^+. Le $\mathbb{Z}[G]$-module :

$$\langle \beta \rangle / \langle \beta \rangle \cap C_p^+$$

est donc un $\mathbb{F}_l[G]$-module qui n'est pas trivial, car $\beta \notin C_p^+$. Puisque $\beta \notin C_p^+$, il existe $\chi \in \hat{G}$ tel que

$$\beta^{\varepsilon_{\overline{\chi}}} \notin C_p^+$$

et on a donc

$$\beta^{l\varepsilon_{\overline{\chi}}} \notin (C_p^+)^l.$$

Soit $b \in \mathbb{Z}$ tel que $\overline{b}$ engendre $(\mathbb{Z}/(p-1)\mathbb{Z})^*$. L'unité cyclotomique

$$\eta = \zeta_p^{(-b+1)/2} \left(\frac{\zeta_p^b - 1}{\zeta_p - 1} \right)$$

engendre C_p^+ comme $\mathbb{Z}[G]$-module (voir [Was 1997], Proposition 8.11). Mais alors η engendre $C_p^+/(C_p^+)^l$ comme $\mathbb{F}_l[G]$-module et donc :

$$\eta^{\varepsilon_{\overline{\chi}}} \in \varepsilon_{\overline{\chi}} C_p^+/(C_p^+)^l$$

et $\eta^{\varepsilon_{\overline{\chi}}}$ n'est pas trivial car l'élément $\beta^{l\varepsilon_{\overline{\chi}}}$ appartient à $\varepsilon_{\overline{\chi}} C_p^+/(C_p^+)^l$, et il n'est pas dans $(C_p^+)^l$.

L'anneau $\varepsilon_{\overline{\chi}}\mathbb{F}_l[G]$ est isomorphe à un corps et, puisque $\varepsilon_{\overline{\chi}} C_p^+/(C_p^+)^l$ est un module cyclique, il existe un élément $\theta \in \mathbb{F}_l[G]$ tel que :

$$\beta^{\theta l\varepsilon_{\overline{\chi}}} = \eta^{m\varepsilon_{\overline{\chi}}}.$$

L'élément θ n'annule pas $\langle\beta\rangle/\langle\beta\rangle \cap C_p^+$, car sinon θ annulerait $\beta^{\theta l\varepsilon_{\overline{\chi}}}$. Donc la classe de l'élément :

$$\beta' = \beta^{\theta\varepsilon_{\overline{\chi}}}$$

est d'ordre l dans E_p^+/C_p^+. De plus, par construction,

$$(\beta')^l = \eta^{m\varepsilon_{\overline{\chi}}}.$$

Le Lemme 2 montre qu'il existe des entiers b_σ avec $|b_\sigma| \leq \phi(m)$ et tels que :

$$\varepsilon_{\overline{\chi}} = \frac{1}{m}\sum_{\sigma\in G} \overline{b_\sigma}\sigma^{-1}.$$

Par les propriétés de la fonction hauteur de Weil h et le fait que $h(\eta) \leq \log(2)$, on obtient la relation suivante :

$$\begin{aligned} h(\beta^l) &= h(\eta^{m\varepsilon_{\overline{\chi}}}) \\ &\leq \sum_{\sigma\in G} |b_\sigma| h(\eta) \\ &\leq m\phi(m)\log(2). \end{aligned}$$

Par le Lemme 1, on a

$$C \leq h(\beta)$$

et donc

$$Cl \leq h(\beta^l).$$

Mais alors

$$Cl \leq h(\beta^l) \leq m\phi(m)\log(2)$$

d'où :

$$l \leq \left(\frac{m}{C}\right)\phi(m)\log(2).$$

□

Références

[Sch 1973] A. Schinzel, *On the Product of the Conjugates Outside the Unit Circle of an Algebraic Number*, Acta Arithmetica **XXIV**, 385-399 (1973).

[Was 1997] L. C. Washinghton, Introduction to cyclotomic fields. 2nd ed. GTM 84, New York, NY, Springer. xiv, 487 p, 1997.