Intersection arithmétique et problème de Lehmer elliptique

Bruno Winckler

université de BORDEAUX

THÈSE

présentée à

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE MATHÉMATIQUES ET INFORMATIQUE

par Bruno WINCKLER

pour obtenir le grade de

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

⋆ ⋆ ⋆

Intersection arithmétique et problème de Lehmer elliptique

⋆ ⋆ ⋆

Soutenue le 20 novembre 2015 à l'Institut de Mathématiques de Bordeaux devant le jury de thèse composé de

Pascal AUTISSIER	Professeur, Université de Bordeaux	Directeur
Yuri BILU	Professeur, Université de Bordeaux	
Éric GAUDRON	Professeur, Université Blaise Pascal	
Philipp HABEGGER	Professeur, Université de Bâle	Rapporteur
Michel LAURENT	Directeur CNRS, Marseille	Rapporteur
Fabien PAZUKI	Professeur associé, Université de Copenhague	Directeur
Olivier RAMARÉ	Chercheur CNRS, Lille	
Gaël RÉMOND	Directeur CNRS, Grenoble	

Intersection arithmétique et problème de Lehmer elliptique

Bruno Winckler

2015

Institut de Mathématiques de Bordeaux
Université de Bordeaux
351, cours de la Libération, 33405 Talence cedex

Remerciements

« Mon bon ami, toute théorie est sèche,
et l'arbre précieux de la vie est fleuri. »
Méphistophélès, dans *Faust* de Goethe

Je remercie chaleureusement Pascal Autissier et Fabien Pazuki, deux directeurs de thèse qui m'ont fait découvrir un pan passionnant de l'arithmétique et m'ont semblé taillés pour moi. Je ne me suis jamais senti abandonné dans la difficulté ni étouffé par le labeur, tout en recevant d'eux, à point nommé, les moyens de mon propre dépassement. Leurs approches mathématiques complémentaires m'inspirèrent grandement pour affiner mon style, à n'en pas douter. Je remercie mes rapporteurs Philipp Habegger et Michel Laurent qui ont bien voulu relire mon manuscrit, malgré quelques majorations assez... Bref. Je suis honoré d'avoir un jury constitué de mathématiciens brillants qui sont, en passant, des êtres humains (ce qui, paraît-il, est déjà formidable pour un mathématicien !) que j'affectionne beaucoup : merci à Yuri Bilu, Éric Gaudron, Gaël Rémond et Olivier Ramaré. Je me dois de mentionner également M. Hanusse, évidemment, diffuseur de mes travaux mathématiques grâce à la Journée de l'École Doctorale : je désespérais de voir l'occasion de les présenter.

L'accessibilité et la bienveillance des chercheurs sont inestimables, d'autant plus qu'ils sont intéressants et intéressés. Je garderai un bon souvenir et un vrai enseignement de mes contacts avec Pierre Parent, Dajano Tossici, Nicola Mazzari, Jean-Paul Cerri, Bill Alombert, Qinq Liu, Charles Dossal, Pierre Mounoud et tant d'autres. Je remercie Karim Belabas pour l'intérêt manifesté concernant mes travaux, qui m'a permis d'améliorer quelques lemmes du chapitre 2.

Parmi mes commensaux bordelais, la première et prime personne remerciée ne laisse, je pense, aucun doute ; aussi, nul ne se vexerait de me voir m'épancher longuement sur elle, mais cela n'est même plus nécessaire : meilleure voisine du monde 2012–2013–2014 et Miss Domercq, son palmarès parle pour elle, Zoé-cœur-avec-les-doigts a marqué de sa très lourde empreinte mes années bordelaises (et mes murs... touche féminine, mon œil ! – pour la peine, je me permets de te genrer). Tout a déjà été dit sur elle. Surtout par elle.

La talonnant, il est impossible d'oublier Tony qui, si l'on formait la Trinité de

l'IMB, serait sans aucun doute le Fils ; plutôt celui qu'on est obligé d'aimer bien qu'on en ait honte. On eut énormément à se raconter mathématiquement ou sportivement, même s'il faut refaire toute l'éducation de ce gros footix, mais c'est surtout son interprétation toute personnelle de la triade dionysienne, plus proche de Dionysos que du Pseudo-Denys, qui nous a rapprochés. Une vertu sérendipiteuse des amalgames.

Romain complète un quartette de **qualiter** ; son enthousiasme et son rendement stakhanoviste qui lui permirent de soutenir si vite m'ont galvanisé ! Par ailleurs, il a toujours su trouver les bons mots quand je doutais de mes convictions (« Était-ce vraiment mieux avant ? – Non : c'était mieux *toujours* »), et j'espère le lui rendre au centuple (en lui promettant que ce sera pire après). Au détour d'une machine à café où l'on s'interroge sur le bien-fondé de l'addition des pièces de monnaie, ou dans un bar-à-vin où la phénoménologie s'invite. Par contre, on se passera de ses questions sur les applications militaires de ma thèse.

Qu'ils ne me trouvent pas ingrat de les reléguer ici. J'ai une pensée évidente pour mes compagnons d'infortune, infortunés de devoir travailler sous la menace quotidienne de mes trames, nommément Giovanni (président providentiel de λ !), Alan (impitoyable, ses questions de géométrie me retenaient de force au bureau jusqu'à 15h voire 15h30), Maarten, plus épisodiquement Baptiste et Guhan. Les autres de la « bande », celle aisément identifiable entre toutes pour ses *party hard* et ses pauses clope ou café interminables, ont largement contribué à m'éviter le *burn-out*. Merci donc à Pierre L., Camille/10 (De surclasser ton pot l'espoir me paraît vain ; tes quiches, tes muffins avaient un goût divin !), Marie, Jocelyn, Jean-Baptiste, Alice, Marc N., Thomas L., Sami (et Leslie), Raphaël, Nikola, Lorrain, Elsa, ainsi qu'aux ramifications : Marc M., qui seul peut témoigner que je n'ai pas cessé d'exister du 12 juin au 13 juillet 2014, Perrine, Francesco, Dario, Étienne Ba., Guillaume D., Nicolas Du., Fabien, Albert, Gu, Corentin, Nicolas H....

Quatre ans de thèse, c'est long, mais je n'ai pas la mémoire courte : je n'ai pas oublié l'ouverture des anciens, ni ceux qui ont commencé avec moi. Que de bons moments, accompagnés de Sophie (deuxième meilleure cavalière de tango au monde), Louis, Johanna, Pierre C., Aurélien, Nicolas D., Nicola del Piero, Laurent A., Andrea, Aurel et Nicolas, *etc* ! Je regretterai l'ambiance détendue qui régnait entre doctorants de l'IMB. Il est plus facile de s'attacher à un métier parfois frustrant (puisqu'on est constamment confronté à ses limites, au doute, à l'échec) avec un environnement si favorable ; constat qui s'étend aux collègues rencontrés en conférences, qui prenaient grâce à eux quelques airs de vacances (mais chut). Parmi les doctorants je pense à la famille mathématique, tante Julie et oncle Richard, puis à la famille strasbourgeoise que je fus ravi de retrouver partiellement à Rennes, composée d'Amandine, Antoine, Gautier, Valentine, William, Michael, Pierre B., Adriane, Amaury, Laurent D., Lauriane, Émilie, *etc.*, et enfin à Adji, Alexandre, Ange, Ariyan et ses lubies mochizukiennes, Benjamin M., Benoît, Charlotte, Christelle, Cyril, Dino, Étienne Be.,

Florent, Giacomo, Gwenaël, Isabelle, Nadim, Nil, Pierre M., Pierre-Antoine, Sergey, Tristan et Salomé, *etc.*, *etc.* Quant aux « vieux », dont la sympathie est rassurante parce qu'on sait qu'on finira par leur ressembler, ils sont bien représentés par des mathématiciens tels que Francesco Amoroso, Aurélien Galateau, Mathilde Herblot, Dan Petersen, Nicolas Ratazzi, J-P, *etc.*, qui furent également d'excellent conseil (plusieurs de vos réponses ont été décisives dans le cheminement de ma thèse), jusque dans les aspects extra-mathématiques. J'ai un affect particulier pour Marc Hindry : mon stage de M1 sous son égide m'a confirmé l'envie de poursuivre dans le monde bigarré de la géométrie arithmétique.

Je ne peux omettre les « Bordelais » qui ont animé la vie hors des mathématiques : Gaëlle du Made in France, Julien du Cock & Bull et ses serveuses, Gregory du tango et ses faire-valoir prodiges (Benjamin S., Amélie, Anna, Benjamin G. et Audrey, CGP, Arnaud, Camille, Nicolas et Mélanie, Aude, Olivier, *etc.*) Sébastien Dos et les compagnons d'armes du BEC (Ludovic, Donatien, Louise, Marine, Guillaume, Victoria, Marie, Vital, *etc.*, c'était un plaisir de décompresser après le travail en ratonnant des droitiers), et enfin les Lacou aux dîners de famille chaleureux.

Dans un souci d'**égaliter**, mes remerciements de *normie* s'appliquent aussi à ceux qui n'en veulent pas : Jamel et son génie indépassable (t'égaler est ma principale motivation au travail ; que dois-je faire de plus ?), Hakan qui régresse (tu vas me manquer quand tu te feras les Croisés, *I still love you*), Matteu WMDJA mon partenaire de khôlles, Victoria qui est pourtant une topologue médiocre et, scandale suprême, non agrégée, Cem, Ivan et Kathleen, Jérémie, Thomas P., Lisandru, Alban, Andria, Benjamin R., Anaïs, Léa, Reda, Quentin et Anne-Fleur, la preuve vivante que « nul n'est plus catholique que le diable ». Épaules luxées, « *street-art* » et autres aventures inavouables, vos passages à Bordeaux furent d'une singularité mémorable.

Citer toute ma généalogie serait aussi fastidieux que de répéter celles de l'Ancien Testament. Je vais donc me contenter de remercier ma mère, mes frères, ma sœur et ma grand-mère pour leur soutien immodéré, même si je sais qu'ils m'ont laissé faire des mathématiques parce qu'il aurait été plus coûteux de tenter de me réinsérer socialement.

Toutes ces personnes ne sont que peu de choses à côté de mon plus grand inspirateur : Patrice Évra, Celui qui réjouit ma jeunesse.

Enfin, j'ai une pensée émue et sincère pour X, X appartenant à l'ensemble des gens que j'ai oubliés mais que j'aime quand même. Chebran.

À mon père

Table des matières

Table des figures

Notations

$\lvert\cdot\rvert_v$	valeur absolue v-adique normalisée
$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v$	intersection locale en v de $\mathcal{D}_1$ et $\mathcal{D}_2$
$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle$	intersection (globale) de $\mathcal{D}_1$ et $\mathcal{D}_2$
$(P\|Q)$	accouplement bilinéaire symétrique induit par $\hat{h}$
$\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]$	automorphisme de Frobenius associé à $\mathfrak{P}$ divisant $\mathfrak{p}$
$\left[\frac{L/K}{\mathfrak{p}}\right]$	classe de conjugaison des $\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]$, pour $\mathfrak{P}$ divisant $\mathfrak{p}$
β, β_0	zéro de Siegel
B	voir $\mathrm{Spec}(\mathcal{O}_K)$
C	sous-ensemble du groupe de Galois G stable par conjugaison
$\widehat{\mathrm{Cl}(\mathcal{X})}$	groupe quotient de $\widehat{\mathrm{Div}(\mathcal{X})}$ par la relation d'équivalence linéaire
$\mathcal{D}$	diviseur sur une surface arithmétique
$\delta_{\chi=1}$	symbole de Kronecker
$\Delta(E/K)$	discriminant minimal de E/K
d_L	discriminant (absolu) de L sur $\mathbb{Q}$
$\mathrm{D}_{\mathfrak{P}}$	groupe de décomposition de $\mathfrak{P}$
$\widehat{\mathrm{Div}(\mathcal{X})}$	groupe des diviseurs d'Arakelov sur $\mathcal{X}$
E/K	courbe elliptique définie sur K
$E[n]$	points de n-torsion sur E
$\mathcal{E}$	modèle minimal régulier de E
$\mathcal{E}_{\mathfrak{p}}$	fibre de $\mathcal{E}$ au-dessus de $\mathfrak{p}$
$e_i, e_{\mathfrak{P}}$	indice de ramification de $\mathfrak{P}_i$, $\mathfrak{P}$ sur K
(f)	diviseur principal d'Arakelov
f_i	degré de $\mathfrak{P}_i$ sur K
$\mathrm{F}_{\mathfrak{p}}$	relèvement de Frobenius sur E associé à $\mathfrak{p}$
F_σ	fibre formelle de $\mathcal{X}$ au-dessus de la place infinie associée à σ
G	groupe de Galois de L/K
$g(P,Q)$	fonction de Green-Arakelov
Γ	fonction Γ d'Euler
Γ_i	composante irréductible d'une fibre de $\mathcal{E}$ ou $\mathcal{X}$
γ_χ	facteur γ de l'équation fonctionnelle de $\mathrm{L}(s,\chi)$

$h(P), \hat{h}(P)$	hauteur naïve, hauteur canonique de P
$h_{F^+}(E/K)$	hauteur de Faltings de E/K
$\mathrm{I}_{\mathfrak{P}}$	groupe d'inertie de $\mathfrak{P}$
j_E	j-invariant de E
K	corps de nombres
$\bar{K}$	clôture algébrique de K
K_v	complété en v de K
$\mathrm{K}_{\mathcal{X}/B}$	diviseur canonique (d'Arakelov) de $\mathcal{X} \to B$
λ_v	fonction de Néron, hauteur locale
$\mathrm{L}(s, \Phi, L/K)$	fonction L d'Artin associée au caractère Φ de G
$\mathrm{L}(s, \chi, L/E)$	fonction L de Hecke associée au caractère χ de $\mathrm{Gal}(L/E)$
Li	logarithme intégral
μ	(1,1)-forme canonique sur X
M_K	ensemble des places de K
M_K^0, M_K^∞	ensemble des places finies, infinies de K
$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$	norme de $\mathfrak{p}$, cardinal de $\mathcal{O}_K/\mathfrak{p}$
$[n]$	multiplication par n sur une courbe elliptique
n_χ	nombre de zéros de $\mathrm{L}(s, \chi)$ dans la bande critique
N_E	norme du conducteur de la courbe elliptique E
n_L	degré de L sur $\mathbb{Q}$
n_v	degré local $[K_v : \mathbb{Q}_v]$ en v
$\mathcal{O}$	section neutre de $\mathcal{E}$
$\mathcal{O}_K$	anneau des entiers de K
$\mathcal{P}$	adhérence d'un point fermé P de la fibre générique
Φ	caractère irréductible de G
π_C	fonction de décompte des idéaux premiers dont le Frobenius est dans C
Π_s	nombres premiers rationnels se décomposant complètement dans K'
ψ_C	fonction sommatoire de von Mangoldt
$\mathfrak{p}$, $\mathfrak{P}$	idéal maximal de l'anneau des entiers de K, de L
r	morphisme canonique $\mathcal{X}' \to \mathcal{X}$
r_v	morphisme de rétraction $E(K_v) \to \mathbb{Q}/\mathbb{Z}$
ρ	zéro non trivial d'une fonction L
$\sigma : L \hookrightarrow \mathbb{C}$	plongement de L dans $\mathbb{C}$ qui fixe K
$\mathrm{Spec}(R)$	ensemble des idéaux premiers de R
$v_{\mathfrak{p}}$	valuation discrète de $\mathcal{O}_{K,\mathfrak{p}}$
W	modèle de Weierstrass de E
$\mathcal{X} \to B$	surface arithmétique sur B
$\mathcal{X}_\sigma$, $\mathcal{X}_{\mathfrak{p}}$	fibre de $\mathcal{X}$ au-dessus de la place associée à σ, au-dessus de $\mathfrak{p}$
w_1, w_{-1}	fonctions de Lambert
ζ_K	fonction dzêta de Dedekind du corps de nombres K

Introduction

« La brièveté de la vie, la grossièreté des organes, la torpeur de la négligence, les occupations oiseuses et l'affaiblissement des facultés de l'âme, ne me permettent pas de savoir beaucoup de choses. Le peu que nous apprenons est continuellement arraché et enlevé de notre esprit par l'ennemi de la science, l'oubli, qui l'efface de notre mémoire. »
Jacques de Guyse, *Histoire de Hainaut*

Machinerie des hauteurs

Dans l'étude des problèmes diophantiens, qui consistent essentiellement à trouver des solutions entières ou rationnelles à des équations polynomiales (et donc, formulé différemment, à trouver des points entiers ou rationnels sur des variétés algébriques), un moyen de résolution pratique passe par la quantification de la taille, ou « complexité arithmétique », des solutions. Supposons qu'on étudie une équation, ou une famille d'équations, dont on cherche les solutions, et qu'on connaît une fonction h, dite de hauteur, mesurant la taille des nombres algébriques en un certain sens, qui vérifie de plus la propriété suivante : pour tout entier $D \geqslant 1$ et tout réel $C > 0$,

$$\{x \text{ algébrique } \mid h(x) \leqslant C, [\mathbb{Q}(x) : \mathbb{Q}] \leqslant D\}$$

est fini ; alors, pour peu qu'on ait réussi à borner la fonction de hauteur sur l'ensemble des solutions des équations étudiées, on a moralement résolu ces équations. C'est à cette propriété, outre la lettre qui les note, qu'on reconnaît de « bonnes » fonctions de hauteurs. Weil fit une construction systématique de hauteurs sur des variétés abéliennes, qui a l'avantage de refléter la structure géométrique des équations étudiées dans les propriétés des hauteurs. Néron, Tate, Faltings, *etc.*, permettent d'autres constructions, qui livrent un arsenal très fourni de hauteurs pour démontrer des résultats de finitude.

La qualité de leur tableau de chasse (non exhaustif) permet de mesurer l'intérêt de leur étude :

1. La hauteur de Néron-Tate, définie sur l'ensemble des points algébriques d'une variété abélienne A/K, est utilisée pour démontrer le théorème de Mordell-Weil : le groupe de ses points rationnels est de type fini. Plus précisément, on peut démontrer que cet énoncé est équivalent à la finitude du groupe quotient $A(K)/2A(K)$, et si S est le maximum des hauteurs de représentants de ce groupe quotient, alors l'ensemble fini $\{P \in A(K) \mid \hat{h}(P) \leqslant S\}$ engendre $A(K)$. Donc la question de déterminer les générateurs se ramène à la question de déterminer une classe de représentants du groupe fini $A(K)/2A(K)$ (un problème plus difficile qu'il n'y paraît, qui n'a toujours pas de solution).
2. Même sans démontrer de résultats de finitude, il est en soi intéressant d'étudier le cardinal d'ensembles de la forme

$$\{P \in X \mid h(P) < B\}, \tag{1}$$

où X est un ensemble géométrique, et B un réel positif. Ainsi, par exemple, l'article [HS99] démontre que pour de « bonnes » courbes elliptiques définies sur un corps de nombres K, le nombre de points de hauteur canonique au plus $\frac{A}{[K:\mathbb{Q}]}$ n'excède pas $B[K:\mathbb{Q}]\ln([K:\mathbb{Q}])$, où A et B sont des constantes absolues explicites ; ils en déduisent, d'une part, une borne polynomiale en $[K:\mathbb{Q}]$ sur le cardinal du sous-groupe de torsion d'une courbe elliptique, et d'autre part une minoration de la hauteur pour les points algébriques d'ordre infini. La stratégie provient de Masser, et se poursuit par exemple dans [Pet06].
3. Le théorème de Siegel, selon lequel une courbe affine de genre au moins un n'a qu'un nombre fini de points entiers, se démontre aussi grâce à la machinerie des hauteurs.
4. L'exemple le plus prestigieux est la conjecture de Mordell, suggérant qu'une courbe de genre au moins deux n'a qu'un nombre fini de points rationnels, qui est désormais un théorème de Faltings ; il s'obtient en définissant une hauteur (maintenant dite de Faltings) sur un ensemble de variétés abéliennes, et en montrant que la conjecture de Mordell revient à compter des variétés abéliennes de hauteur inférieure à une quantité donnée, ce qui signifie bien qu'il n'en existe qu'un nombre fini.

Nous n'avons pris soin de détailler que les applications relativement proches de notre sujet d'étude, même si les connexions entre les différentes hauteurs présentes existent et ne sont pas anecdotiques.

Problème de Lehmer

La mission de cette thèse est d'étudier les points de petite hauteur sur les courbes elliptiques. Pour préciser les termes, revenons d'abord sur la hauteur des nombres

algébriques : partant de la propriété de finitude énoncée ci-dessus, il est aisé de constater que la hauteur d'un nombre algébrique (non nul) est nulle si, et seulement s'il s'agit d'une racine de l'unité. De plus, si l'on restreint la fonction de hauteur aux nombres algébriques non nuls qui ne sont pas des racines de l'unité, et dont on prescrit le degré, alors cette même propriété de finitude démontre que 0 n'est pas une valeur d'accumulation de la hauteur ; il est donc naturel de chercher la borne inférieure de la hauteur. La conjecture qui guide les recherches en ce sens est la suivante :

Conjecture (Problème de Lehmer)**.** Il existe une constante $c > 0$ telle que pour tout nombre algébrique non nul x qui n'est pas une racine de l'unité, on ait :

$$h(x) \geqslant \frac{c}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

La conjecture est trivialement vraie si l'on se restreint au sous-ensemble des nombres algébriques qui ne sont pas des entiers algébriques, et on peut prendre $c = \ln(2)$. Elle est aussi vraie pour les nombres non-réciproques (voir [Smy71]). Le meilleur résultat actuellement valable pour tout nombre algébrique provient de Dobrowolski, qui démontre la conjecture « à un exposant ε près ».

Théorème (Dobrowolski, [Dob79])**.** *Il existe une constante $c > 0$ telle que pour tout nombre algébrique non nul x qui n'est pas une racine de l'unité, on ait :*

$$h(x) \geqslant \frac{c}{D} \left(\frac{\ln(\ln(3D))}{\ln(2D)} \right)^3,$$

où $D = [\mathbb{Q}(x) : \mathbb{Q}]$.

Dans son article, Dobrowolski montre même que l'on peut prendre $c = \frac{1}{1200}$. Depuis, Voutier a montré dans [Vou96] que le choix $c = \frac{1}{4}$ convient déjà, et Cantor et Strauss ont montré dans [CS83] qu'on peut prendre n'importe quelle constante $c < 2$, quitte à ce que la borne ne soit valable que pour un degré suffisamment grand.

Pour démontrer ce théorème, Dobrowolski raisonne par l'absurde en supposant le résultat faux, c'est-à-dire en supposant l'existence d'un nombre algébrique x de grand degré D et de petite hauteur. Il construit alors, en utilisant un lemme de Siegel, un polynôme P à coefficients entiers qui s'annule en x avec une grande multiplicité. Alors, en utilisant le petit théorème de Fermat, il montre que le polynôme P s'annule modulo p premier en x^p ; utilisant l'hypothèse de petite hauteur sur x et l'inégalité de Liouville, on voit qu'un « grand nombre » de x^p ne sont pas seulement des racines modulo p, mais de « vraies » racines de P (tout ceci étant convenablement quantifié en fonction de D). Compter les zéros du polynôme et les comparer à son degré permet alors de conclure.

Une question analogue se pose dans le cadre géométrique des courbes elliptiques sur un corps de nombres : une courbe elliptique E/K admet une fonction de hauteur dite de Néron-Tate, notée $\hat{h} : E(\bar{K}) \to \mathbb{R}$, qui a pour vertus de vérifier, encore, la propriété de finitude des hauteurs, et de refléter la géométrie de la courbe en vérifiant l'identité du parallélogramme ; une conséquence de ces faits est que le lieu d'annulation de cette hauteur est précisément le sous-groupe de torsion de la courbe elliptique. Raisonnant en analogie avec la situation dans le cadre des nombres algébriques, une problématique récurrente en géométrie diophantienne est la minoration uniforme de cette fonction sur une famille de courbes elliptiques (en dehors des sous-groupes de torsion) ; énonçons par exemple la conjecture de Lang (voir [Lan78]), qui s'attend à ce que pour tout corps de nombres K, il existe une minoration uniforme pour toute courbe elliptique définie sur K, de la forme :

$$\hat{h}(P) \geqslant c(K) \max(\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))), h(j_E)), \tag{2}$$

pour tout point $P \in E(K)$ d'ordre infini, où $c(K)$ est une constante ne dépendant que de K, $\Delta(E/K)$ le discriminant minimal de E/K, et $h(j_E)$ la hauteur naïve de l'invariant modulaire j_E de la courbe E. On peut également se demander ce qu'il se passe si on fixe la courbe elliptique, mais qu'on donne toute liberté au corps de rationalité des points à étudier. Alors, on a l'analogue du problème de Lehmer dans le cadre elliptique.

Conjecture (Problème de Lehmer elliptique)**.** Soit E une courbe elliptique sur un corps de nombres K. Il existe une constante $c(E/K) > 0$, dépendant uniquement de E/K, telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, on ait :

$$\hat{h}(P) \geqslant \frac{c(E/K)}{[K(P) : K]}.$$

On ne peut pas espérer une meilleure minoration sans restrictions : en effet, fixons un point $P \in E(\bar{K})$ d'ordre infini, et notons P_n un point algébrique de degré $D_n = [K(P_n) : K]$ tel que $[n]P_n = P$. On a $\hat{h}(P_n) = n^{-2}\hat{h}(P)$, or D_n est majoré par une quantité de la forme $c \cdot n^2$, donc $\hat{h}(P_n) \leqslant \frac{c \cdot \hat{h}(P)}{D_n}$.

Si la question est naturelle, il est tout de même de bon ton de proposer une application possible : on a esquissé la possibilité de produire des bornes sur l'ordre d'un point de torsion de degré D à l'aide de minorations de la hauteur sur les points d'ordre infini. Soit $\psi(E, D)$ la borne inférieure sur la hauteur des points d'ordre infini de E et de degré au plus D ; on en déduit alors qu'un point algébrique P d'une courbe elliptique $E/\mathbb{Q}$, de degré au plus D et de hauteur strictement inférieure à $\psi(E, D)$, est un point de torsion à un ordre au plus $\omega(E, D)$. À présent, soient P_1, …, P_m des points de $E(\bar{\mathbb{Q}})$ de degrés au plus D et de hauteurs au plus Q pour un

réel $Q \geqslant \psi(E, D)$. On peut alors montrer qu'il existe une relation de dépendance linéaire sur $\mathbb{Z}$ entre ces points si, et seulement s'il existe des entiers t_1, …, t_m tels que $\sum_i t_i P_i = 0$ et :

$$0 < \max(|t_1|, \ldots, |t_m|) \leqslant \omega(E, D) \left(\frac{m^2 Q}{\psi(E, D)} \right)^{\frac{m-1}{2}} .$$

Pour les détails, voir [Mas81], section 2.

La minoration la plus proche de celle attendue est obtenue par Laurent, dans le cas des courbes elliptiques à multiplications complexes :

Théorème (Laurent, [Lau83])**.** *Soit E/K une courbe elliptique à multiplications complexes. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on ait :*

$$\hat{h}(P) \geqslant \frac{c(E/K)}{D} \left(\frac{\ln(\ln(3D))}{\ln(2D)} \right)^3 . \tag{3}$$

L'article [Lau83] propose en remarque une explicitation de la constante $c(E/K)$; il est énoncé sans démonstration que :

$$\hat{h}(P) \geqslant \frac{1}{10^{13} n_K^9 n_{\hat{K}}} \frac{1}{D} \left(\frac{\ln(\ln(D))}{\ln(D)} \right)^3 ,$$

où $n_{\hat{K}}$ est le degré sur $\mathbb{Q}$ de la clôture galoisienne de K. Mais cette explicitation n'est pas complètement satisfaisante, parce qu'elle n'est valable que pour un degré D *assez grand*, supposé dépendre des places de mauvaise réduction et d'une version effective du théorème de Chebotarev (en un sens non explicite).

Sa démonstration adapte la démarche de Dobrowolski : reproduire un polynôme convenable, annulateur des coordonnées d'un point algébrique d'ordre infini, passe par la relation de dépendance algébrique entre les fonctions $\mathscr{P}$ de Weierstrass et leurs dérivées, tandis que l'annulation en des exponentiations d'un nombre algébrique est imitée grâce à l'existence de relèvements de Frobenius sur une courbe elliptique à multiplications complexes (ce qui n'est pas aisément transposable à une courbe elliptique générique).

Hors du monde des courbes elliptiques à multiplications complexes, les deux prochains théorèmes, qui passent par l'étude d'ensembles tels qu'en (1), sont les plus proches de la minoration attendue par Lehmer.

Théorème (Masser, [Mas89]). *Soit E/K une courbe elliptique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on ait :*

$$\hat{h}(P) \geqslant \frac{c(E/K)}{D^3(\ln(2D))^2}.$$

C'est le meilleur résultat général actuellement connu. Si E/K admet des places de mauvaise réduction multiplicative, alors on peut améliorer cette inégalité :

Théorème (David, [Dav97]). *Soit E/K une courbe elliptique dont le j-invariant n'est pas un entier algébrique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on ait :*

$$\hat{h}(P) \geqslant \frac{c(E/K)}{D^{\frac{15}{8}}(\ln(2D))^2}.$$

Des cas particuliers de cette conjecture sont étudiés, notamment en supposant que les coordonnées de P engendrent une extension abélienne de K : dans ce cas, on trouve même une minoration par une constante absolue (voir [Sil04]), ce qui incite à modifier le problème de Lehmer en remplaçant le degré $[K(P) : K]$ par $[K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$ (pour ne pas faire intervenir la partie abélienne qui « ne compte pas »). Dans ce cas, [Rat04] obtient la même minoration que Laurent.

Enfin, notons que la conjecture de Lehmer a récemment été prouvée pour les points qui engendrent une extension galoisienne de K.

Théorème (Galateau et Mahé, [GM15a]). *Soit E/K une courbe elliptique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini tel que $K(P)/K$ soit une extension galoisienne, on ait :*

$$\hat{h}(P) \geqslant \frac{c(E/K)}{[K(P) : K]}.$$

Cette prépublication propose d'autres résultats analogues si le groupe de Galois de la clôture galoisienne n'est pas trop « gros ».

Le projet de cette dissertation est d'obtenir un résultat intermédiaire entre les inégalités (2) et (3). Ou, dit autrement, on veut comprendre comment la minoration de Laurent dépend de la courbe elliptique : est-ce que cette dépendance va dans le sens de la conjecture de Lang ? Dépend-elle des places de mauvaise réduction, de la hauteur du j-invariant, ou d'une autre quantité liée à la courbe elliptique ? Notre résultat principal en ce sens est le théorème suivant, qui motive tout le développement de cette thèse.

Théorème (Théorème principal)**.** *Soit $K/\mathbb{Q}$ une extension galoisienne finie de degré n_K et de discriminant absolu d_K. Soit E/K une courbe elliptique à multiplications complexes par l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, ayant bonne réduction partout. Pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on a :*

$$\hat{h}(P) \geqslant \frac{1}{c_{K,E}} \frac{1}{D} \left(\frac{\ln(\ln(4D))}{\ln(4D)} \right)^3, \tag{4}$$

où :

$$c_{K,E} = 5 \cdot 2^{28} \sqrt{6n_K} (59{,}07 + 276{,}48 \ln(|d_K|) + n_K (2911{,}6 + 138{,}3 \ln(-4d)))^6 \cdot (3{,}89 + 0{,}13 h(j_E))^3 .$$

si HRG est vraie, et :

$$c_{K,E} = \exp\left[(|d_K|^{384} d^{92n_K} 192^{384n_K})^{2709} \exp(387(4992n_K + 33)) \right] \times \left(728 + 10^{-4751} \exp\left[(|d_K|^{384} d^{92n_K} 192^{384n_K})^{2709} \exp(387(4992n_K + 33)) \right] \right) \times (3{,}89 + 0{,}13 h(j_E))^3 \cdot 8\sqrt{3n_K}$$

sinon.

Le théorème 6.1, plus général, donne une inégalité valable sans hypothèse sur le type de réduction. Comme on l'explique dans la remarque 6.2, on peut toujours se ramener à l'hypothèse galoisienne, et une isogénie permet de se ramener au cas de la multiplication complexe par $\mathcal{O}_K$, donc ce théorème recouvre bien la version précédente de Laurent pour toute courbe elliptique sur un corps de nombres K non supposé galoisien sur $\mathbb{Q}$, et à multiplications complexes. D'autres réductions sont possibles : on renvoie aux remarques qui suivent le théorème 6.1.

La démonstration suit un chemin différent à bien des égards de celui de [Lau83] : on démontre cette inégalité en interprétant la hauteur de Néron-Tate en terme d'intersection sur le modèle minimal régulier d'une courbe elliptique, grâce au théorème 5.29 (selon les affinités du lecteur, ce théorème peut même faire office de définition de la hauteur de Néron-Tate) et à son corollaire 5.30 : une conséquence particulière de ces résultats est la négativité de l'auto-intersection d'un diviseur du modèle. Une combinaison linéaire convenable de diviseurs liés au point dont on veut estimer la hauteur permet donc, en utilisant ce fait, de comparer cette hauteur à des calculs d'intersections locales impliquant le point en question, ainsi que des images de ce point par des relèvements de Frobenius de la courbe elliptique. Ces endomorphismes sont privilégiés, parce qu'on connaît précisément les points qui coupent leur image par un Frobenius au-dessus de son idéal maximal associé, grâce au petit théorème

de Fermat. Les intersections locales aux places archimédiennes sont évaluées à l'aide d'une version affinée du lemme d'Elkies.

Notre approche a l'avantage d'être géométriquement intrinsèque : il n'y a notamment pas de recours à la hauteur naïve ni de choix de coordonnées projectives à faire.

L'exigence d'explicitation de la constante $c(E/K)$ du théorème de Laurent nous a conduit à expliciter un autre résultat bien connu des théoriciens des nombres, qui mérite donc de consacrer une grande partie de cette thèse : le théorème de Chebotarev, qui possédait déjà un énoncé théoriquement effectif dans [LO77] (avec, donc, un développement asymptotique au second ordre).

Contenu de la thèse

La **première partie** est exclusivement analytique en dehors de quelques rappels préliminaires de théorie algébrique des nombres, et consacrée à la démonstration effectivement effective du théorème de Chebotarev, dont nous avons besoin lors de la démonstration de l'inégalité (4) dans le chapitre 6. J'ai soumis à la publication les résultats de cette partie.

Le **chapitre 1** fournit d'abord les définitions et résultats basiques nécessaires à la simple compréhension de l'énoncé du théorème de Chebotarev ; on esquisse donc le lien entre l'étude d'automorphismes de Galois particuliers (les automorphismes de Frobenius, qu'on cherche à « compter » avec ledit théorème) et la décomposition d'idéaux premiers dans des extensions de corps de nombres. On présente ensuite notre premier résultat sous ses formes inconditionnelle et conditionnelle (en admettant l'hypothèse de Riemann généralisée) : on démontre que si π_C est la fonction de décompte des automorphismes de Frobenius dans la classe de conjugaison C du groupe de Galois G, alors pour $x \geqslant 2$:

$$\left|\pi_C(x) - \frac{|C|}{|G|}\int_2^x \frac{\mathrm{d}x}{\ln(x)}\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\Big[\left(\frac{55}{48} + \frac{177}{\ln(x)}\right)\ln(d_L) + \left(\frac{605}{1152}\ln(x) + 13 + \frac{866}{\ln(x)}\right)n_L + 680\Big]$$

si l'hypothèse de Riemann généralisée est vraie ; je n'écris pas la version inconditionnelle ici pour ne pas alourdir le propos, elle est l'objet du théorème 1.7.

Comme la démonstration est particulièrement technique, j'ai estimé utile de l'esquisser dans ses grandes lignes à la fin du chapitre 1. Sans se répéter, disons simplement qu'intégrer sur un segment vertical une somme de fonctions L relie une certaine fonction arithmétique, notée ψ_C et définie comme une somme à support

dans les idéaux premiers qu'on veut compter, à des intégrales de fonctions L, que le théorème de Cauchy exprime à l'aide des zéros et pôles de ces mêmes fonctions. En explicitant des régions sans zéro pour les fonctions dzêta de corps de nombres, on est en mesure d'en déduire une majoration explicite de ψ_C puis de π_C.

Le **chapitre 2** démontre le théorème de Chebotarev, ainsi que plusieurs résultats inédits de nature arithmétique et analytique pourvus d'intérêt en soi. En premier lieu, approximer l'intégrale sur un segment vertical d'une fonction L de Hecke par une intégrale sur un contour, en vue d'appliquer le théorème de Cauchy, nous mène à expliciter des inégalités sur la fonction $\frac{\Gamma'}{\Gamma}$ dans le lemme 2.7, où Γ est la fonction d'Euler qui intervient dans l'équation fonctionnelle des fonctions L. On en déduit, en particulier, un premier lemme important : si $n_\chi(t)$ est le nombre de zéros non triviaux de $\mathrm{L}(\cdot,\chi)$ de partie imaginaire entre $t-1$ et $t+1$, alors

$$n_\chi(t)+n_\chi(-t) \leqslant \frac{5}{2}\left[\ln(A(\chi)) + 2\delta_{\chi=1}(\chi)\left(\frac{2}{4+t^2}+\frac{1}{1+t^2}\right) + n_E\left(\ln\left(\frac{|t|+3}{2\pi}\right)+2\right)\right]$$

pour tout réel t (lemme 2.9). L'inégalité du théorème 2.15, de laquelle procède presque immédiatement le théorème explicite de Chebotarev, à l'étude des régions sans zéros près, relie la fonction ψ_C à une somme sur les zéros de toutes les fonctions L de Hecke associées à des caractères irréductibles : on l'appelle formule explicite, et elle est approximativement de la forme

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \lesssim \frac{|C|}{|G|}\left(n_L\frac{x(\ln(x))^2}{T} + \frac{x\ln(x)}{T}\left[\ln(d_L)+n_L\left(\ln(T)\right)\right]\right),$$

où

$$S(x,T) = \frac{|C|}{|G|}\sum_\chi \bar\chi(g)\left(\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho} - \sum_{\substack{\rho\\|\rho|<\frac12}}\frac{1}{\rho}\right).$$

Même si cette inégalité n'est pas très engageante, on voit qu'on y gagnerait beaucoup à démontrer que l'hypothèse de Riemann généralisée, adaptée à des familles éventuellement restreintes de fonctions L, est vraie pour tous les zéros non triviaux de partie imaginaire inférieure à une quantité T fixée (un tel effort est déjà fait pour la fonction dzêta classique, qui certes se prête mieux à la vérification numérique) ; une majoration de la somme $S(x,T)$ pourrait alors être considérablement affinée, et améliorer en aval le théorème de Chebotarev effectif.

La démonstration du théorème obtient aussi des régions sans zéros explicites pour la fonction dzêta du corps de nombres L, à la forme qualitativement familière : en effet, ζ_L n'a pas de zéros $\rho=\beta+i\gamma$ dans la région délimitée par les conditions

$$|\gamma| \geqslant \frac{1}{1+4\ln(d_L)}$$

et

$$\beta \geqslant 1 - 7\left(906\ln(d_L) + n_L\left(117\ln\left(\frac{3+|\gamma|}{2\pi}\right)+2\right)+275\right)^{-1}.$$

Pour alléger les inégalités dans cet exposé introductif, j'ai approché les constantes par des entiers. Le lemme 2.16 fournit une région plus fine. Enfin, on conclut par une version du phénomène de répulsion des zéros et une majoration du zéro de Siegel, toutes deux très grossières : on démontre en effet dans le théorème 2.24 que si ζ_L a un zéro réel $\beta_0 > 0$, alors $\zeta_L(s) \neq 0$ pour

$$\mathrm{Re}(s) > 1 + \frac{\ln\left(1536(1-\beta_0)\ln\left(|d_L|^7(|\mathrm{Im}(s)|+1)^{n_L/4}e^{26n_L+32}\right)\right)}{192\ln\left(|d_L|^7(|\mathrm{Im}(s)|+1)^{n_L/4}e^{26n_L+32}\right)},$$

et dans le corollaire 2.26 que si β_0 est un zéro de ζ_L proche de 1, dont on soupçonne évidemment l'inexistence (eu égard de l'hypothèse de Riemann généralisée), alors :

$$1 - \beta_0 \geqslant \frac{1}{1536}\frac{1}{|d_L|^{2709}e^{387(26n_L+32)}}.$$

Le **chapitre 3** ne fait que démontrer des résultats dans la continuité directe du chapitre précédent, qui découlent rapidement des résultats qu'on y a établis, par inertie en quelque sorte. Simplement, comme je n'utiliserai pas les résultats de ce chapitre dans la seconde partie de la thèse, et qu'ils s'éloignent de nos premières considérations, je n'ai pas pris le temps de les affiner.

Soit L/K une extension de corps de nombres. L'objectif de ce chapitre est la majoration du plus petit idéal premier de K dont l'automorphisme de Frobenius associé est dans une classe de conjugaison donnée, et dont la norme est un nombre premier (rationnel). On démontre que sa norme est inconditionnellement inférieure à $d_L^{27175010}$. Cette borne est inutilisable en pratique, mais on donne tous les moyens théoriques et explicites de parvenir à une telle borne qui, je l'espère, deviendra exploitable en soignant les majorations (ceci devra passer entre autres par une meilleure version du phénomène de répulsion des zéros).

La **seconde partie** s'intéresse au problème de Lehmer à travers le formalisme d'Arakelov. Les techniques impliquées sont arithmétiques, c'est-à-dire à la fois géométriques, algébriques et analytiques.

Le **chapitre 4** ne comporte aucun résultat neuf, et fait figure de rappels en théorie de l'intersection d'Arakelov sur les surfaces arithmétiques. Après avoir brièvement exposé les difficultés d'une théorie de l'intersection sur de tels schémas et suggéré les ajustements à faire, nous passerons la majeure partie du chapitre à définir l'intersection locale en une place infinie $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v$, qui nécessite plusieurs prérequis de

nature analytique, tandis que l'intersection locale en une place finie reste finalement assez proche de l'intersection locale sur une surface algébrique. L'intersection globale $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle$ s'obtient alors en sommant les contributions aux places locales infinies et finies. On conclut sur quelques résultats importants et généraux sur l'intersection arithmétique : la formule du changement de base qui montre comment se comporte l'intersection par extension de corps, la formule d'adjonction qui permet essentiellement de calculer les auto-intersections, et enfin le théorème de l'indice de Hodge qui décrit la forme quadratique associée naturellement à l'accouplement d'intersection (nous énonçons une version tronquée de ce théorème, suffisante pour nos préoccupations).

Le **chapitre 5** pose les derniers fondements de notre étude, puisqu'il traite des courbes elliptiques. Au delà des rappels élémentaires sur ces courbes mirifiques et les quantités qui y sont associées (discriminant minimal $\Delta(E/K)$, j-invariant, *etc.*), il est important de passer en revue ce que l'on sait sur leurs modèles minimaux réguliers, et plus particulièrement à quoi ressemble la réduction d'une courbe elliptique en un idéal premier (puisqu'il est ensuite question de chercher des points d'intersection dans les fibres correspondantes). Les courbes elliptiques à multiplications complexes, famille restreinte de courbes pour lesquelles on démontre l'inégalité (4), font également l'objet d'une petite section qui n'évoque que l'essentiel à leur sujet. Les choses deviennent réellement intéressantes lorsqu'on commence à singulariser l'étude du chapitre 4 en liant la hauteur de Néron-Tate (seulement définie pour les courbes elliptiques) à une auto-intersection sur le modèle minimal régulier : le premier lien est le théorème 5.29, dû à Faltings et Hriljac indépendamment, qui implique notamment que sur une courbe elliptique à bonne réduction partout, hauteur et intersection sont liées par la relation

$$\hat{h}(P) = \frac{\langle P, O \rangle}{[K(P) : \mathbb{Q}]},$$

valable pour tout point algébrique P. Une formule étendue au cas semi-stable est donnée dans l'annexe A.2, plus particulièrement dans le corollaire A.12.

Enfin, le **chapitre 6** démontre comment le point de vue arakelovien permet de recouvrer la minoration de Laurent avec une constante explicitant la dépendance en une courbe elliptique E/K à multiplications complexes (c'est-à-dire l'inégalité (4), rappelée dans le théorème 6.1). Pour cela, étant donnés des relèvements de Frobenius F_p (et $\mathrm{F}_1 = \mathrm{Id}$), des paramètres m_p, et P un point d'ordre infini dont on veut minorer la hauteur, on relie la quantité $\hat{h}(P)$ à l'auto-intersection du diviseur

$$\mathcal{L} = \sum_p m_p((\mathrm{F}_p(P)) - [K(P) : K](O))$$

grâce au théorème de Faltings et Hrilac, qui assure par ailleurs qu'elle est négative.

Développer l'auto-intersection du diviseur ci-dessus nous mène ultimement au calcul des intersections locales $\langle \mathrm{F}_p(P), \mathrm{F}_p(P)\rangle_v$ pour v une place finie ou infinie. Les places infinies sont traitées grâce à une nouvelle version du lemme d'Elkies, qu'on baptise ici lemme d'Elkies « pondéré » (lemme 6.8), et qui sert à relativiser en moyenne la négativité de l'intersection de plusieurs points en une place archimédienne : plus on moyenne d'intersections locales de points, plus la minoration est près de zéro (bien que ces intersections archimédiennes soient éventuellement négatives). Plus précisément, si E est une courbe elliptique sur un corps de nombres K, de j-invariant j_E, et L/K une extension finie de degré D, soient P_1, …, P_N des points de $E(L)$ tels qu'eux-mêmes et l'ensemble de leurs conjugués soient tous distincts. Soient m_1, …, m_N des réels strictement positifs qui vérifient $3\sum_{i=1}^{N} m_i^2 < 2D\left(\sum_{i=1}^{N} m_i\right)^2$. Alors,

$$\sum_{\substack{1\leqslant i,j\leqslant N\\(i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geqslant -D\sum_{i=1}^{N} m_i^2 \cdot \left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=1}^{N} m_i\right)^2}{\sum_{i=1}^{N} m_i^2} - 2\right) + \frac{J_v}{12} + \frac{27}{10}\right),$$

où l'on note $J_v = \max(\ln(|j_E|_v),0)$. Si $L = K$ et $m_i = 1$ pour tout i, nous retrouvons le lemme d'Elkies traditionnel.

Il reste à minorer non trivialement les intersections locales aux places finies $\langle \mathrm{F}_{p_i}(P), \mathrm{F}_{p_j}(P)\rangle_v$, ou plus précisément $\langle \mathrm{F}_{p_i}(P), P\rangle_v$. C'est ici que le choix d'une courbe elliptique à multiplications complexes se justifie pleinement, parce que ces fameux endomorphismes de Frobenius induisent des automorphismes de Frobenius sur la réduction modulo des idéaux premiers, et on connaît précisément les points fixes de l'automorphisme de Frobenius sur un corps fini : on en déduit les points d'intersection en une place finie. Ce n'est pas tout à fait direct, puisque P n'est pas supposé rationnel mais algébrique, donc ses coordonnées n'appartiennent pas nécessairement au corps des points fixes de l'automorphisme de Frobenius.

Finalement, il reste à estimer des sommes indexées par des nombres premiers, apparues en cours de route à cause du degré des relèvements du Frobenius et des calculs d'intersections en les places finies. On peut enfin invoquer à propos le théorème de Chebotarev. On démontre notamment dans le lemme 6.9 que si l'hypothèse de Riemann généralisée est vraie, alors pour tout $s \geqslant 10^5$,

$$\sum_{p\in\Pi_s} p \leqslant \frac{1}{2n_K}\left[1 + \frac{3}{\ln(s)}\right]\frac{s^2}{\ln(s)} + \frac{5}{3}\frac{(59{,}07 + 1{,}44\ln(|d_K|) + 76{,}88n_K)}{n_K}s^{3/2}\ln(s),$$

où Π_s désigne l'ensemble des nombres premiers rationnels qui se décomposent complètement dans une extension galoisienne K (une version inconditionnelle existe également).

Obtenir l'inégalité (4) n'est alors plus qu'une affaire de bon choix des paramètres. Il est assez facile de voir que la plupart des inégalités de la démonstration sont optimales en toute généralité, donc une démonstration de la conjecture de Lehmer en utilisant notre méthode nécessiterait un ingrédient supplémentaire, ou un ajustement qui nous a échappé.

Première partie

Théorème de Chebotarev effectif

Chapitre 1

Définitions et théorèmes principaux

« Vous représentez-vous l'humiliation de rectifier, par les humbles chiffres trop certains, ces chiffres grandioses ! »
Léon Bloy, *Exégèse des Lieux Communs* (CXXIX)

1.1 Extensions galoisiennes de corps de nombres

Nous supposons, dans cette section, que nous avons la donnée d'une extension de corps de nombres L/K. Leurs anneaux d'entiers, c'est-à-dire l'ensemble de leurs éléments qui sont annulés par un polynôme unitaire à coefficients entiers, sont respectivement notés $\mathcal{O}_L$ et $\mathcal{O}_K$. Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$ (on dira parfois, simplement, un idéal premier non nul de K), on sait que $\mathfrak{p}\mathcal{O}_L$ s'écrit comme produit d'idéaux premiers de $\mathcal{O}_L$ (voir par exemple [Sam67] ; ceci est valable pour tout anneau de Dedekind). Autrement dit :

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}, \tag{1.1}$$

où les $\mathfrak{P}_i$ sont tous distincts. On appelle l'exposant e_i l'indice de ramification de $\mathfrak{P}_i$ sur $\mathcal{O}_K$ (ou K) et f_i le degré de $\mathfrak{P}_i$ sur K, qui est défini comme la dimension de $\mathcal{O}_L/\mathfrak{P}_i$ sur $\mathcal{O}_K/\mathfrak{p}$ (voir [Sam67], III.§4, théorème 1). En comparant les normes dans cette égalité, puisque la norme est multiplicative, on obtient la formule $\sum_{i=1}^{g} e_i f_i = [L : K]$. On voit alors qu'un idéal maximal de $\mathfrak{p}$ admet au plus $[L : K]$ facteurs premiers dans sa décomposition dans L. En cas d'égalité, on dit que $\mathfrak{p}$ *se décompose complètement* dans L.

Remarque 1.1. Cette formule nous permet aussi de constater qu'il existe au plus $[K : \mathbb{Q}]$ couples $(\mathfrak{p}, m)$, avec $\mathfrak{p}$ idéal premier de K et $m \geqslant 1$, tels que $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}^m) = x$,

pour x un entier donné (l'égalité n'a, par ailleurs, lieu que si x est une puissance d'un nombre premier). En effet, si $x = p^n$ avec p premier et $n \geqslant 1$, alors le nombre g de facteurs premiers de $p\mathcal{O}_K$ vérifie $g \leqslant [K : \mathbb{Q}]$. On conclut en remarquant qu'un idéal premier $\mathfrak{p}$ tel que $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}^m) = p^n$ est nécessairement un diviseur premier de $p\mathcal{O}_K$.

Si tous les exposants e_i égalent 1, on dit que $\mathfrak{p}$ est non ramifié (ou « ne se ramifie pas ») dans L. Il n'y a qu'un nombre fini d'idéaux premiers ramifiés, ce sont ceux qui divisent le discriminant de L sur K. Enfin, tout idéal premier de $\mathcal{O}_L$ ne divise qu'un seul idéal premier de $\mathcal{O}_K$, qu'on détermine en faisant l'intersection avec $\mathcal{O}_K$.

Dorénavant, on fait l'hypothèse supplémentaire que L/K est une extension galoisienne, et on s'intéresse à l'action du groupe de Galois G de L/K sur la décomposition (1.1) d'un idéal maximal de K dans L : il est d'une part assez clair que G laisse stable $\mathcal{O}_K$, comme on le voit en appliquant un de ses éléments à une équation de dépendance intégrale d'un élément entier, et d'autre part si $\mathfrak{P}$ divise $\mathfrak{p}$, alors $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{p}$ pour tout $\sigma \in G$, donc $\sigma(\mathfrak{P})$ figure également dans la décomposition de $\mathfrak{p}\mathcal{O}_K$ (avec le même exposant que $\mathfrak{P}$, puisque G préserve les relations algébriques), ce qui démontre la stabilité de l'action de groupe annoncée.

Nous avons alors le résultat suivant, qui est le point de départ de la théorie galoisienne des décompositions des idéaux maximaux.

Proposition 1.2 ([Sam67], VI.§6.2, proposition 1)**.** *Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_K$, alors l'action de G sur ses diviseurs premiers dans L est transitive. Ils ont tous même indice de ramification e et même degré résiduel f. Ainsi, $\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$, et on a $[L : K] = efg$.*

Pour affiner la compréhension de ces décompositions, deux types de sous-groupes de G sont privilégiés. D'une part, on étudie le stabilisateur $\mathrm{D}_{\mathfrak{P}}$ d'un idéal maximal $\mathfrak{P}$ de la décomposition, qu'on appelle justement groupe de décomposition de $\mathfrak{P}$ (parce que le corps de ses points fixes est une extension maximale de K où $\mathfrak{p}$ se décompose complètement), et d'autre part on s'intéresse au noyau de l'application naturelle

$$\mathrm{red} \ : \begin{cases} \mathrm{D}_{\mathfrak{P}} & \to & \mathrm{Gal}\left(\frac{\mathcal{O}_L}{\mathfrak{P}} / \frac{\mathcal{O}_K}{\mathfrak{p}}\right) \\ \sigma & \mapsto & \bar{\sigma} \end{cases} \tag{1.2}$$

qu'on appelle groupe d'inertie de $\mathfrak{P}$, noté $\mathrm{I}_{\mathfrak{P}}$. D'après la formule des classes, $\mathrm{D}_{\mathfrak{P}}$ est de cardinal $\frac{[L:K]}{g} = ef$.

Proposition 1.3 ([Sam67], VI.§6.2, proposition 2)**.** *Le morphisme* red *est surjectif. On en déduit, en particulier, que* $\mathrm{card}(\mathrm{I}_{\mathfrak{P}}) = e$.

Donc l'idéal premier $\mathfrak{p}$ ne se ramifie pas dans L si, et seulement si $\mathrm{I}_{\mathfrak{P}}$ est trivial. Supposons qu'il n'est pas ramifié ; alors, le groupe de décomposition $\mathrm{D}_{\mathfrak{P}} \subseteq G$ est

canoniquement isomorphe au groupe de Galois de l'extension finie de corps finis $\frac{\mathcal{O}_L}{\mathfrak{P}}/\frac{\mathcal{O}_K}{\mathfrak{p}}$ qui, on le sait, est cyclique. Un générateur privilégié est l'automorphisme de Frobenius $x \mapsto x^q$, où q est le cardinal de $\mathcal{O}_K/\mathfrak{p}$ (ou, de manière équivalente, la norme de $\mathfrak{p}$). L'étude de son élément correspondant dans $\mathrm{D}_{\mathfrak{P}}$ est cruciale en théorie des nombres, et fait l'objet de la définition suivante.

Définition 1.4 (Automorphisme de Frobenius de L/K, [Sam67], VI.§6.3)**.** Si $\mathfrak{p}$ est un idéal maximal de K qui ne se ramifie pas dans L, et $\mathfrak{P}$ un diviseur premier de $\mathfrak{p}$, on appelle automorphisme de Frobenius de L/K associé à $\mathfrak{P}$, qu'on note $\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]$, l'unique automorphisme du groupe de Galois de L/K tel que :

$$\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right](x) \equiv x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \bmod \mathfrak{P}$$

pour tout $x \in \mathcal{O}_L$.

Il est immédiat que deux automorphismes de Frobenius associés à deux diviseurs maximaux de $\mathfrak{p}$ sont conjugués. Donc $\left[\frac{L/K}{\mathfrak{p}}\right] = \left\{\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right] \mid \mathfrak{P}|\mathfrak{p}\right\}$ est une classe de conjugaison de G.

Remarque 1.5. L'action des automorphismes de Frobenius, à la lumière du théorème de Chebotarev énoncé dans la prochaine section, informe grandement à la fois sur la décomposition des idéaux premiers et sur le groupe de Galois de l'extension. Nous n'allons pas expliquer en détail pourquoi, et renvoyons le lecteur intéressé à différents ouvrages et articles sur le sujet : voir [Sam67] §6.4 pour des applications simples aux corps cyclotomiques (démontrant au passage la loi de réciprocité quadratique), [Ser81] pour de nombreuses applications aux courbes elliptiques et formes modulaires, [vdW40] (pages 189–192) pour l'étude de la structure des groupes de Galois, *etc.*, et la dernière partie de ce manuscrit pour les calculs d'intersection. Mentionnons toutefois un lien immédiat entre décomposition d'un idéal maximal et action du Frobenius : si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans L (c'est-à-dire $e = 1$), alors $\mathfrak{p}$ se décompose complètement dans L si, et seulement si $g = [L : K]$ dans la formule de la proposition 1.2, si et seulement si $f = 1$, si et seulement si $\mathrm{D}_{\mathfrak{P}}$ est trivial, si et seulement si $\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]$ est l'automorphisme trivial.

Donc, pour résumer, un idéal maximal $\mathfrak{p}$ non ramifié se décompose complètement dans L si, et seulement si $\left[\frac{L/K}{\mathfrak{p}}\right] = \{1_G\}$. Dans la seconde partie de cette thèse, nous utiliserons le théorème de Chebotarev pour compter précisément le nombre de classes de Frobenius réduites à l'identité.

1.2 Énoncés effectifs du théorème de Chebotarev

Soit L/K une extension galoisienne de corps de nombres, d_L le discriminant absolu de L, n_L le degré de L sur $\mathbb{Q}$. Si G est le groupe de Galois de cette extension, on

désigne un ensemble de G stable par conjugaison par la lettre C ; pour tout $x > 1$, la fonction $\pi_C(x)$ décompte le nombre d'idéaux premiers $\mathfrak{p}$ de K de norme inférieure ou égale à x, qui ne se ramifient pas dans L, et tels que $\left[\frac{L/K}{\mathfrak{p}}\right] \subseteq C$.

Si $C = G$, alors $\pi_G(x)$ compte le nombre d'idéaux premiers de norme inférieure ou égale à x qui ne se ramifient pas dans L, qui est asymptotiquement équivalent au nombre d'idéaux premiers de norme inférieure ou égale à x (puisqu'il n'y a qu'un nombre fini d'idéaux premiers qui se ramifient).

Théorème 1.6 (Théorème des idéaux premiers)**.** *On a, quand $x \to +\infty$,*

$$\pi_G(x) \sim \frac{x}{\ln(x)}.$$

Récemment, Grenié et Molteni ont même obtenu une estimation plus précise au second ordre, sous réserve de la justesse de l'hypothèse de Riemann généralisée (voir [GM15b]).

Le théorème de Chebotarev énonce que plus généralement, on a

$$\pi_C(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)} \text{ quand } x \to \infty.$$

Plus précisément, si $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}$ et $\zeta_L(s) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P})^s}\right)^{-1}$ est la fonction dzêta de Dedekind du corps de nombres L, alors on a une forme effective, qui s'exprime à l'aide de l'éventuel zéro positif β de la fonction ζ_L tel que $0 < 1 - \beta \leqslant \frac{1}{4\ln(d_L)}$ (on l'appelle zéro de Siegel, et on y reviendra dans les sections 2.5 puis 2.7).

Théorème 1.7 (Théorème de Chebotarev effectif)**.** *Conservons les notations ci-dessus. On a, pour tout $x \geqslant \exp\left(110000 n_L (\ln(9d_L^8))^2\right)$,*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\mathrm{Li}\left(x^\beta\right) + 3{,}37 \cdot 10^{13}\frac{|C|}{|G|}x\exp\left(-\frac{1}{12}\sqrt{\frac{\ln(x)}{n_L}}\right).$$

Le terme $\frac{|C|}{|G|}\mathrm{Li}\left(x^\beta\right)$ peut être supprimé en l'absence du zéro exceptionnel β.

On en sait un peu plus sur β : d'après [Sta74], page 148, il existe une constante absolue et effectivement calculable c telle que $\beta < 1 - \frac{1}{cd_L^{1/n_L}}$; d'après [BG62], il est fort probable que $c = \frac{\pi}{6}$ convienne, et nous proposons une borne (moins bonne) dans la section 2.7. Le terme d'erreur est nettement plus petit si on suppose que l'hypothèse de Riemann, énoncée en remarque 2.4, est vérifiée pour ζ_L :

Théorème 1.8. *Supposons que l'hypothèse de Riemann généralisée est vraie pour ζ_L. Alors, pour tout $x \geqslant 2$,*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\Big[\left(\frac{55}{48} + \frac{177}{\ln(x)}\right)\ln(d_L) + \left(\frac{161}{342}\ln(x) + 14 + \frac{352}{\ln(x)}\right)n_L + 682\Big].$$

Remarque 1.9. Dans [Œst79], Oesterlé énonce même, sans démonstration,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\left(\ln(d_L)\left(\frac{1}{\pi} + \frac{5{,}3}{\ln(x)}\right) + n_L\left(2 + \frac{\ln(x)}{2\pi}\right)\right)$$

pour $x \geqslant 3$.

Ces deux théorèmes sont démontrés dans [LO77], mais avec des constantes non explicites. Pour trouver ces constantes, on suit la stratégie de démonstration proposée par [LO77], en soignant les majorations.

1.3 Schéma de démonstration

On suppose dorénavant que C est une unique classe de conjugaison ; le résultat général s'en déduit pour tout ensemble stable par conjugaison par additivité. L'essentiel de la démonstration consiste en la recherche d'une formule asymptotique avec un terme d'erreur explicite pour $\psi_C(x) = \psi_C(x, L/K)$, une sorte de fonction pondérée de décompte des puissances d'idéaux premiers, intimement liée à $\pi_C(x, L/K)$. Cette fonction classique est définie par

$$\psi_C(x, L/K) = \sum_{\substack{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^m \leqslant x \\ \mathfrak{p} \text{ non ramifié} \\ \left[\frac{L/K}{\mathfrak{p}}\right]^m = C}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})).$$

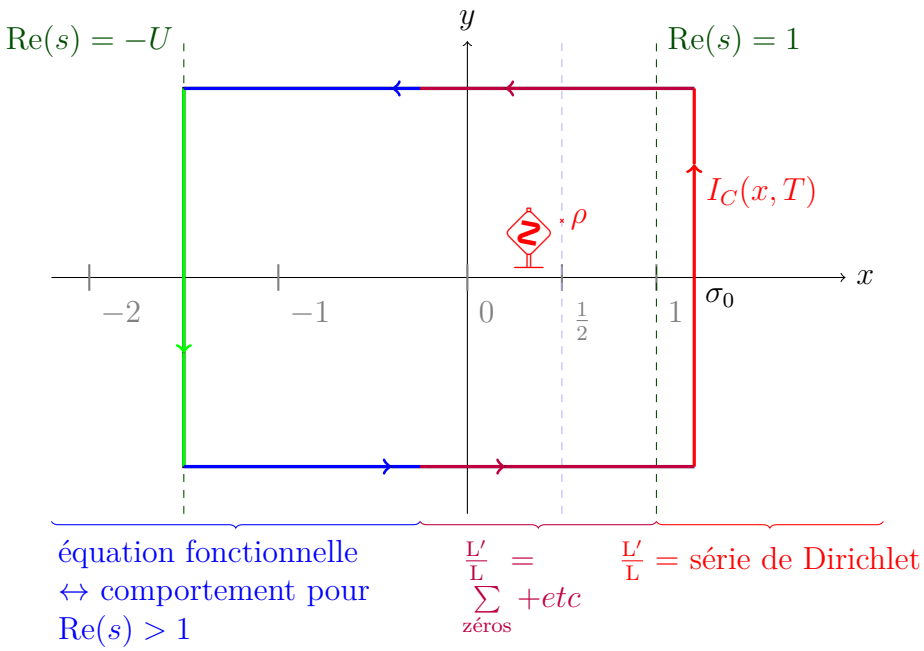
Conformément à [LO77], voici les étapes de la démonstration :

1. La fonction ψ_C est très proche d'une transformée de Mellin inverse tronquée :

$$I_C(x, T) = \frac{1}{2\pi i}\int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s)\frac{x^s}{s}\mathrm{d}s,$$

où la fonction F_C est construite en faisant une combinaison linéaire de dérivées logarithmiques de fonctions L, en profitant de la formule d'orthogonalité des caractères de G pour exclure tous les idéaux premiers qui ne nous intéressent pas ; c'est dans le même esprit que la démonstration traditionnelle du théorème de la progression arithmétique de Dirichlet est construite (voir [Ser77] par exemple). On cherche à étudier l'écart $R_1(x, T)$ entre ψ_C et I_C. Cet écart est explicité dans la section 2.1.

FIGURE 1.1 – Comportement des fonctions L de Hecke le long du contour d'intégration



2. La fonction F_C peut, en fait, être écrite comme combinaison linéaire de dérivées logarithmiques de fonctions L de Hecke. Toutes les singularités de F_C, qui sont des pôles simples, apparaissent en tant que zéros et pôles de ζ_L. Cette étape apparaît dans la section 2.2, et est déjà entièrement explicite dans [LO77] : je citerai le résultat en question *sans le redémontrer*. Notons que les fonctions L sont ici primitives, ce qui permet d'utiliser leurs équations fonctionnelles et la décomposition de leurs dérivées logarithmiques.
3. L'intégrale $I_C(x,T)$ diffère d'une intégrale sur un contour $B_C(x,T)$ par un terme d'erreur $R_2(x,T)$ (la fameuse étape où on « translate à gauche la droite (!) d'intégration »). On a ici besoin de résultats de densité sur les zéros non triviaux de ζ_L pour estimer R_2 ; c'est l'objet de la section 2.2. La figure 1.1 permet de résumer la provenance de chaque inégalité sur les fonctions L de Hecke.
4. L'intégrale sur un contour est évaluée grâce au théorème des résidus, dans la section 2.3. L'intégrande a pour pôles les zéros et les pôles de ζ_L ; on en tire un terme principal $\frac{|C|}{|G|}x$ (c'est la contribution du pôle $s=1$) et une somme $S(x,T)$ indicée par les zéros de ζ_L à l'intérieur du contour de $B_C(x,T)$. On en déduit une formule explicite tronquée pour $\psi_C(x)$ avec un terme d'erreur inconditionnel, qui est donnée dans le théorème 2.15 de la section 2.4.

5. Il faut à présent étudier la somme sur les zéros $S(x,T)$. Si on suppose vraie l'hypothèse de Riemann généralisée, on peut directement aller à la section 2.6. Sinon, on a besoin de mieux connaître l'emplacement des zéros non triviaux : on donne des régions proches de $\mathrm{Re}(s) = 1$ sans zéros pour ζ_L, dans la section 2.5.
6. La formule asymptotique $\psi_C(x) \sim \frac{|C|}{|G|}x$ avec un reste explicité en découle, par un bon choix de T en fonction de x, visant à minimiser les termes d'erreur. C'est traité dans la section 2.6 ; on fait le choix, ici, d'avoir un terme d'erreur valable même pour de petites valeurs de x, mais on peut considérablement améliorer les constantes si on s'affranchit de cette contrainte, *via* d'autres choix de T.
7. Enfin, la formule explicite pour π_C s'obtient par une transformée d'Abel, à la fin de cette démonstration.

Pour résumer, on voit dans la figure 1.2 ce que l'on doit démontrer, en mesurant à chaque étape l'écart explicite entre les deux membres des « égalités ». Au-delà, il faut aimer les calculs.

Les résultats non démontrés ici sont ceux qui ont déjà été explicités dans [LO77], auquel cas on renvoie le lecteur à ce papier. Dans un souci d'auto-suffisance, on rappelle néanmoins toutes les définitions nécessaires à la compréhension de la démonstration. Enfin, quand on remplace les constantes réelles par des nombres rationnels, cela se fait systématiquement grâce aux fractions continuées réduites à l'ordre 3.

FIGURE 1.2 – Schéma grossier de démonstration

$$\begin{aligned}
\psi_C(x, L/K) &\simeq \frac{1}{2\pi i}\int_{\text{segment}} \left(\sum_{\text{L Artin}} \frac{\text{L}'}{\text{L}}\right)\frac{x^s}{s}\mathrm{d}s && \text{(section 2.1)}\\
&= \frac{1}{2\pi i}\int_{\text{segment}} \left(\sum_{\text{L Hecke}} \frac{\text{L}'}{\text{L}}\right)\frac{x^s}{s}\mathrm{d}s && \text{(section 2.2)}\\
&\simeq \frac{1}{2\pi i}\int_{\text{contour}} \left(\sum_{\text{L Hecke}} \frac{\text{L}'}{\text{L}}\right)\frac{x^s}{s}\mathrm{d}s && \text{(section 2.3)}\\
&= \text{résidus} \simeq \frac{|C|}{|G|}x + \frac{|C|}{|G|}\sum_{\chi}\sum_{\rho \text{ zéro}} \bar{\chi}(g)\frac{x^\rho}{\rho} && \text{(section 2.4)}\\
&\simeq \frac{|C|}{|G|}x, && \text{(section 2.6)}
\end{aligned}$$

puis :

$$\psi_C(x, L/K) = \sum_{\substack{\text{N}_{K/\mathbb{Q}}(\mathfrak{p})^m \leqslant x\\ \mathfrak{p} \text{ non ramifié}\\ \left[\frac{L/K}{\mathfrak{p}}\right]^m = C}} \ln(\text{N}_{K/\mathbb{Q}}(\mathfrak{p})) \simeq \sum_{\substack{\text{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x\\ \mathfrak{p} \text{ non ramifié}\\ \left[\frac{L/K}{\mathfrak{p}}\right] = C}} \ln(\text{N}_{K/\mathbb{Q}}(\mathfrak{p})) =: \theta_C(x, L/K),$$

et, enfin :

$$\pi_C(x, L/K) = \frac{|C|}{|G|}\text{Li}(x) + \frac{\theta_C(x) - \frac{|C|}{|G|}x}{\ln(x)} + \int_2^x \frac{\theta_C(t) - \frac{|C|}{|G|}t}{t(\ln(t))^2}\mathrm{d}t \simeq \frac{|C|}{|G|}\text{Li}(x).$$

Chapitre 2

Démonstration effective du théorème de Chebotarev

« Tu m'as donné ta boue et j'en ai fait de l'or. »
Charles Baudelaire, *Les Fleurs du Mal*

2.1 Fonctions L d'Artin et transformées de Mellin

Par commodité, on note $\pi_C(x) = \pi_C(x, L/K)$, $\psi_C(x) = \psi_C(x, L/K)$ et $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$. Enfin, les sommes $\sum_{\mathfrak{p}}$ sont toujours indicées par les idéaux premiers non nuls de l'anneau des entiers de K.

Pour tout caractère irréductible Φ de G, on pose

$$\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in \mathrm{I}_{\mathfrak{P}}} \Phi\left(\left[\frac{L/K}{\mathfrak{P}, \mathfrak{p}}\right]^m \alpha\right)$$

pour $\mathfrak{P}$ divisant $\mathfrak{p}$ dans L : il s'agit de la « moyenne » des images par Φ de tous les éléments de la classe dans $\mathrm{D}_{\mathfrak{P}}/\mathrm{I}_{\mathfrak{P}}$ envoyée sur l'automophisme de Frobenius par le morphisme red défini en (1.2) (notons que si $\mathfrak{p}$ ne se ramifie pas, alors $\Phi_K(\mathfrak{p}^m) = \Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\right)$) ; la quantité ne dépend pas du $\mathfrak{P}$ choisi. Alors, conformément à [LO77] (3.2), la fonction L d'Artin associée à Φ admet pour dérivée logarithmique :

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s, \Phi, L/K) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \Phi_K(\mathfrak{p}^m) \frac{\ln(\mathrm{N}(\mathfrak{p}))}{(\mathrm{N}(\mathfrak{p}))^{ms}}.$$

Motivons cette égalité en examinant les termes correspondant aux idéaux premiers non ramifiés, sans nous étendre sur les complications : une telle fonction L est un produit de facteurs locaux de la forme $\det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1}$ en un idéal premier $\mathfrak{p}$ non ramifié, où ρ est la représentation associée à Φ (voir la troisième

section de [Hei67], qui traite aussi les idéaux ramifiés). Alors, pour $\mathrm{Re}(s) > 1$, en prenant la détermination principale du logarithme,

$$\ln\left(\det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1}\right) = \sum_{m=1}^{\infty}\frac{1}{m}\mathrm{tr}\left(\rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\right)(\mathrm{N}(\mathfrak{p}))^{-ms}\right)$$
$$= \sum_{n=1}^{\infty}\frac{1}{m}\Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\right)(\mathrm{N}(\mathfrak{p}))^{-ms}$$

et sa dérivée égale $-\sum\limits_{m=1}^{\infty}\Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\right)\ln(\mathrm{N}(\mathfrak{p}))(\mathrm{N}(\mathfrak{p}))^{-ms}$.

Revenons à la démonstration. Choisissons un élément g dans C, et posons

$$F_C(s) = -\frac{|C|}{|G|}\sum_{\Phi}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi,L/K).$$

D'après la relation d'orthogonalité des caractères, on a

$$\sum_{\Phi}\bar{\Phi}(g)\Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\alpha\right) = \begin{cases} 0 & \text{si } \left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m\alpha \notin C, \\ \frac{|G|}{|C|} & \text{sinon,}\end{cases}$$

Donc, au bout du compte, la fonction F_C a pour expression

$$F_C(s) = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\theta(\mathfrak{p}^m)\frac{\ln(\mathrm{N}(\mathfrak{p}))}{(\mathrm{N}(\mathfrak{p}))^{ms}}$$

où, pour $\mathfrak{p}$ non ramifié dans L, on a $\theta(\mathfrak{p}^m) = 1$ si $\left[\frac{L/K}{\mathfrak{p}}\right]^m = C$, $\theta(\mathfrak{p}^m) = 0$ sinon, et $|\theta(\mathfrak{p}^m)| \leqslant 1$ si $\mathfrak{p}$ se ramifie dans L.

On voit alors que si on oublie un instant les facteurs correspondant aux idéaux premiers ramifiés, $\psi_C(x)$ est une somme partielle des coefficients de $F_C(s)$. Pour obtenir $\psi_C(x)$ à partir de $F_C(s)$, on utilise la version tronquée de la transformée inverse de Mellin.

Lemme 2.1. *Si $y > 0$, $\sigma > 0$ et $T > 0$, alors*

$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\mathrm{d}s - 1\right| \leqslant \frac{y^\sigma}{\pi}\min\left(\frac{7}{2}, T^{-1}|\ln(y)|^{-1}\right) \quad \textit{si } y > 1,$$
$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\mathrm{d}s - \frac{1}{2}\right| \leqslant \sigma T^{-1} \quad \textit{si } y = 1,$$
$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\mathrm{d}s\right| \leqslant \frac{y^\sigma}{\pi}\min\left(\frac{7}{2}, T^{-1}|\ln(y)|^{-1}\right) \quad \textit{si } 0 < y < 1.$$

Démonstration. Voir [Ram07], lemme 7.1, et [Dav67], pages 109–110, pour le cas $y = 1$ (qu'on n'utilisera toutefois pas par la suite). □

Soient $\sigma_0 > 1$ et $x \geqslant 2$. Supposons provisoirement que x n'est pas un entier. On définit $I_C(x,T) = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} F_C(s)\frac{x^s}{s}\mathrm{d}s$. Comme la série de Dirichlet définissant F_C est absolument convergente pour $\mathrm{Re}(s) > 1$, on peut intégrer terme à terme (suivant le lemme 2.1) pour obtenir

$$\left| I_C(x,T) - \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p})^m \leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p})) \right| \leqslant R_0(x,T),$$

où

$$R_0(x,T) = \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p}^m)\neq x}} \left(\frac{x}{\mathrm{N}(\mathfrak{p}^m)}\right)^{\sigma_0} \min\left(\frac{7}{2}, T^{-1}\left|\ln\left(\frac{x}{\mathrm{N}(\mathfrak{p}^m)}\right)\right|^{-1}\right)\frac{\ln(\mathrm{N}(\mathfrak{p}))}{\pi}. \tag{2.1}$$

Si x est entier, la continuité de $x \mapsto I_C(x,T)$ et de $x \mapsto R_0(x,T)$ permet d'écrire l'inégalité suivante, finalement valable pour tout $x \geqslant 2$:

$$\left| I_C(x,T) - \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p})^m \leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p})) \right| \leqslant R_0(x,T) + \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p}^m) = x}} \ln(\mathrm{N}(\mathfrak{p})). \tag{2.2}$$

La somme du membre de gauche dans (2.2) égale $\psi_C(x)$, aux termes ramifiés près. On a $\mathrm{N}(\mathfrak{p}) \geqslant 2$, et d'après [Ser81] (prop. 5 du n°1.3) on a

$$\sum_{\mathfrak{p}\text{ ramifié}} \ln(\mathrm{N}(\mathfrak{p})) \leqslant \frac{2}{|G|}\ln(d_L). \tag{2.3}$$

Donc,

$$\begin{aligned}
\left| \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p}^m)\leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p})) - \psi_C(x) \right| &\leqslant \sum_{\substack{\mathfrak{p},m \\ \mathfrak{p}\text{ ramifié} \\ \mathrm{N}(\mathfrak{p}^m)\leqslant x}} \ln(\mathrm{N}(\mathfrak{p})) \\
&\leqslant \sum_{\mathfrak{p}\text{ ramifié}} \ln(\mathrm{N}(\mathfrak{p})) \sum_{\substack{m \\ \mathrm{N}(\mathfrak{p}^m)\leqslant x}} 1 \\
&\leqslant \frac{\ln(x)}{\ln(2)} \sum_{\mathfrak{p}\text{ ramifié}} \ln(\mathrm{N}(\mathfrak{p})) \\
&\leqslant \frac{2}{\ln(2)}\frac{\ln(x)\ln(d_L)}{|G|}.
\end{aligned} \tag{2.4}$$

Comme il y a au plus n_K paires distinctes $(\mathfrak{p}, m)$ telles que $\mathrm{N}(\mathfrak{p}^m) = x$, on a

$$\sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p}^m)=x}} \ln(\mathrm{N}(\mathfrak{p})) \leqslant n_K \ln(x). \tag{2.5}$$

Alors, (2.2), (2.4) et (2.5) entraînent

$$\psi_C(x) = I_C(x,T) + R_1(x,T),$$

où

$$|R_1(x,T)| \leqslant \frac{2}{\ln(2)} \frac{\ln(x)\ln(d_L)}{|G|} + n_K \ln(x) + R_0(x,T).$$

Le reste de la section est voué à estimer $R_0(x,T)$. À présent, on prend $\sigma_0 = 1 + \frac{1}{\ln(x)}$ (on a alors $x^{\sigma_0} = ex$). Écrivons $R_0(x,T) = S_1 + S_2 + S_3$, où S_1 est la somme dans (2.1) n'impliquant que les idéaux $\mathfrak{p}$ tels que $|x - \mathrm{N}(\mathfrak{p}^m)| \geqslant \frac{1}{4}x$, tandis que S_2 est indicé par ceux tels que $|x - \mathrm{N}(\mathfrak{p}^m)| \leqslant 1$, et S_3 récupère les termes restants.

Pour $\mathfrak{p}$ tel que $|\mathrm{N}(\mathfrak{p}^m) - x| \geqslant \frac{1}{4}x$, on a $\min\left(\frac{7}{2}, T^{-1}\left|\ln\left(\frac{x}{\mathrm{N}(\mathfrak{p})^m}\right)\right|^{-1}\right) \leqslant \frac{T^{-1}}{\ln\left(\frac{5}{4}\right)}$. On obtient alors,

$$S_1 \leqslant \frac{xT^{-1}e}{\pi \ln\left(\frac{5}{4}\right)} \sum_{\mathfrak{p},m} \mathrm{N}(\mathfrak{p})^{-m\sigma_0} \ln(\mathrm{N}(\mathfrak{p})) = \frac{xT^{-1}e}{\pi \ln\left(\frac{5}{4}\right)} \left(-\frac{\zeta_K'}{\zeta_K}(\sigma_0)\right).$$

La dernière majoration dépend de la comparaison entre $-\frac{\zeta_{\mathbb{Q}}'}{\zeta_{\mathbb{Q}}}(\sigma_0)$ et $(\sigma_0 - 1)^{-1}$. De l'analyse classique permet d'obtenir :

Lemme 2.2. *On a, pour $\sigma > 1$,*

$$0 \leqslant -\frac{\zeta_K'}{\zeta_K}(\sigma) \leqslant -n_K \frac{\zeta_{\mathbb{Q}}'}{\zeta_{\mathbb{Q}}}(\sigma) \leqslant n_K(\sigma - 1)^{-1}.$$

Démonstration. Partant de la formule du produit eulérien pour ζ_K, on a pour $\mathrm{Re}(s) > 1$,

$$-\frac{\zeta_K'}{\zeta_K}(s) = \sum_{m=1}^{\infty} \Lambda_K(m) m^{-s}, \tag{2.6}$$

où

$$\Lambda_K(m) = \begin{cases} \left(\sum\limits_{\substack{\mathfrak{p}|p \\ \mathfrak{f}(\mathfrak{p}/p)|r}} \mathfrak{f}(\mathfrak{p}/p) \right) \ln(p) \text{ si } n = p^r, p \text{ premier}, r \geqslant 1, \\ 0 \text{ sinon.} \end{cases} \tag{2.7}$$

Le terme général de la série de Dirichlet de $-\frac{\zeta_K'}{\zeta_K}$ est positif, donc elle est évidemment positive quand on l'évalue en $\sigma > 1$.

La seconde inégalité est prouvée dans [LO77], page 426, et [Del87] démontre l'inégalité $-\frac{\zeta'_{\mathbb{Q}}}{\zeta_{\mathbb{Q}}}(\sigma) \leqslant \frac{1}{\sigma-1} - \frac{1}{2\sigma^2}$; on propose une démonstration plus courte de la dernière inégalité du lemme, moins exigeante : elle se déduit de l'égalité

$$\zeta_{\mathbb{Q}}(\sigma) = \frac{\sigma}{\sigma-1} - \sigma I(\sigma),$$

où $I(\sigma) = \int_1^\infty (t-[t])t^{-\sigma-1}\mathrm{d}t$. Sachant cela, on obtient facilement

$$\frac{\zeta'_{\mathbb{Q}}}{\zeta_{\mathbb{Q}}}(\sigma) + \frac{1}{\sigma-1} > \frac{1-(2\sigma-1)I(\sigma)}{\zeta(\sigma)(\sigma-1)}$$

pour tout $\sigma > 1$. Comme $I(\sigma) = \frac{1}{\sigma}\left(\frac{\sigma}{\sigma-1} - \zeta_{\mathbb{Q}}(\sigma)\right)$, l'inégalité à démontrer se réduit à l'inégalité $\zeta_{\mathbb{Q}}(\sigma) \geqslant \frac{\sigma^2}{(\sigma-1)(2\sigma-1)} = \frac{1}{2} + \frac{1}{\sigma-1} - \frac{1}{2}\frac{1}{2\sigma-1}$, qui est un exercice simple d'analyse une fois qu'on a constaté que $\zeta_{\mathbb{Q}}(\sigma) \geqslant 1 + \int_2^\infty \frac{\mathrm{d}t}{t^\sigma} = 1 + \frac{1}{\sigma-1}\frac{1}{2^{\sigma-1}}$. □

Reprenons. On a

$$S_1 \leqslant \frac{xT^{-1}e}{\pi \ln\left(\frac{5}{4}\right)}\left(-n_K\frac{\zeta'_{\mathbb{Q}}}{\zeta_{\mathbb{Q}}}(\sigma_0)\right) \leqslant \frac{e}{\pi \ln\left(\frac{5}{4}\right)} n_K x T^{-1}\ln(x). \tag{2.8}$$

La majoration de S_2 est poussée plus loin que dans [LO77] assez facilement : on a, pour $x \geqslant 2$,

$$S_2 \leqslant \frac{7}{\pi} n_K \ln(x+1)\left(\frac{x}{x-1}\right)^{\sigma_0} \leqslant \frac{14e\ln(3)}{\pi\ln(2)} n_K \ln(x). \tag{2.9}$$

Enfin, pour S_3 (qui est indicé par les idéaux $\mathfrak{p}$ tels que $1 < |\mathrm{N}(\mathfrak{p}^m) - x| < \frac{x}{4}$) on a, en vertu de l'inégalité $\left|\ln\left(\frac{x}{n}\right)\right|^{-1} \leqslant \frac{2n}{|x-n|}$ (pour $2n \geqslant x$),

$$\begin{aligned}
S_3 &\leqslant \frac{4e^2}{3^{1+1/\ln(2)}\pi} T^{-1}\ln\left(\frac{5x}{4}\right) \sum_{\substack{n \\ 1<|n-x|<\frac{x}{4}}} \left|\ln\left(\frac{x}{n}\right)\right|^{-1} \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}(\mathfrak{p})^m = n}} 1 \\
&\leqslant \frac{8e^2}{3^{1+1/\ln(2)}\pi} n_K T^{-1}\ln\left(\frac{5x}{4}\right) \sum_{\substack{n\in\mathbb{N} \\ 1<|n-x|<\frac{x}{4}}} \frac{n}{|x-n|} \\
&\leqslant \frac{16e^2}{3^{1+1/\ln(2)}\pi} n_K T^{-1}\ln\left(\frac{5x}{4}\right) \sum_{\substack{k\in\mathbb{N} \\ 1<k<\frac{x}{4}}} \left(1+\frac{x}{k}\right) \\
&\leqslant \frac{16e^2}{3^{1+1/\ln(2)}\pi} n_K T^{-1} x \ln\left(\frac{5x}{4}\right)\left(\frac{1}{4} + \ln\left(\frac{x}{2}\right)\right) \\
&\leqslant \frac{16e^2}{3^{1+1/\ln(2)}\pi} n_K T^{-1} x (\ln(x))^2
\end{aligned} \tag{2.10}$$

En regroupant (2.8), (2.9) et (2.10), on obtient une majoration de R_0, puis de R_1 :

$$\begin{aligned} R_0(x,T) &\leqslant \frac{14e\ln(3)}{\pi\ln(2)} n_K \ln(x) + \left(\frac{16e^2}{3^{1+1/\ln(2)}\pi} + \frac{e}{\ln\left(\frac{5}{4}\right)\ln(2)\pi} \right) n_K T^{-1} x (\ln(x))^2 \\ &\leqslant \frac{72440}{3773} n_K \ln(x) + \frac{49}{6} n_K T^{-1} x (\ln(x))^2, \end{aligned}$$

valable pour tout $x \geqslant 2$ et tout $T \geqslant 1$, et donc,

$$|R_1(x,T)| \leqslant \frac{2}{\ln(2)} \frac{\ln(x)\ln(d_L)}{|G|} + \frac{76213}{3773} n_K \ln(x) + \frac{49}{6} n_K T^{-1} x (\ln(x))^2. \tag{2.11}$$

2.2 Réduction au cas des fonctions L de Hecke

Soit $g \in C$, et soit H le sous-groupe de G engendré par g, E le corps fixé par H, et notons avec la lettre χ les caractères irréductibles de H (qui sont de dimension 1).

Lemme 2.3 ([LO77], pages 429–431)**.** *On a*

$$F_C(s) = -\frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{\mathrm{L}'}{\mathrm{L}}(s, \chi, L/E).$$

Ainsi, F_C s'écrit non seulement à l'aide de fonctions L d'Artin correspondant à des caractères non linéaires de G, mais on peut aussi les exprimer comme combinaison linéaire de dérivées logarithmes de fonctions L de Hecke *abéliennes*.

On a donc

$$I_C(x,T) = -\frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{\mathrm{L}'}{\mathrm{L}}(s, \chi, L/E) \mathrm{d}s, \tag{2.12}$$

et on a vu que ψ_C s'écrit comme somme de cette intégrale et de R_1, qu'on a déjà estimé en (2.11). Il s'agit donc, à présent, d'évaluer les intégrales présentes dans (2.12). D'où la nécessité de borner le nombre de singularités de $\frac{\mathrm{L}'}{\mathrm{L}}$. C'est l'occasion de rappeler quelques propriétés classiques de ces fonctions L, qu'on peut retrouver dans le chapitre 7, §8, de [Neu99].

Comme les corps L et E sont fixés, on peut omettre L/E dans l'écriture de $\mathrm{L}(s, \chi, L/E)$. Soit $F(\chi)$ le conducteur de χ, et soit

$$A(\chi) = d_E \mathrm{N}_{E/\mathbb{Q}}(F(\chi)).$$

On définit $\delta_{\chi=1}(\chi)$ comme étant égal à 1 pour le caractère principal, et 0 sinon. Enfin, pour rappel, pour chaque χ il existe deux entiers naturels $a(\chi)$ et $b(\chi)$ tels que $a(\chi) + b(\chi) = n_E$, de sorte que si on pose

$$\gamma_\chi(s) = \left(\pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2} \right) \right)^{b(\chi)} \left(\pi^{-s/2} \Gamma\left(\frac{s}{2} \right) \right)^{a(\chi)}$$

et

$$\xi(s,\chi) = (s(s-1))^{\delta_{\chi=1}(\chi)} A(\chi)^{s/2} \gamma_\chi(s) \mathrm{L}(s,\chi), \tag{2.13}$$

alors on a l'équation fonctionnelle

$$\xi(1-s,\bar{\chi}) = W(\chi)\xi(s,\chi),$$

où $W(\chi)$ est une constante de module 1. De plus, $\xi(\cdot,\chi)$ est une fonction entière d'ordre 1 qui ne s'annule pas en 0, donc

$$\xi(s,\chi) = e^{B_1(\chi)+B(\chi)s} \prod_\rho \left(1-\frac{s}{\rho}\right) e^{s/\rho} \tag{2.14}$$

pour des constantes $B_1(\chi)$ et $B(\chi)$, où $\rho = \beta + i\gamma$ parcourt l'ensemble des zéros (non triviaux) de $\mathrm{L}(\cdot,\chi)$ tels que $0 < \beta < 1$. La lettre ρ désignera toujours ces zéros.

Remarque 2.4. Si l'ensemble des zéros non triviaux de $\mathrm{L}(\cdot,\chi)$ est situé sur la droite $\mathrm{Re}(s) = \frac{1}{2}$, on dit que l'hypothèse de Riemann est vérifiée pour $\mathrm{L}(\cdot,\chi)$. On appelle hypothèse de Riemann généralisée (notée « HRG » dans cette dissertation) l'affirmation que cette hypothèse est vérifiée pour toute fonction L de Hecke.

En dérivant logarithmiquement (2.13) et (2.14), on obtient la relation importante

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = B(\chi) + \sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{\rho}\right) - \frac{1}{2}\ln(A(\chi)) - \delta_{\chi=1}(\chi)\left(\frac{1}{s}+\frac{1}{s-1}\right) - \frac{\gamma_\chi'}{\gamma_\chi}(s), \tag{2.15}$$

valable pour tout nombre complexe s où ces quantités sont définies. On ne sait pas déterminer exactement la dépendance de B en fonction de χ, mais on sait tout de même déduire de l'équation fonctionnelle ceci :

Lemme 2.5 ([Odl77], (2.8))**.** *En conservant les notations ci-dessus,*

$$\mathrm{Re}(B(\chi)) = -\sum_\rho \mathrm{Re}\left(\frac{1}{\rho}\right),$$

et

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) + \frac{\mathrm{L}'}{\mathrm{L}}(s,\bar{\chi}) = \sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{s-\bar{\rho}}\right) - \ln(A(\chi)) - 2\delta_{\chi=1}(\chi)\left(\frac{1}{s}+\frac{1}{s-1}\right) - 2\frac{\gamma_\chi'}{\gamma_\chi}(s). \tag{2.16}$$

On établit ici quelques résultats préliminaires.

Lemme 2.6. *Si* $\mathrm{Re}(s) > 1$*, alors* $\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leqslant \frac{n_E}{\mathrm{Re}(s)-1}$.

Démonstration. En comparant leurs séries de Dirichlet, on voit que

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leqslant -\frac{\zeta_E'}{\zeta_E}(\mathrm{Re}(s)),$$

et le lemme 2.2 permet de conclure aisément. □

Lemme 2.7. *Soit z un nombre complexe.*

1. *Si* $\mathrm{Re}(z) \geqslant a > 0$, *alors*
$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|) + \frac{\pi}{2} + \frac{1}{a}.$$
2. *Si* $\mathrm{Re}(z) > \frac{1}{2}$, *alors*
$$\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(z)\right) \leqslant \ln(|z|).$$
3. *Si* $|\mathrm{Im}(z)| \geqslant b \geqslant 1$, *alors*
$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|) + \pi\left(1 + \frac{1}{2b}\right) + \frac{1}{2b}.$$
4. *Si* $|z+k| \geqslant \frac{1}{8}$ *pour tout entier naturel* k, *alors*
$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|) + \frac{83}{5}.$$

Démonstration. Le produit de Weierstrass de Γ nous enseigne, en considérant sa dérivée logarithmique, que

$$-\frac{\Gamma'}{\Gamma}(z) = \gamma_0 + \sum_{n=1}^{\infty}\left(\frac{1}{z+n-1} - \frac{1}{n}\right)$$

pour tout complexe z différent des entiers négatifs (γ_0 désigne la constante d'Euler-Mascheroni). Alors, en utilisant la formule d'Euler-McLaurin (pour $z > 0$) avec cette somme, on obtient que

$$\frac{\Gamma'}{\Gamma}(z) = \ln(z) - \frac{1}{2z} + \int_0^{\infty}\frac{B_1(\{x\})}{(z+x)^2}\mathrm{d}x = \ln(z) + \int_0^{\infty}\frac{B_1(\{x\}) - 1/2}{(z+x)^2}\mathrm{d}x,$$

où ln est la détermination principale du logarithme, et $B_1 = X - \frac{1}{2}$ est le premier polynôme de Bernoulli ; l'égalité pour tout z complexe (à l'exception de $z \leqslant 0$) s'obtient par le principe du prolongement analytique. On en déduit que, pour $\mathrm{Re}(z) \geqslant a \geqslant 1$,

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|) + \frac{\pi}{2} + \frac{1}{a}.$$

On procède de même pour l'inégalité concernant la partie réelle, ainsi que pour l'inégalité dans le domaine $|\mathrm{Im}(z)| \geqslant 1$. Passons à la quatrième inégalité : si $\mathrm{Re}(z) < 1$ et $|\mathrm{Im}(z)| < 1$ (notons que le cas $|\mathrm{Im}(z)| \geqslant 1$ est déjà traité et vérifie l'inégalité annoncée), l'équation fonctionnelle vérifiée par Γ permet de montrer que

$$\frac{\Gamma'}{\Gamma}(z) = \frac{\Gamma'}{\Gamma}(z+m) - \sum_{k=0}^{m-1} \frac{1}{z+k}$$

pour tout entier $m > 0$. On pose $m = -[\mathrm{Re}(z) - 1]$, de sorte que $\mathrm{Re}(z+m) \geqslant 1$ (c'est le plus petit entier naturel à vérifier cette inégalité), ce qui permet de borner $\frac{\Gamma'}{\Gamma}(z+m)$:

$$\left|\frac{\Gamma'}{\Gamma}(z+m)\right| \leqslant \ln\left(\sqrt{5}\right) + \frac{\pi}{2} + 1.$$

Comme $|z+k| < \frac{1}{2}$ pour au plus un entier naturel k, et qu'on a en plus supposé que $|z+k| \geqslant \frac{1}{8}$ pour tout entier naturel k et $\mathrm{Re}(z) < 2 - m$, on a

$$\left|\sum_{k=0}^{m-1} \frac{1}{z+k}\right| \leqslant 10 + \sum_{k=0}^{m-3} \frac{1}{-2+(m-k)} < 10 + \sum_{j=1}^{m-2} \frac{1}{j} \leqslant 11 + \ln(|z|+1),$$

ce raisonnement valant du moins si $m > 2$ (si $m \leqslant 2$, l'inégalité vaut même sans le terme logarithmique), pour finalement donner l'inégalité

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|) + \ln(9) + \ln\left(\sqrt{5}\right) + \frac{\pi}{2} + 12,$$

valable pour tout z complexe tel que $|z+k| \geqslant \frac{1}{8}$ pour tout entier naturel k. D'où l'inégalité annoncée. □

Lemme 2.8. *Soit s un nombre complexe.*

1. *Si $\mathrm{Re}(s) > -\frac{1}{2}$ et $|s| \geqslant \frac{1}{8}$, alors*

$$\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \leqslant \frac{n_E}{2}\left(\ln(1+|s|) + \frac{164}{7}\right).$$

2. *Si $\mathrm{Re}(s) > 1$, alors*

$$\mathrm{Re}\left(\frac{\gamma_\chi'}{\gamma_\chi}(s)\right) \leqslant \frac{n_E}{2}\ln\left(\frac{|s+1|}{2\pi}\right).$$

3. *Si $s = \sigma + it$ avec $\sigma \geqslant a > 0$, alors*

$$\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \leqslant \frac{n_E}{2}\left(\ln(|t|+\sigma+1) + \left(\frac{\pi}{2} + \frac{2}{a} + \ln\left(\frac{\pi}{2}\right)\right)\right),$$

Par exemple, pour $a = 1$, on a $\frac{\pi}{2} + \frac{2}{a} + \ln\left(\frac{\pi}{2}\right) \leqslant \frac{539}{134}$. Si $a = 2$, cette même quantité est inférieure à $\frac{405}{134}$.

4. Si s est tel que $|s+k| \geqslant \frac{1}{8}$ pour tout entier naturel k, alors

$$\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \leqslant \frac{n_E}{2}\left(\ln(1+|s|)+\frac{989}{58}\right).$$

Démonstration. Le lemme précédent montre que si $|z| \geqslant \frac{1}{16}$ et $\mathrm{Re}(z) \geqslant -\frac{1}{4}$, alors :

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leqslant \ln(|z|)+\frac{827}{36}. \tag{2.17}$$

En effet, si on suppose $\mathrm{Re}(z) > -\frac{1}{4}$, alors $\mathrm{Re}(z+2) > \frac{7}{4}$, donc

$$\left|\frac{\Gamma'}{\Gamma}(z+2)\right| \leqslant \ln(|z|+2)+\frac{\pi}{2}+\frac{4}{7}.$$

L'équation fonctionnelle donne alors l'inégalité (2.17). En particulier, si

$$\gamma_\chi(s) = \left[\pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)\right]^{b(\chi)} \cdot \left[\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right]^{a(\chi)},$$

alors

$$\frac{\gamma_\chi'}{\gamma_\chi}(s) = -\frac{n_E\ln(\pi)}{2}+\frac{b(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+1}{2}\right)+\frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right), \tag{2.18}$$

car $a(\chi)+b(\chi) = n_E$. La première inégalité découle de (2.17), la seconde du deuxième point du lemme 2.7, la troisième du premier point du même lemme, et enfin la dernière inégalité se déduit du dernier point de ce même lemme. □

Fort de tous ces résultats, on peut démontrer le premier lemme important de [LO77] sous une forme explicite :

Lemme 2.9. *Soit $n_\chi(t)$ le nombre de zéros $\rho = \beta + i\gamma$ de $\mathrm{L}(\cdot,\chi)$ avec $0 < \beta < 1$ et $|\gamma - t| \leqslant 1$. Pour tout t, on a*

$$n_\chi(t)+n_\chi(-t) \leqslant \frac{5}{2}\left[\ln(A(\chi))+2\delta_{\chi=1}(\chi)\left(\frac{2}{4+t^2}+\frac{1}{1+t^2}\right)+n_E\left(\ln\left(\frac{|t|+3}{2\pi}\right)+2\right)\right].$$

Démonstration. On part de l'identité (2.16) :

$$\sum_\rho\left(\frac{1}{s-\rho}+\frac{1}{s-\bar\rho}\right) = \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)+\frac{\mathrm{L}'}{\mathrm{L}}(s,\bar\chi)+\ln(A(\chi))+2\delta_{\chi=1}(\chi)\left(\frac{1}{s}+\frac{1}{s-1}\right)+2\frac{\gamma_\chi'}{\gamma_\chi}(s).$$

On sait estimer chacune des quantités du membre de droite, d'après ce qui précède. Prenons $s = 2 + it$. On a :

$$\mathrm{Re}\left(\sum_{\rho}\left(\frac{1}{s-\rho}+\frac{1}{s-\bar{\rho}}\right)\right) \leqslant 2n_E + \ln(A(\chi)) + 2\delta_{\chi=1}(\chi)\left(\frac{2}{4+t^2}+\frac{1}{1+t^2}\right) + n_E \ln\left(\frac{|t|+3}{2\pi}\right),$$

puis

$$\sum_{\rho}\mathrm{Re}\left(\frac{1}{s-\rho}+\frac{1}{s-\bar{\rho}}\right) \geqslant \sum_{\substack{\rho \\ |\gamma-t|\leqslant 1}} \frac{2-\beta}{(2-\beta)^2+(t-\gamma)^2} + \sum_{\substack{\rho \\ |\gamma+t|\leqslant 1}} \frac{2-\beta}{(2-\beta)^2+(t+\gamma)^2},$$

ce dont on déduit facilement :

$$\sum_{\rho}\mathrm{Re}\left(\frac{1}{s-\rho}+\frac{1}{s-\bar{\rho}}\right) \geqslant \left(\sum_{\substack{\rho \\ |\gamma-t|\leqslant 1}} + \sum_{\substack{\rho \\ |\gamma+t|\leqslant 1}}\right)\frac{2}{5} = \frac{2}{5}(n_\chi(t)+n_\chi(-t)). \qquad \square$$

Remarque 2.10. On peut déduire du théorème 1 de [KN12] une majoration explicite plus fine de n_χ pour χ le caractère trivial.

Ce lemme permet d'obtenir d'autres estimations qui informent sur l'importance des zéros des fonctions L dans la démonstration effective du théorème de Chebotarev : des calculs lourds mais sans mystère conduisent à :

Lemme 2.11. *Pour tout réel ε tel que $0 < \varepsilon \leqslant 1$, on a*

$$\left|B(\chi)+\sum_{|\rho|<\varepsilon}\frac{1}{\rho}\right| \leqslant \frac{1}{8}\left(5\pi^2+34+\frac{10}{\varepsilon}\right)\ln(A(\chi)) + \delta_{\chi=1}(\chi)\left(\frac{295}{16}+\frac{15}{4\varepsilon}\right) + \left(\frac{549}{25}+\frac{31}{8\varepsilon}\right)n_E$$

Démonstration. On a :

$$\left|B(\chi)+\sum_{|\rho|<\varepsilon}\frac{1}{\rho}\right| \leqslant \left|B(\chi)+\sum_{\rho}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| \tag{2.19}$$

$$+ \left|\sum_{|\rho|\geqslant 1}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| \tag{2.20}$$

$$+ \left|\sum_{|\rho|<1}\frac{1}{2-\rho}\right|$$

$$+ \left|\sum_{\varepsilon<|\rho|<1}\frac{1}{\rho}\right|. \tag{2.21}$$

Les sommes dans (2.20) et (2.21) s'estiment de la même manière, à l'aide de la fonction n_χ introduite pour le lemme 2.9. Par exemple, dans le cas de (2.20), comme $\left|\frac{1}{2-\rho}+\frac{1}{\rho}\right| = \frac{2}{|(2-\rho)\rho|} \leqslant \frac{2}{|\rho|^2}$, on a

$$\begin{aligned}\left|\sum_{|\rho|\geqslant 1}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| &\leqslant \sum_{\substack{t=-\infty\\ t \text{ impair}}}^{\infty}\sum_{\substack{|\rho|\geqslant 1\\ t\leqslant\gamma\leqslant t+2}}\frac{2}{|\rho|^2}\\ &\leqslant 2\sum_{j=0}^{\infty}\frac{n_\chi(2j+2)+n_\chi(-(2j+2))}{(2j+1)^2}+2n_\chi(0),\end{aligned}$$

et alors, grâce au lemme 2.9,

$$\begin{aligned}\left|\sum_{|\rho|\geqslant 1}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| &\leqslant 5\left(\sum_{j=0}^{\infty}\frac{1}{(2j+1)^2}+\frac{1}{2}\right)\left(\ln(A(\chi))+2n_E\right)\\ &\quad+5n_E\left(\sum_{j=0}^{2}\frac{\ln\left(\frac{2j+5}{2\pi}\right)}{(2j+1)^2}+\int_2^{\infty}\frac{\ln\left(\frac{2t+5}{2\pi}\right)}{(2t+1)^2}\mathrm{d}t+\frac{1}{2}\ln\left(\frac{3}{2\pi}\right)\right)\\ &\quad+5\delta_{\chi=1}(\chi)\left(\frac{12}{5}+\int_0^{\infty}\left(\frac{2}{4+(u+2)^2}+\frac{1}{1+(u+2)^2}\right)\frac{\mathrm{d}u}{(u+1)^2}\right)\\ &=\frac{5}{8}(\pi^2+4)\ln(A(\chi))+\delta_{\chi=1}(\chi)\left(\frac{33}{2}-\frac{6}{5}\ln(2)-\frac{3\pi}{20}-\frac{5}{4}\ln(5)\right)\\ &\quad+\frac{59336}{3949}n_E.\end{aligned}$$

Semblablement, on trouve

$$\left|\sum_{\varepsilon\leqslant|\rho|<1}\frac{1}{\rho}\right| \leqslant \frac{n_\chi(0)}{\varepsilon} \leqslant \frac{5}{4\varepsilon}\left[\ln(A(\chi))+3\delta_{\chi=1}(\chi)+n_E\left(\ln(3)+2\right)\right].$$

Si $|\rho|<1$, alors $|2-\rho|>1$, donc

$$\left|\sum_{|\rho|<1}\frac{1}{2-\rho}\right| \leqslant \frac{5}{4}\left[\ln(A(\chi))+3\delta_{\chi=1}(\chi)+n_E\left(\ln(3)+2\right)\right],$$

et il ne reste plus que la somme (2.19) à évaluer. Pour cela, on pose $s=2$ dans (2.15), et on estime tous les termes qui nous intéressent grâce au lemme 2.6 et au lemme 2.8 :

$$\left|B(\chi)+\sum_{\rho}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| \leqslant \frac{3}{2}\delta_{\chi=1}(\chi)+\frac{n_E}{2}\left(\ln(3)+\frac{673}{134}\right)+\frac{1}{2}\ln(A(\chi)).$$

En regroupant toutes ces estimations, on obtient le lemme annoncé. □

Dans le même esprit de démonstration :

Lemme 2.12. *Si $s = \sigma + it$ avec $-\frac{1}{2} \leqslant \sigma \leqslant 3$ et $|s| \geqslant \frac{1}{8}$, alors :*

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) + \frac{\delta_{\chi=1}(\chi)}{s-1} - \sum_{\substack{\rho \\ |\gamma - t| \leqslant 1}} \frac{1}{s-\rho}\right| \leqslant \frac{5}{4}\left(1 + \frac{7}{4}\pi^2\right)\ln(A(\chi))$$
$$+ \left(\frac{79}{3} + \frac{5}{2}\left(\frac{2}{4+t^2} + \frac{1}{1+t^2}\right)\right)\delta_{\chi=1}(\chi) + \frac{n_E}{2}\ln(|t|+5)\left(57 + \frac{35}{|t|+4}\right) + \frac{176}{3}n_E.$$

Démonstration. On évalue l'identité (2.15) en $\sigma + it$ puis en $3 + it$, et on soustrait les deux égalités résultantes. Ainsi, $B(\chi)$ est éliminé, et on a :

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) - \frac{\mathrm{L}'}{\mathrm{L}}(3+it,\chi) = \sum_{\rho}\left(\frac{1}{s-\rho} - \frac{1}{3+it-\rho}\right) - \frac{\gamma_\chi'}{\gamma_\chi}(s) + \frac{\gamma_\chi'}{\gamma_\chi}(3+it)$$
$$- \delta_{\chi=1}(\chi)\left(\frac{1}{s} + \frac{1}{s-1} - \frac{1}{2+it} - \frac{1}{3+it}\right).$$

La seule quantité à réellement poser problème, dans la majoration qui nous intéresse, est la somme sur les zéros ρ. L'application des lemmes 2.6 et 2.8 (première et troisième inégalités avec $a = 3$) permet de majorer de la façon suivante :

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) + \frac{\delta_{\chi=1}(\chi)}{s-1} - \sum_{\substack{\rho \\ |\gamma - t| \leqslant 1}} \frac{1}{s-\rho}\right| \leqslant \sum_{\substack{\rho \\ |\gamma - t| > 1}} \left|\frac{1}{s-\rho} - \frac{1}{3+it-\rho}\right| \tag{2.22}$$
$$+ \sum_{\substack{\rho \\ |\gamma - t| \leqslant 1}} \left|\frac{1}{3+it-\rho}\right| \tag{2.23}$$
$$+ \frac{53}{6}\delta_{\chi=1}(\chi) + \left(\ln(|t|+4) + \frac{961}{74}\right)n_E.$$

On a fait disparaître la contribution de $\frac{\ln(\pi)}{2}$ dans la constante en facteur de n_E, puisque comme on le voit en examinant l'identité (2.18), cette constante disparaît en faisant ici la différence des facteurs γ_χ. On a $|3 + it - \rho| > 2$ pour tout zéro ρ non trivial (car $0 < \mathrm{Re}(\rho) < 1$), donc

$$\sum_{\substack{\rho \\ |\gamma - t| \leqslant 1}} \left|\frac{1}{3+it-\rho}\right| \leqslant \frac{1}{2}n_\chi(t),$$

et on utilise alors le lemme 2.9 pour majorer (2.23). À présent, (2.22) se calcule progressivement (on note $s = \sigma + it$ et $\rho = \beta + i\gamma$) :

$$\begin{aligned}\sum_{\substack{\rho \\ |\gamma - t| > 1}} \left| \frac{1}{s-\rho} - \frac{1}{3+it-\rho} \right| &= \sum_{\substack{\rho \\ |\gamma - t| > 1}} \frac{3-\sigma}{|s-\rho||3+it-\rho|} \\ &\leqslant \frac{7}{2} \sum_{k=1}^{\infty} \sum_{\substack{\rho \\ |\gamma-(t+2k)|\leqslant 1}} \frac{1}{|t-\gamma|^2} \\ &+ \frac{7}{2} \sum_{k=1}^{\infty} \sum_{\substack{\rho \\ |\gamma-(t-2k)|\leqslant 1}} \frac{1}{|t-\gamma|^2} \\ &\leqslant \frac{7}{2} \sum_{k=1}^{\infty} \frac{n_\chi(t+2k) + n_\chi(t-2k)}{(2k-1)^2},\end{aligned}$$

et donc, après avoir repris son souffle,

$$\begin{aligned}\sum_{\substack{\rho \\ |\gamma - t| > 1}} \left| \frac{1}{s-\rho} - \frac{1}{3+it-\rho} \right| &\leqslant \frac{35\pi^2}{16} \left(\ln(A(\chi)) + 2n_E \right) \\ &+ \frac{35}{2} \sum_{k=1}^{\infty} \left(\frac{2}{4+(t+2k)^2} + \frac{1}{1+(t+2k)^2} \right) \frac{1}{(2k-1)^2} \delta_{\chi=1}(\chi) \\ &+ \frac{35}{2} \sum_{k=1}^{\infty} \left(\frac{2}{4+(t-2k)^2} + \frac{1}{1+(t-2k)^2} \right) \frac{1}{(2k-1)^2} \delta_{\chi=1}(\chi) \\ &+ \frac{35}{2} \sum_{k=1}^{\infty} \frac{\ln(|t|+2k+3)}{(2k-1)^2} n_E.\end{aligned}$$

Ces sommes se majorent par une comparaison série-intégrale ; on prouve ainsi que les deux premières sommes sont, chacune, inférieures strictement à $\frac{1}{2}$, tandis qu'on majore la dernière somme par $\frac{\ln(|t|+5)}{2}\left(3 + \frac{1}{|t|+4}\right)$. On en déduit le lemme, en regroupant les différentes estimations faites ici. Par commodité, on utilise la majoration $\frac{961}{74} + 2\left(\frac{5}{4} + \frac{35\pi^2}{16}\right) \leqslant \frac{176}{3}$. □

2.3 L'intégrale sur un contour

Maintenant, on se charge d'évaluer $I_C(x,T)$ en passant par l'évaluation de

$$I_\chi(x,T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) \mathrm{d}s \tag{2.24}$$

pour chaque caractère irréductible χ de H. À présent, on a besoin que T soit différent des zéros de toutes les fonctions $\mathrm{L}(\cdot,\chi)$ (cette condition s'éclairera plus tard ; un T qui

ne vérifie pas cette condition sera dit *spécial*). On introduit un nouveau paramètre U, vérifiant $U = j + \frac{1}{2}$ pour un certain entier naturel j (plus tard, on fera tendre U vers $+\infty$), et on définit

$$I_\chi(x,T,U) = \frac{1}{2\pi i}\int_{B_{T,U}} \frac{x^s}{s}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\mathrm{d}s, \tag{2.25}$$

où $B_{T,U}$ est le rectangle (orienté dans le sens trigonométrique) dont les sommets sont $\sigma_0 - iT$, $\sigma_0 + iT$, $-U + iT$ et $-U - iT$. Cette intégrale s'exprime simplement à l'aide des singularités de l'intégrande, mais ceci attendra encore un peu. Dans cette section, on montrera que $R_\chi(x,T,U) = I_\chi(x,T,U) - I_\chi(x,T)$ est petit. On divise $R_\chi(x,T,U)$ en trois intégrales, celle verticale

$$V_\chi(x,T,U) = \frac{1}{2\pi}\int_T^{-T} \frac{x^{-U+it}}{-U+it}\frac{\mathrm{L}'}{\mathrm{L}}(-U+it,\chi)\mathrm{d}t, \tag{2.26}$$

et les deux intégrales horizontales

$$H_\chi(x,T,U) = \frac{1}{2\pi i}\int_{-U}^{-1/4}\left(\frac{x^{\sigma-iT}}{\sigma-iT}\frac{\mathrm{L}'}{\mathrm{L}}(\sigma-iT,\chi) - \frac{x^{\sigma+iT}}{\sigma+iT}\frac{\mathrm{L}'}{\mathrm{L}}(\sigma+iT,\chi)\right)\mathrm{d}\sigma \tag{2.27}$$

et

$$H^*_\chi(x,T) = \frac{1}{2\pi i}\int_{-1/4}^{\sigma_0}\left(\frac{x^{\sigma-iT}}{\sigma-iT}\frac{\mathrm{L}'}{\mathrm{L}}(\sigma-iT,\chi) - \frac{x^{\sigma+iT}}{\sigma+iT}\frac{\mathrm{L}'}{\mathrm{L}}(\sigma+iT,\chi)\right)\mathrm{d}\sigma$$

Pour borner $\frac{\mathrm{L}'}{\mathrm{L}}$, et donc estimer ces intégrales, on a besoin du lemme 2.7, qui renseigne sur la taille de $\frac{\Gamma'}{\Gamma}$.

On en déduit :

Lemme 2.13. *Si $s = \sigma + it$ avec $\sigma \leqslant -\frac{1}{4}$ et $|s+m| \geqslant \frac{1}{4}$ pour tout entier naturel m, alors*

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leqslant \ln(A(\chi)) + n_E\left(\ln(|s|+2) + \frac{19683}{812}\right).$$

Démonstration. Partant de l'équation fonctionnelle vérifiée par $\mathrm{L}(\cdot,\chi)$, on a

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = -\frac{\mathrm{L}'}{\mathrm{L}}(1-s,\bar\chi) - \ln(A(\chi)) - \frac{\gamma'_\chi}{\gamma_\chi}(1-s) - \frac{\gamma'_\chi}{\gamma_\chi}(s),$$

et $\mathrm{Re}(1-s) \geqslant \frac{5}{4}$, ce qui permet d'utiliser le lemme 2.6 pour borner $\frac{\mathrm{L}'}{\mathrm{L}}(1-s,\bar\chi)$. En utilisant la quatrième inégalité du lemme 2.8 pour estimer $\frac{\gamma'_\chi}{\gamma_\chi}(s)$, on a :

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leqslant \ln(A(\chi)) - \frac{n_E}{\sigma} + n_E\left(\ln(|s|+2) + \frac{16435}{812}\right),$$

d'où le résultat. □

Reprenons : les intégrales verticale (2.26) et horizontale (2.27) sont estimées à l'aide de l'inégalité ci-dessus. On a, pour $x \geqslant 2$, $T \geqslant 1$ et $U \geqslant \frac{1}{2}$,

$$\begin{aligned}|V_\chi(x,T,U)| &\leqslant \frac{x^{-U}}{2\pi U}\int_{-T}^{T}\left|\frac{\mathrm{L}'}{\mathrm{L}}(-U+it,\chi)\right|\mathrm{d}t\\ &\leqslant \frac{x^{-U}T}{\pi U}\left(\ln(A(\chi))+n_E\left(\ln(U+T+2)+\frac{19683}{812}\right)\right),\end{aligned}\tag{2.28}$$

et, sous ces mêmes conditions,

$$\begin{aligned}|H_\chi(x,T,U)| &\leqslant \frac{1}{\pi T}\int_{-\infty}^{-\frac{1}{4}} x^\sigma\left(\ln(A(\chi))+n_E\left(\ln(|\sigma|+T+2)+\frac{19683}{812}\right)\right)\mathrm{d}\sigma\\ &\leqslant \frac{x^{-1/4}}{\pi T\ln(x)}\left[\ln(A(\chi))+n_E\left(\ln\left(T+\frac{9}{4}\right)+\frac{19683}{812}\right)\right]\\ &\quad+\frac{n_E x^{-1/4}}{\pi T(\ln(x))^2}\frac{1}{\left(T+\frac{9}{4}\right)},\end{aligned}\tag{2.29}$$

Estimer l'intégrale $H^*_\chi(x,T)$ est un peu plus ardu, et nécessite le lemme 2.12. Il nous indique que

$$\begin{aligned}\left|\frac{\mathrm{L}'}{\mathrm{L}}(\sigma+iT,\chi)-\sum_{\substack{\rho\\|\gamma-T|\leqslant 1}}\frac{1}{\sigma+iT-\rho}\right| &\leqslant \frac{571}{25}\ln(A(\chi))+\frac{671}{24}\delta_{\chi=1}(\chi)\\ &\quad+n_E\left(\frac{57}{2}\ln(T+5)+\frac{2252}{35}\right)\end{aligned}$$

pour σ dans $\left[-\frac{1}{4},\sigma_0\right]$, $x \geqslant 2$ et $T \geqslant 2$. On a la même estimation en $\sigma - iT$. Alors,

$$\begin{aligned}&\left|H^*_\chi(x,T)-\frac{1}{2\pi i}\int_{-1/4}^{\sigma_0}\left(\frac{x^{\sigma-iT}}{\sigma-iT}\sum_{\substack{\rho\\|\gamma+T|\leqslant 1}}\frac{1}{\sigma-iT-\rho}-\frac{x^{\sigma+iT}}{\sigma+iT}\sum_{\substack{\rho\\|\gamma-T|\leqslant 1}}\frac{1}{\sigma+iT-\rho}\right)\mathrm{d}\sigma\right|\\ &\quad\leqslant\frac{ex-x^{-1/4}}{\pi T\ln(x)}\left[\frac{571}{25}\ln(A(\chi))+\frac{671}{24}\delta_{\chi=1}(\chi)+n_E\left(\frac{57}{2}\ln(T+5)+\frac{2252}{35}\right)\right].\end{aligned}$$

Pour en finir avec l'estimation de $H^*_\chi(x,T)$, on doit encore vérifier que l'intégrale ci-dessus reste assez « petite ».

Lemme 2.14. *Soit $\rho = \beta + i\gamma$, avec $0 < \beta < 1$ et $\gamma \neq t$. Si $|t| \geqslant 2$, $x \geqslant 2$ et $1 < \sigma_1 \leqslant 3$, alors :*

$$\left|\int_{-1/4}^{\sigma_1}\frac{x^{\sigma+it}}{(\sigma+it)(\sigma+it-\rho)}\mathrm{d}\sigma\right| \leqslant \left(\sigma_1+\frac{9}{4}\right)\frac{x^{\sigma_1}}{(|t|-1)(\sigma_1-\beta)}.$$

Démonstration. Supposons d'abord que $\gamma > t$. Soit B le rectangle (orienté dans le sens trigonométrique) dont les sommets ont pour affixes $\sigma_1 + i(t-1)$, $\sigma_1 + it$, $-\frac{1}{4} + it$ et $-\frac{1}{4} + i(t-1)$. Le théorème de Cauchy assure que

$$\int_B \frac{x^s}{s(s-\rho)} \mathrm{d}s = 0,$$

puisque l'intégrande n'a pas de singularité à l'intérieur du rectangle. En outre, sur les arêtes du rectangle, à l'exception de celle joignant $-\frac{1}{4} + it$ et $\sigma_1 + it$, on peut le majorer par $\frac{x^{\sigma_1}}{(|t|-1)(\sigma_1-\beta)}$. D'où le résultat pour $\gamma > t$. On procède de même si $\gamma < t$, en changeant $i(t-1)$ en $i(t+1)$ dans les affixes des sommets du rectangle. □

Ceci prouve que

$$\left| \frac{1}{2\pi i} \int_{-1/4}^{\sigma_0} \frac{x^{\sigma - iT}}{\sigma - iT} \left(\sum_{\substack{\rho \\ |\gamma+T| \leqslant 1}} \frac{1}{\sigma - iT - \rho} \right) \mathrm{d}\sigma \right| \leqslant \frac{\sigma_0 + \frac{9}{4}}{2\pi} n_\chi(-T) \frac{x^{\sigma_0}}{(T-1)(\sigma_0 - 1)},$$

puis, grâce au lemme 2.9,

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{-1/4}^{\sigma_0} \frac{x^{\sigma - iT}}{\sigma - iT} \left(\sum_{\substack{\rho \\ |\gamma+T| \leqslant 1}} \frac{1}{\sigma - iT - \rho} \right) \mathrm{d}\sigma \right| &\leqslant \frac{5\,(13\ln(x) + 4)\,ex}{16\pi(T-1)} \\ &\times \left[\ln(A(\chi)) + \frac{9}{10}\delta_{\chi=1}(\chi) + n_E \left(\ln\left(\frac{T+3}{2\pi} \right) + 2 \right) \right] \end{aligned}$$

pour $x \geqslant 2$ et $T \geqslant 2$. On a le même résultat pour les zéros indicés grâce à la condition $|\gamma - T| \leqslant 1$. Si on suppose HRG, le terme en $\ln(x)$ disparaît, d'après [LO77], page 445. On ne s'en chargera pas ici.
En fin de compte, on obtient

$$\begin{aligned} |H_\chi^*(x,T)| \leqslant & \left(\frac{5\,(13\ln(x) + 4)\,ex}{8(T-1)} + \frac{571}{25} \frac{ex - x^{-1/4}}{T\ln(x)} \right) \frac{\ln(A(\chi))}{\pi} \\ & + \left(\frac{9}{10} \frac{5\,(13\ln(x) + 4)\,ex}{8(T-1)} + \frac{671}{24} \frac{ex - x^{-1/4}}{T\ln(x)} \right) \frac{\delta_{\chi=1}(\chi)}{\pi} \\ & + \Bigg[\left(\frac{5\,(13\ln(x) + 4)\,ex}{8(T-1)} + \frac{57}{2} \frac{ex - x^{-1/4}}{T\ln(x)} \right) \ln(T+5) \\ & + \frac{5\,(13\ln(x) + 4)\,ex}{4(T-1)} + \frac{2252}{35} \frac{ex - x^{-1/4}}{T\ln(x)} \Bigg] \frac{n_E}{\pi} \end{aligned} \tag{2.30}$$

En combinant (2.28), (2.29) et (2.30), on obtient le résultat principal de la section, à savoir,

$$\begin{aligned}|I_\chi(x,T)-I_\chi(x,T,U)| \leqslant{}& \frac{65e}{8\pi}\frac{x\ln(x)}{T-1}\left[\ln(A(\chi))+\frac{9}{10}\delta_{\chi=1}(\chi)+n_E\left(\ln(T+5)+2\right)\right]\\ &+\frac{5e}{2\pi}\frac{x}{T-1}\left[\ln(A(\chi))+\frac{9}{10}\delta_{\chi=1}(\chi)+n_E\left(\ln(T+5)+2\right)\right]\\ &+\frac{e}{\pi}\frac{x}{T\ln(x)}\Big[\frac{571}{25}\ln(A(\chi))+\frac{671}{24}\delta_{\chi=1}(\chi)\\ &+n_E\left(\frac{57}{2}\ln(T+5)+\frac{2252}{35}\right)\Big]\\ &+\frac{x^{-U}T}{\pi U}\left[\ln(A(\chi))+n_E\left(\ln(U+T+2)+\frac{19683}{812}\right)\right]\\ &+\frac{4n_Ex^{-1/4}}{17\pi T(\ln(x))^2}. \end{aligned} \tag{2.31}$$

On a fait le choix de ne pas retenir la contribution négative en $\frac{x^{-1/4}}{\ln(x)}$, qui affecte très peu la suite des calculs.

2.4 La formule explicite

On en arrive enfin à une formule explicite pour ψ_C en fonction des zéros ρ. On revient à la définition de $I_\chi(x,T,U)$ donnée en (2.25), où on rappelle que $x \geqslant 2$ et $U = j+\frac{1}{2}$ pour un certain entier naturel j. Soit $T \geqslant 2$ non spécial. Par le théorème de Cauchy, $I_\chi(x,T,U)$ égale la somme des résidus de l'intégrande aux pôles à l'intérieur de $B_{T,U}$. Pour un décompte détaillé des résidus, on renvoie à [LO77], pages 446–448 : on a en tout cas

$$\begin{aligned}I_\chi(x,T,U) = -\delta_{\chi=1}(\chi)x+\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}-b(\chi)\sum_{1\leqslant m\leqslant\frac{U+1}{2}}\frac{x^{1-2m}}{2m-1}-a(\chi)\sum_{1\leqslant m\leqslant\frac{U}{2}}\frac{x^{-2m}}{2m}\\ +r(\chi)+(a(\chi)-\delta_{\chi=1}(\chi))\ln(x),\end{aligned} \tag{2.32}$$

où :

$$r(\chi) = B(\chi)-\frac{1}{2}\ln(A(\chi))+\frac{n_E}{2}\ln(\pi)+\delta_{\chi=1}(\chi)-\frac{b(\chi)}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right)-\frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}(1).$$

Quand $U \to +\infty$, (2.31) et (2.32) donnent la formule explicite suivante, valide pour tout $x \geqslant 2$ et tout $T \geqslant 2$ non spécial.

$$\begin{aligned}\Big| I_\chi(x,T) + \delta_{\chi=1}(\chi)x - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - r(\chi) - (a(\chi) - \delta_{\chi=1}(\chi))\ln(x) \\ - \frac{n_E}{2}\ln\left(1-\frac{1}{x}\right) + \frac{1}{2}(b(\chi)-a(\chi))\ln\left(1+\frac{1}{x}\right)\Big| \\ \leqslant \frac{65e}{8\pi}\frac{x\ln(x)}{T-1}\left[\ln(A(\chi)) + \frac{9}{10}\delta_{\chi=1}(\chi) + n_E\left(\ln(T+5)+2\right)\right] \\ + \frac{5e}{2\pi}\frac{x}{T-1}\left[\ln(A(\chi)) + \frac{9}{10}\delta_{\chi=1}(\chi) + n_E\left(\ln(T+5)+2\right)\right] \\ + \frac{e}{\pi}\frac{x}{T\ln(x)}\Big[\frac{571}{25}\ln(A(\chi)) + \frac{671}{24}\delta_{\chi=1}(\chi) \\ + n_E\left(\frac{57}{2}\ln(T+5) + \frac{2252}{35}\right)\Big] + \frac{4n_E x^{-1/4}}{17\pi T(\ln(x))^2}.\end{aligned}$$

On a alors presque ce qu'on veut :

Théorème 2.15. *Si $x \geqslant 2$ et $T \geqslant 2$, alors*

$$\begin{aligned}\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \frac{|C|}{|G|}\Big(\frac{49}{6}n_L\frac{x(\ln(x))^2}{T} \\ + \frac{65e}{8\pi}\frac{x\ln(x)}{T-1}\left[\ln(d_L) + \frac{9}{10} + n_L\left(\ln(T+5)+2\right)\right] \\ + \frac{5}{2}\left(\frac{e}{\pi}+1\right)\frac{x}{T-1}\left[\ln(d_L) + \frac{9}{10} + n_L\left(\ln(T+5)+2\right)\right] \\ + \frac{e}{\pi}\frac{x}{T\ln(x)}\left[\frac{571}{25}\ln(d_L) + \frac{671}{24} + n_L\left(\frac{57}{2}\ln(T+5) + \frac{2252}{35}\right)\right] \\ + \ln(x)\left[\frac{79986}{3773}n_L + \frac{2}{\ln(2)} + 1\right] + \frac{431}{16} + \frac{94}{7}\ln(d_L) + \frac{350}{11}n_L \\ + \frac{4n_L x^{-1/4}}{17\pi T(\ln(x))^2}\Big),\end{aligned}$$

où

$$S(x,T) = \frac{|C|}{|G|}\sum_\chi \bar{\chi}(g)\left(\sum_{\substack{\rho \\ |\gamma|<T}}\frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<\frac{1}{2}}}\frac{1}{\rho}\right), \tag{2.33}$$

les deux dernières sommes étant sur les zéros non triviaux de $\mathrm{L}(\cdot,\chi)$.

Démonstration. D'après le lemme 2.11, on a

$$\left|r(\chi)+\sum_{|\rho|<\frac{1}{2}}\frac{1}{\rho}\right|\leqslant\left(\frac{5\pi^2}{8}+\frac{29}{4}\right)\ln(A(\chi))+\frac{431}{16}\delta_{\chi=1}(\chi)+\left(\frac{2971}{100}+\frac{\ln(\pi)}{2}+\frac{\gamma_0}{2}+\ln(2)\right)n_E,$$

donc

$$\begin{aligned}\left|I_\chi(x,T)+\delta_{\chi=1}(\chi)x-\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}-\sum_{|\rho|<\frac{1}{2}}\frac{1}{\rho}\right|&\\ \leqslant\frac{65e}{8\pi}\frac{x\ln(x)}{T-1}\left[\ln(A(\chi))+\frac{9}{10}\delta_{\chi=1}(\chi)+n_E\left(\ln(T+5)+2\right)\right]&\\ +\frac{5e}{2\pi}\frac{x}{T-1}\left[\ln(A(\chi))+\frac{9}{10}\delta_{\chi=1}(\chi)+n_E\left(\ln(T+5)+2\right)\right]&\\ +\frac{e}{\pi}\frac{x}{T\ln(x)}\Big[\frac{571}{25}\ln(A(\chi))+\frac{671}{24}\delta_{\chi=1}(\chi)&\\ +n_E\left(\frac{57}{2}\ln(T+5)+\frac{2252}{35}\right)\Big]+n_E\ln(x)+\left(\ln(x)+\frac{431}{16}\right)\delta_{\chi=1}(\chi)&\\ +\frac{94}{7}\ln(A(\chi))+\frac{350}{11}n_E+\frac{4n_Ex^{-1/4}}{17\pi T(\ln(x))^2}.&\end{aligned}$$

Alors, (2.12) et (2.24) donnent, pour T non spécial, la même majoration (à une multiplication par $\frac{|C|}{|G|}$ près) pour

$$\left|I_C(x,T)-\frac{|C|}{|G|}\sum_\chi\bar{\chi}(g)\left(\delta_{\chi=1}(\chi)x-\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}+\sum_{|\rho|<\frac{1}{2}}\frac{1}{\rho}\right)\right|$$

en remplaçant $\delta_{\chi=1}(\chi)$ par 1, $\ln(A(\chi))$ par $\ln(d_L)$ et n_E par n_L, en vertu des formules

$$\sum_\chi\ln(A(\chi))=\ln(d_L)\text{ (formule du discriminant) et }n_E\cdot[L:E]=n_L.$$

Comme $\psi_C(x,T)=I_C(x,T)+R_1(x,T)$,

$$\begin{aligned}\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \frac{|C|}{|G|}\Big(&\frac{49}{6}n_L\frac{x(\ln(x))^2}{T}\\ &+ \frac{65e}{8\pi}\frac{x\ln(x)}{T-1}\left[\ln(d_L) + \frac{9}{10} + n_L\left(\ln(T+5)+2\right)\right]\\ &+ \frac{5e}{2\pi}\frac{x}{T-1}\left[\ln(d_L) + \frac{9}{10} + n_L\left(\ln(T+5)+2\right)\right]\\ &+ \frac{e}{\pi}\frac{x}{T\ln(x)}\left[\frac{571}{25}\ln(d_L) + \frac{671}{24} + n_L\left(\frac{57}{2}\ln(T+5) + \frac{2252}{35}\right)\right]\\ &+ \ln(x)\left[\frac{2}{\ln(2)} + \frac{79986}{3773}n_L + 1\right] + \frac{431}{16} + \frac{94}{7}\ln(d_L) + \frac{350}{11}n_L\\ &+ \frac{4n_Lx^{-1/4}}{17\pi T(\ln(x))^2}\Big),\end{aligned}$$

ce qui donne le théorème si T n'est pas spécial. Maintenant, si $T = \mathrm{Im}(\rho_T)$ pour un certain zéro ρ_T (ou plusieurs ; il y en a au plus $\sum_\chi n_\chi(T)$), on a, pour ε assez proche de 0,

$$S(x, T+\varepsilon) = S(x,T) + \frac{|C|}{|G|}\sum_\chi \bar\chi(g) \sum_{\substack{\rho_T \\ T=\mathrm{Im}(\rho_T)}} \frac{x^{\rho_T}}{\rho_T}$$

et $T+\varepsilon$ n'est pas spécial. Alors,

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T+\varepsilon)\right| + \frac{|C|}{|G|}\sum_\chi n_\chi(T)\frac{x}{T}$$

On sait estimer la dernière somme grâce au lemme 2.9 et la formule du discriminant, tandis que la première quantité du membre de droite s'évalue à l'aide des calculs qui précèdent. On obtient la majoration du théorème en faisant tendre ε vers 0. □

C'est le résultat principal du chapitre : on a exprimé $\psi_C(x)$ en fonction d'un terme principal $\frac{|C|}{|G|}x$, de $S(x,T)$ et un terme d'erreur relativement petit. Il reste à estimer $S(x,T)$. Si on suppose HRG, on peut avoir une bonne borne à partir des résultats déjà établis ; si on veut un résultat inconditionnel, on doit montrer que les zéros ρ ne s'approchent pas trop de la droite $\mathrm{Re}(s) = 1$.

2.5 Les régions sans zéros

Cette section concerne les zéros exceptionnels que les fonctions ζ_L peuvent éventuellement avoir. Pour rappel, comme $\zeta_L = \prod_\chi \mathrm{L}(\cdot,\chi)$, un zéro pour ζ_L en entraîne un

pour au moins une des fonctions $\mathrm{L}(\cdot,\chi)$; dans le cas du lemme 2.17 à venir, il n'y a en vérité qu'une seule fonction $\mathrm{L}(\cdot,\chi)$ éventuellement concernée. Seul un résultat nécessite d'être explicité, c'est le lemme 8.1 de [LO77], que voici :

Lemme 2.16. *La fonction ζ_L n'a pas de zéros $\rho = \beta + i\gamma$ dans la région délimitée par les conditions*

$$|\gamma| \geqslant \frac{1}{1 + 4\ln(d_L)}$$

et

$$\beta \geqslant 1 - \left(12 - \sqrt{\frac{179}{2}}\right)^2 \left(\frac{2719}{3}\ln(d_L) + n_L\left(\frac{469}{4}\ln\left(\frac{3+|\gamma|}{2\pi}\right) + \frac{64}{29}\right) + \frac{3307}{12}\right)^{-1}.$$

Démonstration. Pour obtenir ce genre de région sans zéros, la méthode est classique, et on peut en trouver un exposé systématique dans [Lan53], §65 : on a vu en (2.6) et (2.7) que pour $\sigma = \mathrm{Re}(s) > 1$,

$$-\frac{\zeta_L'}{\zeta_L}(s) = \sum_{m=1}^{\infty} \Lambda_L(m) m^{-s},$$

où $\Lambda_L(m) \geqslant 0$ pour tout entier naturel non nul m. Par conséquent, s'il existe des réels positifs a_i tels que $a_0 < a_1$ et :

$$\forall \theta \in \mathbb{R}, \quad a_0 + a_1\cos(\theta) + \cdots + a_N\cos(N\theta) \geqslant 0,$$

alors on sait que

$$\mathrm{Re}\left(-\sum_{k=0}^{N} a_k \frac{\zeta_L'}{\zeta_L}(\sigma + kit)\right) = \sum_{m=1}^{\infty} \Lambda_L(m) m^{-\sigma} \sum_{k=0}^{N} a_k \cos(kt\ln(m)) \geqslant 0. \tag{2.34}$$

Notons que pour cela, il faut au moins $N \geqslant 2$. Or, si on prend pour χ le caractère trivial, l'égalité (2.15) montre que

$$2\frac{\zeta_L'}{\zeta_L}(s) = \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}}\right) - \ln(d_L) - 2\left(\frac{1}{s} + \frac{1}{s-1}\right) - 2\frac{\gamma_L'}{\gamma_L}(s),$$

où la somme est indicée par les zéros ρ de ζ_L. Si $\mathrm{Re}(s) > 1$, alors $\mathrm{Re}\left(\frac{1}{s-\rho}\right) > 0$ pour tout ρ. À présent, considérons $\beta + i\gamma$ un zéro tel que $|\gamma| \geqslant \frac{1}{1+4\ln(d_L)}$. Alors, pour $2 \geqslant \sigma > 1$, d'après le lemme 2.8,

$$\begin{aligned} -\frac{\zeta_L'}{\zeta_L}(\sigma) &\leqslant \frac{1}{\sigma-1} + \frac{1}{\sigma} + \frac{1}{2}\ln(d_L) + \frac{\gamma_L'}{\gamma_L}(\sigma), \\ &\leqslant \frac{1}{\sigma-1} + 1 + \frac{1}{2}\ln(d_L) + \frac{n_L}{2}\ln\left(\frac{3}{2\pi}\right). \end{aligned}$$

De même, si k est un entier naturel différent de 0 et 1,

$$-\mathrm{Re}\left(\frac{\zeta_L'}{\zeta_L}(\sigma+ki\gamma)\right) \leqslant \frac{1}{2}\ln(d_L) + \mathrm{Re}\left(\frac{1}{\sigma+ki\gamma-1}+\frac{1}{\sigma+ki\gamma}\right) + \mathrm{Re}\left(\frac{\gamma_L'}{\gamma_L}(\sigma+ki\gamma)\right)$$
$$\leqslant \ln(d_L)\left(\frac{1}{2}+\frac{4}{k}\right)+\frac{1}{k}+\frac{n_L}{2}\ln\left(\frac{3+k|\gamma|}{2\pi}\right),$$

et, en conservant la contribution du zéro $\rho=\beta+i\gamma$,

$$-\mathrm{Re}\left(\frac{\zeta_L'}{\zeta_L}(\sigma+i\gamma)\right) \leqslant \frac{9}{2}\ln(d_L)+1+\frac{n_L}{2}\ln\left(\frac{3+|\gamma|}{2\pi}\right)-\frac{1}{\sigma-\beta}.$$

Ces inégalités et (2.34) impliquent que pour tout $\sigma>1$,

$$\frac{a_1}{\sigma-\beta} \leqslant \frac{a_0}{\sigma-1}+\ln(d_L)\left(\frac{a_0}{2}+\sum_{k=1}^{N}a_k\left(\frac{1}{2}+\frac{4}{k}\right)\right)+\frac{n_L}{2}\sum_{k=0}^{N}a_k\ln\left(\frac{3+k|\gamma|}{2\pi}\right)+a_0+\sum_{k=1}^{N}\frac{a_k}{k}.$$

Notant $A(a_0,\dots,a_N,\gamma,d_L)$ le membre de droite moins $\frac{a_0}{\sigma-1}$, il suffit alors de prendre

$$\sigma = 1+\sqrt{a_0}(\sqrt{a_1}-\sqrt{a_0})A(a_0,\dots,a_N,\gamma,d_L)^{-1} > 1$$

pour obtenir une condition sur β, plus précisément

$$\beta \leqslant 1-(\sqrt{a_1}-\sqrt{a_0})^2A(a_0,\dots,a_N,\gamma,d_L)^{-1}.$$

Le résultat du lemme s'obtient en prenant pour inégalité trigonométrique

$$\forall\theta\in\mathbb{R},\quad \frac{179}{2}+144\cos(\theta)+72\cos(2\theta)+18\cos(3\theta)+\frac{1}{2}\cos(6\theta)\geqslant 0.$$

En effet, le membre de gauche peut s'écrire $(1+\cos(\theta))(1+2\cos(\theta))^2(8+(3-2\cos(\theta)))^2$ (voir [Lan53], §65). Par commodité, on utilise la majoration

$$\frac{1}{2}\left(\frac{179}{2}\ln\left(\frac{3}{2\pi}\right)+72\ln(2)+18\ln(3)+\frac{1}{2}\ln(6)\right)<\frac{64}{29}.$$

□

Lemme 2.17 ([LO77], pages 455–456)**.** *Si $n_L>1$, alors ζ_L a au plus un zéro $\rho=\beta+i\gamma$ dans la région délimitée par les conditions*

$$|\gamma| \leqslant \frac{1}{4\ln(d_L)} \text{ et } \beta \geqslant 1-\frac{1}{4\ln(d_L)}.$$

Ce zéro, s'il existe, est réel et simple, et annule $\mathrm{L}(\cdot,\chi_0)$ pour un unique caractère (réel) χ_0. Par ailleurs, si $n_L=1$, alors ζ_L n'admet pas de zéro tel que $|\gamma|<14$.

Remarque 2.18. Ces deux résultats sont démontrés avec de meilleures constantes *pour d_L assez grand* dans [Kad12]. Dans un souci d'effectivisation, on donne des bornes valables pour tout d_L.

2.6 Estimations finales

Théorème 2.19. *Si ζ_L vérifie HRG, alors*

$$\left|\psi_C(x)-\frac{|C|}{|G|}x\right|\leqslant\frac{|C|}{|G|}\sqrt{x}\ln(x)\Big[\left(\frac{55}{48}+\frac{1815}{37\ln(x)}\right)\ln(d_L)+\left(\frac{161}{342}\ln(x)+\frac{605}{54}+\frac{148890}{653\ln(x)}\right)n_L+\frac{5920}{59}\Big]$$

pour tout $x\geqslant 2$.

Remarque 2.20. Plus précisément, on a, pour tout $x\geqslant 2$,

$$\begin{aligned}\left|\psi_C(x)-\frac{|C|}{|G|}x\right|\leqslant\frac{|C|}{|G|}\sqrt{x}\Big[&\left(\frac{55}{48}\ln(x)+\frac{64}{5}+\frac{32}{7\ln(x)}+\frac{155}{16(\ln(x))^2}+\frac{94}{7\sqrt{x}}\right)\ln(d_L)\\&+\Big(\frac{161}{342}(\ln(x))^2+\frac{605}{54}\ln(x)+\frac{212}{5}+\frac{86}{3\ln(x)}\\&+\frac{38949}{763(\ln(x))^2}+\frac{79986}{3773}\frac{\ln(x)}{\sqrt{x}}+\frac{350}{11\sqrt{x}}+\frac{25}{681x^{5/4}(\ln(x))^3}\Big)n_L\\&+\frac{2639}{155}+\frac{144}{35\ln(x)}+\frac{83}{7(\ln(x))^2}+\frac{35\ln(x)}{9\sqrt{x}}+\frac{431}{16\sqrt{x}}\Big],\end{aligned}$$

et de cette écriture, on voit que les termes d'erreur peuvent être améliorés pour une grande valeur de x. Par exemple, pour $x\geqslant 100$, on peut remplacer $\frac{148890}{653}\simeq 228$ par $\frac{2431}{38}\simeq 64$.

Démonstration. Si ζ_L vérifie HRG, alors toutes les fonctions $\mathrm{L}(\cdot,\chi)$ associées à ζ_L par la formule $\zeta_L=\prod_\chi \mathrm{L}(\cdot,\chi)$ la vérifient également, parce que ces fonctions L sont holomorphes dans la bande critique (c'est un des gains primordiaux acquis en se ramenant au cas des fonctions L de Hecke). Ainsi, pour chaque χ il n'existe pas de zéro ρ non trivial tel que $|\rho|<\frac{1}{2}$, et par le lemme 2.9 :

$$\begin{aligned}\left|\sum_{\substack{\rho\\|\gamma|<T}}\frac{x^\rho}{\rho}-\sum_{|\rho|<\frac{1}{2}}\frac{1}{\rho}\right|&\leqslant\sqrt{x}\left(2n_\chi(0)+\sum_{0\leqslant j\leqslant\frac{T-1}{2}}\frac{n_\chi(2j+2)+n_\chi(-(2j+2))}{2j+1}\right)\\&\leqslant\frac{5}{2}\sqrt{x}\Big[\left(2+\frac{\ln(T)}{2}\right)(\ln(A(\chi))+(2-\ln(2\pi))n_E)\\&\quad+2\delta_{\chi=1}(\chi)\left(\frac{3}{2}+\frac{9}{20}+\left(\frac{3}{10}\ln(2)-\frac{3\pi}{20}+\frac{\ln(5)}{8}+\frac{\arctan(2)}{4}\right)\right)\\&\quad+\left(\frac{27}{7}+\frac{\ln(T+4)\ln(T)}{4}\right)n_E\Big],\end{aligned}$$

car

$$\begin{aligned}\int_1^{\frac{T-1}{2}} \frac{\ln(2t+5)}{2t+1}\mathrm{d}t &= \frac{1}{2}\int_1^{\frac{T-1}{2}} \left(\frac{\ln(2t+5)}{2t+1} + \frac{\ln(2t+1)}{2t+5}\right)\mathrm{d}t \\ &\quad + \frac{1}{2}\int_1^{\frac{T-1}{2}} \left(\frac{\ln(2t+5)}{2t+1} - \frac{\ln(2t+1)}{2t+5}\right)\mathrm{d}t \\ &= \frac{\ln(T)\ln(T+4) - \ln(3)\ln(7)}{4} + \frac{1}{2}\int_1^{\frac{T-1}{2}} \frac{\ln\left(1+\frac{4}{2t+1}\right)}{2t+1}\mathrm{d}t \\ &\quad + 2\int_1^{\frac{T-1}{2}} \frac{\ln(2t+1)}{(2t+1)(2t+5)}\mathrm{d}t \\ &\leqslant \frac{\ln(T)\ln(T+4) - \ln(3)\ln(7)}{4} + 2\int_1^{\frac{T-1}{2}} \frac{(1+\ln(2t+1))\mathrm{d}t}{(2t+1)^2} \\ &\leqslant \frac{\ln(T)\ln(T+4) - \ln(3)\ln(7)}{4} + \frac{2+\ln(3)}{3}.\end{aligned}$$

En se rappelant la définition de $S(x,T)$ donnée dans le théorème 2.15, ceci implique que pour tout $T \geqslant 2$,

$$\begin{aligned}|S(x,T)| &\leqslant \frac{5|C|}{2|G|}\sqrt{x}\Big[\frac{\ln(T+4)\ln(T)}{4}n_L + \ln(T)\left(\frac{\ln(d_L)}{2} + n_L\left(1 - \frac{\ln(2\pi)}{2}\right)\right) \\ &\quad + 2\ln(d_L) + \left(\frac{27}{7} + 2(2-\ln(2\pi))\right)n_L + \frac{368}{85}\Big] \\ &\leqslant \frac{5|C|}{2|G|}\sqrt{x}\Big[\frac{(\ln(T))^2}{4}n_L + \ln(T)\left(\frac{\ln(d_L)}{2} + \frac{5}{14}n_L\right) + 2\ln(d_L) + \frac{46}{11}n_L + \frac{368}{85}\Big].\end{aligned}$$

On pose $T = \frac{\sqrt{2}}{\ln(2)}\sqrt{x}\ln(x)$, par exemple (on a $T \geqslant 2$ pour $x \geqslant 2$), et la formule explicite du théorème 2.15 donne l'inégalité de la remarque 2.20, puis le résultat désiré (on majore $\ln(\sqrt{x}\ln(x))$ par $\left(\frac{1}{2}+\frac{1}{e}\right)\ln(x)$). □

Remarque 2.21. D'autres choix de T donnent d'autres termes d'erreur. Par exemple, $T = x$ donne, pour tout $x \geqslant 2$,

$$\begin{aligned}\left|\psi_C(x) - \frac{|C|}{|G|}x\right| &\leqslant \frac{|C|}{|G|}\Big[\left(\frac{5}{4}\sqrt{x}\ln(x) + 5\sqrt{x} + \frac{464}{33}\ln(x) + \frac{1115}{49} + \frac{336}{17\ln(x)}\right)\ln(d_L) \\ &\quad + \Big(\frac{5}{8}\sqrt{x}(\ln(x))^2 + \frac{25}{28}\sqrt{x}\ln(x) + \frac{115}{11}\sqrt{x} + \frac{2009}{103}(\ln(x))^2 + \frac{1449}{19}\ln(x) \\ &\quad + \frac{955}{11} + \frac{606}{7\ln(x)} + \frac{3}{40x^{5/4}(\ln(x))^2}\Big)n_L \\ &\quad + \frac{184}{17}\sqrt{x} + \frac{182}{11}\ln(x) + \frac{5441}{154} + \frac{1645}{68\ln(x)}\Big].\end{aligned}$$

Le choix fait dans la démonstration du théorème revient à minimiser à la fois le terme croissant (en T) dominant $\sqrt{x}(\ln(T))^2$ et le terme décroissant dominant $\frac{\ln(T)}{T}x(\ln(x))^2$.

Théorème 2.22. *Soit β_0 le zéro réel éventuel de ζ_L vérifiant $\beta_0 \geqslant 1 - \frac{1}{4\ln(d_L)}$, et χ_0 le caractère (réel) tel que $\mathrm{L}(\beta_0, \chi_0) = 0$. Si $x \geqslant \exp\left(\frac{219961}{4} n_L (\ln(9d_L^8))^2\right)$, alors*

$$\psi_C(x) = \frac{|C|}{|G|}x - \frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\beta_0} + \frac{|C|}{|G|}R(x),$$

où $|R(x)| \leqslant 3448193801529x \exp\left(-\frac{1}{8}\sqrt{\frac{\ln(x)}{n_L}}\right)$. Le second terme peut être supprimé en l'absence du zéro exceptionnel β_0.

Démonstration. Pour alléger les calculs, posons $a = \exp\left(\frac{3307}{10876}\right)$, $b = \exp\left(\frac{64}{29}\right)$, $N_1 = \frac{2719}{3}$, $N_2 = \frac{469}{4}$ et $c = \left(12 - \sqrt{\frac{179}{2}}\right)^2$. Si $\rho = \beta + i\gamma$ avec $\rho \neq \beta_0$ est un zéro non trivial d'une fonction L tel que $|\gamma| < T$, alors la borne inconditionnelle du lemme 2.16 montre que

$$|x^\rho| = x^\beta \leqslant x \exp\left(-\frac{c\ln(x)}{\ln\left((ad_L)^{N_1}\left(b\left(\frac{T+3}{2\pi}\right)^{N_2}\right)^{n_L}\right)}\right)$$

pour $x \geqslant 2$ et $T \geqslant 2$. De plus, le lemme 2.9 montre, en imitant le raisonnement de la démonstration du théorème 2.19, que

$$\sum_{\chi}\sum_{\substack{|\rho|\geqslant\frac{1}{2}\\ |\gamma|\leqslant T}}\left|\frac{1}{\rho}\right| \leqslant \frac{5}{2}\left[\frac{(\ln(T))^2}{4}n_L + \ln(T)\left(\frac{\ln(d_L)}{2} - \frac{9}{16}n_L\right) + 2\ln(d_L) + \frac{48}{7}n_L + \frac{368}{85}\right].$$

Par ce même lemme, comme $\rho \neq 1 - \beta_0$ implique $|\rho| \geqslant \frac{1}{4\ln(d_L)}$ (par le lemme 2.17), on a

$$\begin{aligned}\left|\sum_{\chi}\sum_{\substack{\rho\neq 1-\beta_0\\ |\rho|<\frac{1}{2}}}\left(\left|\frac{x^\rho}{\rho}\right| + \left|\frac{1}{\rho}\right|\right)\right| &\leqslant (\sqrt{x}+1)\sum_{\chi}\sum_{\substack{\rho\neq 1-\beta_0\\ |\rho|<\frac{1}{2}}}\left|\frac{1}{\rho}\right| \\ &\leqslant 5(\sqrt{x}+1)\left[\ln(d_L) + 3 + n_L\left(\ln\left(\frac{3}{2\pi}\right) + 2\right)\right]\ln(d_L) \\ &\leqslant \frac{2507}{16}(\sqrt{x}+1)(\ln(d_L))^2 \qquad (2.35)\end{aligned}$$

par l'inégalité de Hermite-Minkowski $d_L \geqslant \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n_L-1}$ ([Sam67], IV.2, corollaire 2), valable quand $n_L > 1$ (ce dont on déduit plus précisément $n_L \leqslant \frac{\ln(d_L)}{\ln\left(\frac{\pi}{3}\right)}$) ; cette même inégalité démontre que si $n_L > 1$, alors $d_L \geqslant 3$, si bien que $3 \leqslant 3\ln(d_L)$; en vérité, on a même $d_L \geqslant 4$ car le discriminant est congru à 0 ou 1 modulo 4, mais cette majoration suffira. À noter que si $n_L = 1$ (et $\ln(d_L) = 0$), alors (2.35) est également vraie. Pour finir,

$$\frac{x^{1-\beta_0}}{1-\beta_0} - \frac{1}{1-\beta_0} = x^\sigma \ln(x) \leqslant \sqrt{x}\ln(x)$$

pour un certain $\sigma \in [0{,}1-\beta_0]$. Supposons provisoirement $n_L \geqslant 2$. Tout ceci nous permet d'obtenir :

$$\begin{aligned}\left|S(x,T) - \frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\beta_0}\right| &= \frac{|C|}{|G|}\left|\sum_\chi \bar{\chi}(g)\left(\sum_{\substack{|\rho|>\frac{1}{2}\\|\gamma|<T}}\frac{x^\rho}{\rho} + \sum_{\substack{|\rho|<\frac{1}{2}\\|\gamma|<T}}\frac{x^\rho}{\rho} - \sum_{|\rho|<\frac{1}{2}}\frac{1}{\rho}\right) - \chi_0(g)\frac{x^{\beta_0}}{\beta_0}\right| \\ &\leqslant \frac{|C|}{|G|}\frac{5}{2}\Bigg[\frac{(\ln(T))^2}{4}n_L + \ln(T)\left(\frac{\ln(d_L)}{2} + \frac{5}{14}n_L\right) + 2\ln(d_L) \\ &\quad + \frac{46}{11}n_L + \frac{368}{85}\Bigg]x\exp\left(-\frac{c\ln(x)}{\ln\left((ad_L)^{N_1}\left(b\left(\frac{T+3}{2\pi}\right)^{N_2}\right)^{n_L}\right)}\right) \\ &\quad + \frac{|C|}{|G|}\left(\frac{2507}{16}(\sqrt{x}+1)(\ln(d_L))^2 + \frac{x^{1-\beta_0}}{1-\beta_0} - \frac{1}{1-\beta_0}\right),\end{aligned}$$

et puis :

$$\begin{aligned}\left|S(x,T) - \frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\beta_0}\right| &\leqslant \frac{|C|}{|G|}\frac{5}{2}\left[\frac{(\ln(T))^2}{4\ln\left(\frac{\pi}{3}\right)} + \frac{\ln(T)}{2} + 2 + \frac{48}{7\ln\left(\frac{\pi}{3}\right)} + \frac{368}{85}\right]\ln(d_L) \\ &\quad \times x\exp\left(-\frac{c\ln(x)}{\ln\left((ad_L)^{N_1}\left(b\left(\frac{T+3}{2\pi}\right)^{N_2}\right)^{n_L}\right)}\right) \\ &\quad + \frac{|C|}{|G|}\sqrt{x}\left(\ln(x) + \frac{2507}{16}\left(1+\frac{1}{\sqrt{x}}\right)(\ln(d_L))^2\right).\end{aligned}$$

En posant $T = \frac{2\pi}{(b(ad_L)^{N_1})^{1/N_2}}\exp\left(\sqrt{\frac{\ln(x)}{n_L}}\right) - 3$ et en considérant les réels $x \geqslant 2$ tels

que $\ln(x) \geqslant 4n_L N_2^2 \left[\ln\left(\frac{5}{2\pi}\left(b(ad_L)^{N_1}\right)^{1/N_2}\right)\right]^2$, on a bien $T \geqslant 2$, et

$$\begin{aligned}\left|S(x,T) - \frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\beta_0}\right| &\leqslant \frac{|C|}{|G|}\frac{5}{2}\ln(d_L)\left(\frac{(\ln(T))^2}{4\ln\left(\frac{\pi}{3}\right)} + \frac{\ln(T)}{2} + 156\right) \\ &\quad \times x\exp\left(-c\sqrt{\frac{\ln(x)}{n_L}}\right) \\ &\quad + \frac{|C|}{|G|}\sqrt{x}\ln(x)\left(1 + \frac{2507}{16n_L}\left(1 + \frac{1}{\sqrt{x}}\right)\left(\frac{N_2}{2N_1}\right)^2\right) \\ &\leqslant \frac{|C|}{|G|}\left(2106 + 2771482n_L\right)x\exp\left(-\frac{c}{2}\sqrt{\frac{\ln(x)}{n_L}}\right), \qquad (2.36)\end{aligned}$$

d'après les inégalités (2.37) et (2.38) listées ci-après. On invoque à nouveau le théorème 2.15. Ce choix pour T, ainsi que les inégalités suivantes,

$$\sqrt{\frac{\ln(x)}{n_L}} \leqslant \exp\left(\frac{1}{a}\sqrt{\frac{\ln(x)}{n_L}}\right) + a(\ln(a) - 1) \text{ pour tous } x \geqslant 2, a > 0, \qquad (2.37)$$

$$\sqrt{\frac{\ln(x)}{n_L}} \leqslant \exp\left(\frac{1}{4a^2 n_L}\right)x\exp\left(-\frac{1}{a}\sqrt{\frac{\ln(x)}{n_L}}\right) \text{ pour tous } x \geqslant 2, a > 0, \qquad (2.38)$$

$$\frac{N_1}{N_2}\ln(d_L) \leqslant \ln\left(\frac{5}{2\pi}(b(ad_L)^{N_1})^{1/N_2}\right) \leqslant \frac{1}{2}\sqrt{\frac{\ln(x)}{n_L}} \text{ (supposée vérifiée ci-dessus)},$$

$$n_L \leqslant \frac{N_2}{2N_1\ln\left(\frac{\pi}{3}\right)}\sqrt{\frac{\ln(x)}{n_L}} \text{ (Hermite-Minkowski et l'inégalité ci-dessus)}$$

((2.37) provient de la recherche du maximum de $t \mapsto t - \exp\left(\frac{t}{a}\right)$ par dérivation, tandis que (2.38) procède de même en étudiant $t \mapsto \frac{\exp\left(t^2 - \frac{t}{a\sqrt{n_L}}\right)}{t}$) impliquent que :

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant 3448189912192\frac{|C|}{|G|}x\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(x)}{n_L}}\right). \qquad (2.39)$$

Finalement, le rassemblement de (2.36) et (2.39) donne le théorème. Pour $n_L = 1$, les calculs à mener sont essentiellement les mêmes malgré l'absence de l'inégalité de Minkowski (grâce aux inégalités (2.37) et (2.38)), et on obtient la même inégalité. □

Pour passer de ψ_C à π_C, le raisonnement est assez classique. Posons

$$\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \mathrm{N}(\mathfrak{p}) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}(\mathfrak{p})).$$

Il y a au plus n_K idéaux $\mathfrak{p}^m$, avec $\mathfrak{p}$ premier, dont la norme a une certaine valeur donnée, et de plus

$$\sum_{\substack{\mathfrak{p}, m \geqslant 2 \\ \mathfrak{p} \text{ non ramifié} \\ \mathrm{N}(\mathfrak{p}^m) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}(\mathfrak{p})) = \theta_C(x^{1/2}) + \theta_C(x^{1/3}) + \cdots + \theta_C(x^{1/[\ln(x)/\ln(2)]})$$

car $x^{1/M} < 2$ pour $M > \ln(x)/\ln(2)$, donc l'inégalité $\theta_C(x) \leqslant n_K \theta_{\mathbb{Q}}(x) < 1{,}01624 n_K x$ (tirée de [RS62], théorème 9, valable pour tout $x \geqslant 2$) implique que :

$$0 \leqslant \psi_C(x) - \theta_C(x) = \sum_{\substack{\mathfrak{p}, m \geqslant 2 \\ \mathfrak{p} \text{ non ramifié} \\ \mathrm{N}(\mathfrak{p}^m) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}(\mathfrak{p})) \leqslant \frac{22}{15} n_K \sqrt{x} \ln(x).$$

Ceci prouve que θ_C vérifie presque la même formule asymptotique que ψ_C :

$$\left|\theta_C(x) - \frac{|C|}{|G|}x\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\ln(x)\Big[\left(\frac{55}{48} + \frac{1815}{37\ln(x)}\right)\ln(d_L) + \left(\frac{161}{342}\ln(x) + \frac{3421}{270} + \frac{148890}{653\ln(x)}\right)n_L + \frac{5920}{59}\Big] \tag{2.40}$$

si on suppose HRG, et, inconditionnellement,

$$\theta_C(x) = \frac{|C|}{|G|}x - \frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\beta_0} + \frac{|C|}{|G|}R_0(x), \tag{2.41}$$

où β_0 est l'éventuel zéro exceptionnel de ζ_L dans la région décrite dans le lemme 2.17, χ_0 le caractère tel que $\mathrm{L}(\beta_0, \chi_0) = 0$, avec

$$|R_0(x)| \leqslant 3448193801726 x \exp\left(-\frac{1}{8}\sqrt{\frac{\ln(x)}{n_L}}\right).$$

Une transformée d'Abel et une intégration par parties donnent les théorèmes 1.7 et 1.8 : on a en effet

$$\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x) = \frac{\theta_C(x) - \frac{|C|}{|G|}x}{\ln(x)} + \int_2^x \frac{\theta_C(t) - \frac{|C|}{|G|}t}{t(\ln(t))^2}\mathrm{d}t + \frac{|C|}{|G|}\frac{2}{\ln(2)}.$$

On utilise la majoration $\int_2^x \frac{\mathrm{d}t}{\sqrt{t}\ln(t)} \leqslant \frac{4\sqrt{x}}{\ln(x)}$, obtenue *via* le changement de variable $u = \frac{-\ln(t)}{2}$ qui nous ramène à l'étude de l'exponentielle intégrale, dont on trouve toute une étude dans [AS64], page 228.

Il faut toutefois être vigilant pour obtenir le théorème inconditionnel : comme le théorème 2.22 donne une estimation valable pour $x \geqslant a := \exp\left(\frac{219961}{4} n_L (\ln(9d_L^8))^2\right)$, on doit faire un léger découpage :

$$\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x) = -\frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\ln(x^{\beta_0})} + \frac{|C|}{|G|}\frac{R_0(x)}{\ln(x)} + \int_2^{\sqrt{x}} \frac{\theta_C(t) - \frac{|C|}{|G|}t}{t(\ln(t))^2}\mathrm{d}t + \int_{\sqrt{x}}^x \frac{\theta_C(t) - \frac{|C|}{|G|}t}{t(\ln(t))^2}\mathrm{d}t.$$

Si, à partir de maintenant, on suppose $x \geqslant a^2$, alors

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \left|-\frac{|C|}{|G|}\chi_0(g)\frac{x^{\beta_0}}{\ln(x^{\beta_0})} + \frac{|C|}{|G|}\int_{\sqrt{x}}^x \frac{-\chi_0(g)\frac{t^{\beta_0}}{\beta_0} + R_0(t)}{t(\ln(t))^2}\mathrm{d}t\right| + \frac{|C|}{|G|}\frac{R_0(x)}{\ln(2)} + n_K\int_2^{\sqrt{x}} \frac{2{,}01624}{(\ln(t))^2}\mathrm{d}t,$$

et

$$\begin{aligned} n_K\int_2^{\sqrt{x}}\mathrm{d}t &\leqslant \frac{|C|}{|G|}\frac{1407}{43504\ln\left(\frac{\pi}{3}\right)}\sqrt{\frac{\ln(x)}{n_L}}\sqrt{x} \\ &\leqslant \frac{|C|}{|G|}\frac{1407\sqrt{2}}{43504\ln\left(\frac{\pi}{3}\right)}\exp\left(\frac{1}{4}\left(\frac{1}{8}\right)^2\right)x\exp\left(-\frac{1}{8\sqrt{2}}\sqrt{\frac{\ln(x)}{n_L}}\right), \end{aligned}$$

tandis que

$$\int_{\sqrt{x}}^x \frac{\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(t)}{n_L}}\right)}{(\ln(t))^2}\mathrm{d}t \leqslant 4x\frac{\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(x)}{2n_L}}\right)}{(\ln(x))^2},$$

d'où le théorème 1.7.

2.7 Majoration du zéro de Siegel

L'éventuel zéro de Siegel de la fonction ζ_L de Dedekind apparaît dans l'énoncé du théorème 1.7, ainsi que dans les estimations inconditionnelles des sommes du lemme 6.9. Il convient donc d'en avoir une majoration explicite. Pour cela, on démontre une version explicite (probablement très grossière) du phénomène de Deuring-Heilbronn,

ou phénomène de répulsion des zéros. Il est démontré dans [KN12], théorème 4, mais pour un discriminant suffisamment grand (en un sens non explicite). On propose donc une démonstration qui vaut pour tout discriminant, et qui s'inspire de celle, non explicite, de [LMO79]. Notons β_0 le zéro de Siegel.

Lemme 2.23 (Densité des zéros)**.** *Soit $n(u)$ le nombre de zéros non triviaux ρ de ζ_L tels que $|\mathrm{Im}(\rho)| \leqslant u$. Alors, pour $u \geqslant 1$,*

$$\left| n(u) - \frac{u}{\pi} \ln\left(\left(\frac{u}{2\pi e} \right)^{n_L} |d_L| \right) \right| \leqslant \ln\left(|d_L| (e^6 u)^{n_L} e^8 \right).$$

Démonstration. Voir [KN12], théorème 1, où on pose $\eta = \frac{1}{2}$. □

Théorème 2.24 (Phénomène de Deuring-Heilbronn)**.** *Si ζ_L a un zéro réel $\beta_0 > 0$, alors $\zeta_L(s) \neq 0$ pour*

$$\mathrm{Re}(s) > 1 + \frac{\ln\left(1536(1-\beta_0)\ln\left(|d_L|^7(|\mathrm{Im}(s)|+1)^{n_L/4}e^{26n_L+32}\right)\right)}{192\ln\left(|d_L|^7(|\mathrm{Im}(s)|+1)^{n_L/4}e^{26n_L+32}\right)}.$$

On a besoin, pour ce résultat, du lemme suivant.

Lemme 2.25 ([LMO79], lemme 4.1 et théorème 4.2)**.** *Soit $s_m = \sum_{n=1}^{\infty} b_n z_n^m$, et supposons que :*

- *$|z_n| \leqslant |z_1|$ pour tout $n \geqslant 1$;*
- *les b_n sont réels ;*
- *$b_n \geqslant 0$ pour tout n tel que $\frac{1}{3}|z_1| \leqslant |z_n| \leqslant |z_1|$.*

Posons $S = (b_1|z_1|)^{-1} \sum_{n=1}^{\infty} |b_n z_n|$. Alors, il existe un entier naturel non nul j_0 tel que $j_0 \leqslant 24S$, et :

$$\mathrm{Re}(s_{j_0}) \geqslant \frac{b_1}{8}|z_1|^{j_0}.$$

Démonstration du théorème 2.24. La fonction $s \mapsto (s-1)\zeta_L(s)$ étant entière et d'ordre 1, elle admet un produit de Hadamard :

$$(s-1)\zeta_L(s) = s^r \exp(B_1 + B_2 s) \prod_{\omega} \left(1 - \frac{s}{\omega}\right) \exp\left(\frac{s}{\omega}\right),$$

où ω parcourt les zéros non nuls ζ_L (triviaux compris), et r est l'ordre d'annulation en 0. La dérivée logarithmique de cette fonction vérifie donc :

$$-\frac{\zeta_L'}{\zeta_L}(s) = \frac{1}{s-1} - B_2 - \sum_{\omega} \left(\frac{1}{s-\omega} + \frac{1}{\omega} \right) - \frac{r}{s}.$$

En comparant cette identité à la dérivée logarithmique du produit eulérien de ζ_L, nous avons pour tout $\mathrm{Re}(s) > 1$,

$$\sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \ln(\mathrm{N}(\mathfrak{p}))(\mathrm{N}(\mathfrak{p}))^{-ms} = \frac{1}{s-1} - B_2 - \sum_{\omega} \left(\frac{1}{s-\omega} + \frac{1}{\omega} \right) - \frac{r}{s},$$

et donc, en dérivant $2j-1$ fois, on obtient pour tout $j \geqslant 1$,

$$\frac{1}{(2j-1)!} \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \ln(\mathrm{N}(\mathfrak{p}))(\ln(\mathrm{N}(\mathfrak{p}^m)))^{2j-1}(\mathrm{N}(\mathfrak{p}))^{-ms} = \frac{1}{(s-1)^{2j}} - \sum_{\omega} \frac{1}{(s-\omega)^{2j}},$$

où ω parcourt tous les zéros de ζ_L (0 compris, avec multiplicité). On évalue cette égalité en $s = \sigma$ et en $s = \sigma + it$, et on ajoute les résultats obtenus :

$$\begin{aligned} &\frac{1}{(2j-1)!} \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \ln(\mathrm{N}(\mathfrak{p}))(\ln(\mathrm{N}(\mathfrak{p}^m)))^{2j-1}(\mathrm{N}(\mathfrak{p}))^{-m\sigma}(1 + (\mathrm{N}(\mathfrak{p}))^{-mit}) \\ &= \frac{1}{(\sigma-1)^{2j}} + \frac{1}{(\sigma+it-1)^{2j}} - \frac{1}{(\sigma-\beta_0)^{2j}} - \frac{1}{(\sigma+it-\beta_0)^{2j}} - \sum_{n=1}^{\infty} z_n^j, \end{aligned} \tag{2.42}$$

où $(z_n)_{n\geqslant 1}$ est la suite (ordonnée par ordre de décroissance) des termes $\frac{1}{\sigma+it-\omega}$ et $\frac{1}{\sigma-\omega}$ (où ω parcourt tous les zéros de ζ_L, y compris 0 avec multiplicité, excepté β_0). La partie réelle du membre de gauche de (2.42) est positive, donc $\sigma = 2$ fournit :

$$\mathrm{Re}\left(\sum_{n=1}^{\infty} z_n^j \right) \leqslant 1 - \frac{1}{(2-\beta_0)^{2j}} + \mathrm{Re}\left(\frac{1}{(1+it)^{2j}} - \frac{1}{(2-\beta_0+it)^{2j}} \right) \leqslant 1 + 2j(1-\beta_0),$$

parce que

$$\begin{aligned} \mathrm{Re}\left(\frac{1}{(1+it)^{2j}} - \frac{1}{(2-\beta_0+it)^{2j}} \right) &= 2j \int_1^{2-\beta_0} \mathrm{Re}\left(\frac{1}{(x+it)^{2j+1}} \right) \mathrm{d}x \\ &\leqslant 2j(1-\beta_0). \end{aligned} \tag{2.43}$$

À présent, supposons que $\rho = \beta + i\gamma \neq \beta_0$ est un zéro de ζ_L. On pose $t = \gamma$, et on applique le lemme 2.25 à la suite $(z_n)_{n\geqslant 1}$: il existe un entier naturel non nul $j_0 \leqslant 24S$ tel que

$$\mathrm{Re}\left(\sum_{n=1}^{\infty} z_n^{j_0} \right) \geqslant \frac{b_1}{8} |z_1|^{j_0} \geqslant \frac{1}{8} \frac{1}{(2-\beta)^{2j_0}} \geqslant \frac{1}{8} \exp(-2j_0(1-\beta)), \tag{2.44}$$

où S est défini dans l'énoncé du lemme 2.25. Comme $z_1 \geqslant \frac{1}{(2-\beta)^2}$, nous pouvons borner S :

$$S \leqslant (2-\beta)^2 \sum_{\omega} \left(\frac{1}{|2-\omega|^2} + \frac{1}{|2+i\gamma-\omega|^2} \right).$$

Le lemme 2.23 permet d'estimer cette somme. D'abord,

$$\sum_{\omega}\left(\frac{1}{|2-\omega|^2}+\frac{1}{|2+i\gamma-\omega|^2}\right)\leqslant 2\left(\int_0^\infty\frac{\mathrm{d}n(u)}{1+u^2}+\int_0^\infty\frac{\mathrm{d}n(u)}{1+(\gamma-u)^2}\right),$$

puis, par intégration par parties :

$$\begin{aligned}\sum_{\omega}\left(\frac{1}{|2-\omega|^2}+\frac{1}{|2+i\gamma-\omega|^2}\right)\leqslant 2\left(7n_L+\ln\left(|d_L|e^8\right)+\frac{\ln\left(|d_L|\right)}{2}\right)\\ +2\left(n_L\left(6+\frac{\ln(|\gamma|+1)}{8}\right)+2\ln\left(|d_L|e^4\right)\right),\end{aligned}$$

Enfin,

$$S\leqslant 4\ln\left(|d_L|^7(|\gamma|+1)^{n_L/4}e^{26n_L+32}\right).$$

Cette majoration de S, combinée à (2.43) et (2.44), donne le résultat voulu. □

On en déduit une borne (très) grossière sur le zéro de Siegel.

Corollaire 2.26. *Soit β_0 l'éventuel zéro de Siegel de ζ_L. Alors,*

$$1-\beta_0\geqslant\frac{1}{1536}\frac{1}{|d_L|^{2709}e^{387(26n_L+32)}}.$$

Démonstration. En effet, dans le cas contraire, alors le théorème précédent implique que ζ_L ne s'annule pas sur la droite réelle pour $\mathrm{Re}(s)>-1{,}01$ hormis en β_0, ce qui est impossible : la fonction admet un zéro trivial en -1 ou 0. □

Chapitre 3

Idéal premier de petite norme

« Tout ce qui est nouveau, c'est bien. »
Zinédine Zidane

Le théorème suivant n'est pas utilisé dans le reste de cette thèse, mais n'est pas sans intérêt arithmétique. On en fournit donc une démonstration. L'inégalité est très loin d'être optimale.

Théorème 3.1. *Conservons les notations ci-dessus. Il existe un idéal premier non nul* $\mathfrak{p}$ *de l'anneau d'entiers de* K *vérifiant* $\left[\frac{L/K}{\mathfrak{p}}\right] = C$*, de degré* $f = 1$ *sur* $\mathbb{Q}$*, et tel que*

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant \max\left(2, d_L^{27175010}\right)$$

Le cas où la norme égale 2 se produit pour $L = K = \mathbb{Q}$. On est en droit d'espérer une majoration bien meilleure : si l'on suppose que HRG est vraie pour ζ_L, alors on sait démontrer qu'on peut remplacer le majorant du théorème ci-dessus par $\max(2{,}70(\ln(d_L))^2)$ (voir [Ser81], théorème 5).

Une approche naïve pour obtenir une telle borne serait d'utiliser le théorème de Chebotarev explicite (théorème 1.7) pour résoudre l'inégalité $\pi_C(x) > 0$. Mais la borne obtenue serait incomparablement plus laide que celle ci-dessus à cause de l'intervention du zéro de Siegel. On procède avec plus de finesse, si j'ose dire, dans les sections suivantes, selon une démarche très proche de celle adoptée pour démontrer le théorème 1.7 : toujours grâce à la relation d'orthogonalité des caractères et à la transformée de Mellin inverse, on exprime une somme de termes positifs, à support dans les idéaux premiers qui nous intéressent, en fonction d'intégrales (avec noyaux, à la différence de celles du chapitre précédent) de fonctions L d'Artin puis, en vérité, de Hecke, grâce au lemme 2.3. Si cette somme est strictement positive, en particulier son support est non vide, prouvant l'existence d'un idéal premier vérifiant les conditions prescrites. Pour minorer cette somme, on l'exprime à l'aide des zéros de fonctions L de Hecke, en approchant les intégrales qui lui sont liées par des intégrales sur un

contour, puis en utilisant le théorème des résidus ; estimer cette somme dépend donc d'informations sur la localisation des zéros, déjà obtenues partiellement dans les sections 2.2 et 2.7, et complétées ici à la fin de la section 3.2. D'éventuelles améliorations proviendront, je pense, d'une meilleure version du phénomène de Deuring-Heilbronn (théorème 2.24 ; rappelons que [KN12] fournit une meilleure borne, mais valable pour un discriminant suffisamment grand en un sens non explicite) et d'un meilleur choix que x^{10} dans l'approximation de la somme avec le second noyau.

La notation $\sum_{\mathfrak{p}}$ désigne toujours une somme indicée par les idéaux maximaux $\mathfrak{p}$ de l'anneau d'entiers de K. Pour alléger les notations, on note $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$.

3.1 Transformée de Mellin inverse

Reprenons l'étude de $F_C(s) = -\frac{|C|}{|G|}\sum_{\Phi}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi,L/K)$, où Φ parcourt l'ensemble des caractères irréductibles de G et $\mathrm{L}(\cdot,\Phi,L/K)$ désigne la fonction L d'Artin attachée au caractère Φ (voir le début de la section 2.1). La relation d'orthogonalité des caractères implique, on l'a vu dans la section 2.1, que pour $\mathrm{Re}(s) > 1$,

$$F_C(s) = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))(\mathrm{N}(\mathfrak{p}))^{-ms}$$

où, pour $\mathfrak{p}$ non ramifié dans L, on a $\theta(\mathfrak{p}^m) = 1$ dès que $\left[\frac{L/K}{\mathfrak{p}}\right]^m = C$, $\theta(\mathfrak{p}^m) = 0$ sinon, tandis que $|\theta(\mathfrak{p}^m)| \leqslant 1$ si $\mathfrak{p}$ se ramifie dans L. La fonction F_C peut s'exprimer, d'après le lemme 2.3, comme somme de fonctions L de Hecke, nous permettant d'utiliser leurs équations fonctionnelles et les propriétés qui en découlent. On a :

$$F_C(s) = -\frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi),$$

où χ parcourt l'ensemble des caractères *irréductibles* de H, et $\mathrm{L}(s,\chi)$ est une fonction L de Hecke associée à E et au caractère de Hecke *primitif* χ.

Soient

$$k_{1,x}(s) = \left(\frac{x^{2(s-1)} - x^{s-1}}{s-1}\right)^2 \text{ et } k_{2,x}(s) = x^{s^2+s}$$

nos deux « noyaux », où $x \geqslant 4$ est un paramètre réel implicite. Le calcul de la transformée inverse de Mellin de ces noyaux est assez directe et on obtient, pour $u > 0$,

$$\hat{k}_{1,x}(u) = \begin{cases} u^{-1}\ln(x^4/u) & \text{si } x^3 \leqslant u \leqslant x^4, \\ u^{-1}\ln(u/x^2) & \text{si } x^2 \leqslant u \leqslant x^3, \\ 0 & \text{sinon,} \end{cases}$$

puis

$$\hat{k}_{2,x}(u) = \frac{1}{\sqrt{4\pi \ln(x)}} \exp\left(-\frac{(\ln(u/x))^2}{4\ln(x)}\right).$$

La convergence uniforme des séries de Dirichlet définissant $\mathrm{L}(\cdot,\chi)$ pour $\mathrm{Re}(s) > 1$, ainsi que la convergence absolue des intégrales des noyaux sur les droites verticales, démontrent que pour $j \in \{1,2\}$:

$$I_j := \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} F_C(s)k_{j,x}(s)\mathrm{d}s = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{j,x}(\mathrm{N}(\mathfrak{p}^m)).$$

Nous allons d'abord estimer la contribution provenant des idéaux premiers qui se ramifient (il n'y en a qu'un nombre fini), puis celle des termes contenant $\mathrm{N}(\mathfrak{p}^m)$ pour $m > 1$, et enfin celle des idéaux premiers de « grande norme » ; le choix de $k_{2,x}$ est précisément fait pour minimiser leur contribution. Les trois prochains lemmes contiennent les inégalités désirées.

Lemme 3.2 (Idéaux premiers ramifiés)**.** *On a, pour $x \geqslant 4$,*

$$\left|\sum_{\mathfrak{p}\ ramifié}\sum_{m=1}^{\infty} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant \frac{2}{|G|}\frac{\ln(x)}{x^2-1}\ln(d_L),\ \textit{et}$$

$$\left|\sum_{\mathfrak{p}\ ramifié}\sum_{\substack{m=1\\ \mathrm{N}(\mathfrak{p}^m)\leqslant x^{10}}}^{\infty} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant 10\frac{\sqrt{\ln(x)}}{\sqrt{\pi}\ln(2)}\frac{\ln(d_L)}{|G|}.$$

Démonstration. Comme $\hat{k}_{1,x}(u) = 0$ pour $u < x^2$ et $u > x^4$, on a :

$$\left|\sum_{\mathfrak{p}\ \text{ramifié}}\sum_{m=1}^{\infty} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant \ln(x)\sum_{\mathfrak{p}\ \text{ramifié}}\ln(\mathrm{N}(\mathfrak{p}))\sum_{\substack{m=1\\ \mathrm{N}(\mathfrak{p}^m)\geqslant x^2}}(\mathrm{N}(\mathfrak{p}))^{-m}.$$

Utilisant (2.3) et l'inégalité suivante,

$$\sum_{\substack{m=1\\ \mathrm{N}(\mathfrak{p}^m)\geqslant x^2}}(\mathrm{N}(\mathfrak{p}))^{-m} \leqslant \sum_{m=1}^{\infty}\frac{1}{x^{2m}} = \frac{1}{x^2-1}, \tag{3.1}$$

on obtient la première majoration du lemme (on aurait également pu majorer le membre de gauche de (3.1) par $\frac{1}{x^2}+\frac{1}{x^4}$, mais cela n'affecte pas du tout l'inégalité du théorème 3.1). La deuxième majoration du lemme est obtenue par des calculs analogues, à l'aide de l'estimation triviale $\exp\left(-\frac{(\ln(u/x))^2}{4\ln(x)}\right) \leqslant 1$. □

Lemme 3.3 (Puissances d'idéaux premiers)**.** *Si* $\sum_P$ *désigne les sommes indicées par les paires* $(\mathfrak{p}, m)$ *telles que* $\mathrm{N}(\mathfrak{p})^m$ *ne soit pas un nombre premier, alors pour* $x \geqslant 4$*,*

$$\left|\sum_P \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant 4n_K\frac{(\ln(x))^2}{x^2-1}, \text{ et}$$

$$\left|\sum_P \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant n_K x^{3/4}\sqrt{\ln(x)}\left(1+\frac{104}{\ln(x)}\right).$$

Démonstration. Il existe au plus n_K puissances d'idéaux premiers distinctes de norme donnée (qui, de plus, doit être la puissance d'un nombre premier). Par conséquent,

$$\begin{aligned}\left|\sum_P \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p}^m))\right| &\leqslant n_K\ln(x)\sum_{p\in\mathrm{Spec}(\mathbb{Z})\setminus\{0\}}\sum_{\substack{h=2\\ x^2\leqslant p^h\leqslant x^4}}^{\infty}\frac{\ln(p^h)}{p^h}\\ &\leqslant 4n_K(\ln(x))^2\sum_{\substack{p\in\mathrm{Spec}(\mathbb{Z})\setminus\{0\}\\ x\leqslant p\leqslant x^2}}\sum_{\substack{h=2\\ x^2\leqslant p^h\leqslant x^4}}^{\infty}\frac{1}{p^h}\\ &\leqslant 4n_K(\ln(x))^2\sum_{\substack{p\in\mathrm{Spec}(\mathbb{Z})\setminus\{0\}\\ x\leqslant p\leqslant x^2}}\left(\frac{1}{p^2-1}-\frac{1}{p^2}\right)\\ &\leqslant 4n_K\frac{(\ln(x))^2}{x^2-1}.\end{aligned}$$

Une meilleure estimation découle bien entendu du théorème des nombres premiers, mais cette borne est suffisamment bonne pour nos desseins. On passe donc au second noyau :

$$\begin{aligned}\left|\sum_P \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p}^m))\right| &\leqslant n_K\sum_{p\in\mathrm{Spec}(\mathbb{Z})\setminus\{0\}}\sum_{h=2}^{\infty}\ln(p^h)\hat{k}_{2,x}(p^h)\\ &\leqslant n_K\int_1^{\infty}\ln(u)\hat{k}_{2,x}(u)\mathrm{d}S(u),\end{aligned}$$

où S est la fonction de décompte des puissances h-ièmes, avec $h \geqslant 2$ (l'intégrale ci-dessus est de Riemann-Stieltjes). Trouvons d'abord une majoration de S. On a, pour $u \geqslant 2$,

$$\begin{aligned}S(u) = \sum_{\substack{m=2\\ m\leqslant\sqrt{u}}}^{\infty}\sum_{\substack{h=2\\ m^h\leqslant u}}^{\infty}1 \leqslant \sum_{\substack{m=2\\ m\leqslant\sqrt{u}}}^{\infty}\frac{\ln(u)}{\ln(m)} &\leqslant \ln(u)\left(\frac{1}{\ln(2)}+\int_2^{\sqrt{u}}\frac{\mathrm{d}t}{\ln(t)}\right)\\ &\leqslant \sqrt{u}\left(1+\frac{35}{\ln(u)}\right).\end{aligned}$$

Une intégration par parties donne :

$$\begin{aligned}\int_1^\infty \ln(u)\hat{k}_{2,x}(u)\mathrm{d}S(u) &= -\int_2^\infty \left(\frac{\hat{k}_{2,x}(u)}{u} + \ln(u)\hat{k}'_{2,x}(u)\right) S(u)\mathrm{d}u \\ &\leqslant \int_x^\infty \left(1+\frac{35}{\ln(u)}\right)\ln(u)\frac{\ln(u/x)}{\sqrt{u}}\exp\left(-\frac{(\ln(u/x))^2}{4\ln(x)}\right)\mathrm{d}u \\ &\times \frac{1}{4\sqrt{\pi}(\ln(x))^{3/2}} \\ &\leqslant \sqrt{\frac{x}{\pi}}\frac{\left(1+\frac{35}{\ln(x)}\right)}{4(\ln(x))^{3/2}}\int_1^\infty \ln(vx)\frac{\ln(v)}{\sqrt{v}}\exp\left(-\frac{(\ln(v))^2}{4\ln(x)}\right)\mathrm{d}v \\ &\leqslant \int_0^\infty (w+\ln(x))w\exp\left(-\frac{1}{4}\left(\frac{w}{\sqrt{\ln(x)}}-\sqrt{\ln(x)}\right)^2\right)\mathrm{d}w \\ &\times \frac{x^{3/4}}{\sqrt{\pi}}\frac{\left(1+\frac{35}{\ln(x)}\right)}{4(\ln(x))^{3/2}},\end{aligned}$$

grâce au changement de variable $w = \ln(v) = \ln\left(\frac{u}{x}\right)$ et quelques calculs anodins. L'intégrale obtenue est proche de la fonction d'erreur de Gauss, définie par

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \exp(-t^2)\mathrm{d}t,$$

et dont nous connaissons des estimations (voir par exemple [AS92], chapitre 7) nous permettant d'obtenir :

$$\begin{aligned}\int_0^\infty (w+\ln(x))w\exp\left(-\frac{1}{4}\left(\frac{w}{\sqrt{\ln(x)}}-\sqrt{\ln(x)}\right)^2\right)\mathrm{d}w &\leqslant \left(\sqrt{\pi}\left(1+\frac{1}{\ln(x)}\right)+\frac{1}{x^{1/4}}\right) \\ &\times 4(\ln(x))^2.\end{aligned}$$

On en déduit le lemme. □

Lemme 3.4 (« Grands » idéaux premiers)**.** *On a, pour $x \geqslant 4$,*

$$\left|\sum_{\mathfrak{p}}\sum_{\substack{m=1\\ \mathrm{N}(\mathfrak{p}^m)>x^{10}}}^{\infty}\theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant \frac{10}{7\sqrt{\pi}}\frac{n_K}{x^{41/4}}\sqrt{\ln(x)}.$$

Démonstration. En effet,

$$\left|\sum_{\mathfrak{p}}\sum_{\substack{m=1\\ \mathrm{N}(\mathfrak{p}^m)>x^{10}}}^{\infty}\theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p}^m))\right| \leqslant n_K\sum_{\substack{q=1\\ q>x^{10}}}^{\infty}\ln(q)\hat{k}_{2,x}(q) \leqslant n_K\int_{x^{10}}^\infty \ln(u)\hat{k}_{2,x}(u)\mathrm{d}u,$$

puisque $u \mapsto \ln(u)\hat{k}_{2,x}(u)$ décroît sur $[x^{10}, \infty[$. Comme dans la démonstration du lemme précédent, le changement de variable $v = \ln\left(\frac{u}{x}\right)$ mène à l'intégrale de Gauss.

$$\begin{aligned}\int_{x^{10}}^{\infty} \ln(u)\hat{k}_{2,x}(u)\mathrm{d}u &= \frac{x^2}{\sqrt{4\pi\ln(x)}} \int_{9\ln(x)}^{\infty} (v+\ln(x)) \exp\left(-\left(\frac{v}{2\sqrt{\ln(x)}} - \sqrt{\ln(x)}\right)^2\right)\mathrm{d}v \\ &\leqslant \frac{x^2}{\sqrt{4\pi\ln(x)}} \cdot \frac{20}{7}\frac{\ln(x)}{x^{49/4}},\end{aligned}$$

ce qui démontre le lemme. □

On peut désormais évaluer les intégrales I_j. Soit Π_C l'ensemble des idéaux premiers de K non ramifiés dans L, de degré un sur $\mathbb{Q}$, et tels que $\left[\frac{L/K}{\mathfrak{p}}\right] = C$. Alors, ces trois lemmes montrent que :

$$\left| I_1 - \sum_{\mathfrak{p}\in\Pi_C} \ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p})) \right| \leqslant \left(\frac{2}{|G|}\frac{\ln(d_L)}{\ln(x)} + 4n_K\right)\frac{(\ln(x))^2}{x^2-1}, \tag{3.2}$$

et, après quelques arrangements,

$$\left| I_2 - \sum_{\substack{\mathfrak{p}\in\Pi_C \\ \mathrm{N}(\mathfrak{p})<x^{10}}} \ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p})) \right| \leqslant \left(\frac{5}{|G|}\ln(d_L) + 152n_K\right) x^{3/4}\sqrt{\ln(x)}. \tag{3.3}$$

3.2 L'intégrale sur un contour, le retour

Maintenant, d'après le schéma de démonstration décrit en début de chapitre, il nous faut calculer I_1 et I_2 en intégrant sur un contour bien choisi pour ensuite, grâce au théorème des résidus, relier une certaine somme indexée par des zéros de fonctions L de Hecke à une somme sur les idéaux premiers qui nous intéressent. Plus précisément, il suffira de calculer les intégrales de la forme

$$J_j(\chi) = -\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{j,x}(s)\mathrm{d}s,$$

où χ est un caractère primitif de Hecke. Les J_j s'avéreront être proches des intégrales sur un contour suivantes :

$$J_j(\chi, T) = -\frac{1}{2\pi i}\int_{B(T)} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{j,x}(s)\mathrm{d}s,$$

où, pour $T > 0$ différent de tout zéro de $\mathrm{L}(\cdot, \chi, E)$, le contour $B(T)$ est le rectangle orienté dans le sens trigonométrique, dont les sommets sont aux affixes $2-iT$, $2+iT$, $-\frac{1}{2}+iT$ et $-\frac{1}{2}-iT$. Par le théorème de Cauchy,

$$J_j(\chi, T) = \delta_{\chi=1}(\chi)k_{j,x}(1) - a(\chi)k_{j,x}(0) - \sum_{\substack{\rho \\ |\gamma|<T}} k_{j,x}(\rho),$$

où $a(\chi) \leqslant n_E$ est un entier naturel introduit juste avant (2.13).

Lemme 3.5 (Intégration sur un segment vertical)**.** *Pour $j \in \{1,2\}$ et $x \geqslant 4$, on a :*

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{j,x}(s)\mathrm{d}s\right| \leqslant 4\left|k_{j,x}\left(-\frac{1}{2}\right)\right|\left(\ln(A(\chi)) + 28n_E\right).$$

Pour $j = 2$, on peut même remplacer la constante multiplicative 4 par 1.

Démonstration. D'après le lemme 2.13,

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{1,x}(s)\mathrm{d}s\right| \leqslant \int_{-T}^{T} \frac{\ln(A(\chi)) + n_E\left(\ln\left(\frac{5}{2}+|t|\right) + \frac{19683}{812}\right)}{\frac{9}{4}+t^2} \times \left(\frac{1}{2\pi x^3}\left(\frac{1}{x^3}+1\right) - \frac{\cos(t\ln(x))}{\pi x^{9/2}}\right)\mathrm{d}t.$$

La seule intégrale qui nécessite un peu de travail est :

$$\int_{-T}^{T} \frac{\ln\left(\frac{5}{2}+|t|\right)}{\frac{9}{4}+t^2}\mathrm{d}t \leqslant 2\int_0^1 \frac{\ln\left(\frac{5}{2}+t\right)}{\frac{9}{4}+t^2}\mathrm{d}t + 2\int_1^T \frac{\ln\left(\frac{5}{2}+t\right)}{t^2}\mathrm{d}t \leqslant 1 + \frac{14}{5}\ln\left(\frac{7}{2}\right).$$

À présent, il n'est pas difficile d'obtenir la majoration suivante :

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{1,x}(s)\mathrm{d}s\right| \leqslant \frac{2}{3x}\left[\left(\ln(A(\chi)) + \frac{19683}{812}n_E\right) + 3n_E\right]$$

Remarquons que $\frac{1}{x} \leqslant 4\left|k_{1,x}\left(-\frac{1}{2}\right)\right|$ pour tout $x \geqslant 4$. Maintenant, on s'occupe du second noyau :

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{2,x}(s)\mathrm{d}s\right| \leqslant \frac{k_{2,x}\left(-\frac{1}{2}\right)}{2\pi}\int_{-T}^{T} \frac{\ln(A(\chi)) + n_E\left(\ln\left(\frac{5}{2}+|t|\right) + \frac{19683}{812}\right)}{x^{t^2}}\mathrm{d}t.$$

Comme

$$\int_{-T}^{T} x^{-t^2}\mathrm{d}t \leqslant \int_{\mathbb{R}} x^{-t^2}\mathrm{d}t = \sqrt{\frac{\pi}{\ln(x)}}, \text{ et}$$

$$\int_{-T}^{T} \ln\left(\frac{5}{2}+|t|\right)x^{-t^2}\mathrm{d}t \leqslant 2\int_0^T \left(t+\frac{3}{2}\right)x^{-t^2}\mathrm{d}t \leqslant \frac{3}{2}\sqrt{\frac{\pi}{\ln(x)}} + \frac{1}{\ln(x)},$$

on trouve le résultat voulu. □

Il est plus délicat d'obtenir des bornes pour l'intégrale sur les segments horizontaux (on devrait imiter les calculs de la section 2.3). Toutefois, on peut toujours démontrer que cette contribution s'annule quand $T \to +\infty$.

Lemme 3.6 (Intégration sur les segments horizontaux)**.** *Pour $j \in \{1,2\}$ et $x \geqslant 4$, on a :*

$$\frac{1}{2\pi i}\int_{2\pm iT}^{-\frac{1}{2}\pm iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{j,x}(s)\mathrm{d}s \ll |k_j(iT)|(\ln(A(\chi)+n_E\ln(T)).$$

En particulier, $\frac{1}{2\pi i}\int\limits_{2\pm iT}^{-\frac{1}{2}\pm iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)k_{j,x}(s)\mathrm{d}s \to 0$ *quand* $T \to \infty$.

Démonstration. Voir [LMO79], page 287, (3.21). □

Ensemble, ces deux lemmes démontrent que, quand $T \to \infty$,

$$J_j(\chi) \geqslant \delta_{\chi=1}(\chi)k_{j,x}(1) - n_E k_{j,x}(0) - \sum_{\rho}|k_{j,x}(\rho)| - 4\left|k_{j,x}\left(-\frac{1}{2}\right)\right|(\ln(A(\chi)) + 28n_E),$$

La définition de F_C, après usage de la formule du discriminant $\sum\limits_{\chi}\ln(A(\chi)) = \ln(d_L)$ et de l'égalité $n_E[L:E] = n_L$, implique que :

$$I_j \geqslant \frac{|C|}{|G|}\left(k_{j,x}(1) - \sum_{\rho}|k_{j,x}(\rho)| - n_L k_{j,x}(0) - 4\left|k_{j,x}\left(-\frac{1}{2}\right)\right|(\ln(d_L)+28n_L)\right), \quad (3.4)$$

où ρ parcourt les zéros non triviaux de ζ_L. Pour achever la démonstration (en trouvant un x tel que $I_j > 0$), nous devons maintenant trouver de bonnes minorations de $k_{j,x}(1) - \sum\limits_{\rho}|k_{j,x}(\rho)|$, qui nécessitent des informations supplémentaires sur la localisation des zéros de la fonction ζ_L. Plus précisément, si ζ_L a un zéro de Siegel, sa contribution peut être non négligeable, mais pour compenser la contribution des autres zéros est petite (c'est le phénomène de Deuring-Heilbronn, qui fait l'objet du lemme 2.24). On complète ce que nous devons savoir sur les zéros de ζ_L :

Lemme 3.7 (Densité des zéros de ζ_L le long de la droite $\mathrm{Re}(s) = 1$)**.** *Soit $n(r,s)$ le nombre de zéros non triviaux ρ de ζ_L tels que $|s-\rho| \leqslant r$. Alors, pour $r > 0$ et $\mathrm{Re}(s) \geqslant 1$,*

$$n(r,s) \leqslant (8+4n_L) + 2r\left(\ln(d_L) + n_L\ln\left(\frac{\frac{3}{2}+|\mathrm{Im}(s)|}{2\pi}\right)\right).$$

Démonstration. La majoration pour $r \geqslant \frac{1}{2}$ découle du lemme 2.23. Supposons donc $0 < r < \frac{1}{2}$. Puisque $n(r,1+it) \geqslant n(r,\sigma+it)$ pour tout $\sigma \geqslant 1$, il nous suffit de

démontrer le lemme pour $s = 1 + it$. De plus, il est évident qu'on a l'inégalité $n(r,1+it) \leqslant n(2r,1+r+it)$. Pour $s = 1+r+it$,

$$2\frac{\zeta_L'}{\zeta_L}(s) = 2\sum_\rho \frac{1}{s-\rho} - \ln(d_L) - 2\left(\frac{1}{s} + \frac{1}{s-1}\right) - 2\frac{\gamma_L'}{\gamma_L}(s),$$

où ρ parcourt les zéros de ζ_L (voir (2.16)), de sorte que

$$\mathrm{Re}\left(\sum_\rho \frac{1}{s-\rho}\right) \leqslant \frac{n_L}{r} + \frac{\ln(d_L)}{2} + \frac{2}{r} + \frac{n_L}{2}\ln\left(\frac{\frac{3}{2}+|t|}{2\pi}\right), \tag{3.5}$$

le facteur γ étant estimé à partir du lemme 2.8. De plus,

$$\sum_\rho \mathrm{Re}\left(\frac{1}{s-\rho}\right) = \sum_\rho \frac{1+r-\mathrm{Re}(\rho)}{|s-\rho|^2} \geqslant \sum_{|s-\rho|\leqslant 2r} \frac{r}{|s-\rho|^2} \geqslant \frac{n(2r,s)}{4r}. \tag{3.6}$$

Le lemme s'obtient en comparant (3.5) et (3.6). □

3.3 Estimations finales

Il ne reste plus qu'à obtenir une bonne minoration de la somme $k_{j,x}(1) - \sum_\rho |k_{j,x}(\rho)|$, où ρ parcourt les zéros non triviaux de ζ_L. Pour aiser les notations, appelons β_0 le zéro de Siegel de ζ_L *s'il existe*, et $\beta_0 = 1 - \frac{1}{4\ln(d_L)}$ sinon. Dans tous les cas,

$$k_{j,x}(1) - \sum_\rho |k_{j,x}(\rho)| \geqslant k_{j,x}(1) - k_{j,x}(\beta_0) - \sum_{\rho\neq\beta_0} |k_{j,x}(\rho)|.$$

De plus, [LMO79], en (6.2) et (6.3), établit que :

$$k_{1,x}(1) - k_{1,x}(\beta_0) \geqslant \frac{(\ln(x))^2}{10}\min(1,(1-\beta_0)\ln(x)), \text{ et}$$

$$k_{2,x}(1) - k_{2,x}(\beta_0) \geqslant \frac{x^2}{10}\min(1,(1-\beta_0)\ln(x)).$$

La somme sera scindée en les zéros proches de 1 et les autres. Selon la proximité de β_0 et 1, on préférera travailler avec un noyau ou l'autre.

Si $\sqrt{1-\beta_0} \geqslant \frac{1}{1536\ln\left(d_L^7 2^{n_L/4} e^{26n_L+32}\right)}$: on utilise ici le noyau $k_{1,x}$. Le lemme 3.7 permet de calculer la somme sur les zéros, pour obtenir :

$$\sum_{|\rho-1|\geqslant 1} |k_{1,x}(\rho)| \leqslant \int_1^\infty \frac{2}{t^2}\mathrm{d}n(t,1) = 4\int_1^\infty \frac{n(t,1)}{t^3}\mathrm{d}t \leqslant 8(4n_L + 2\ln(d_L) + 1).$$

La somme sur les zéros tels que $|\rho-1|<1$ requiert plus d'efforts ; nous allons prouver que si $\rho=\beta+i\gamma\neq\beta_0$, alors

$$\beta\leqslant 1+\frac{\ln\left((1-\beta_0)\ln(d_L)\right)}{487296\ln\left(d_L\right)}.$$

Si un zéro de Siegel existe et vérifie $1-\beta_0\leqslant\left(\frac{1}{5076\cdot1536}\right)^2\frac{1}{\ln(d_L)}$, alors, comme l'inégalité d'Hermite-Minkowski implique $d_L^4\geqslant 2^{n_L/4}$, on a

$$1536(1-\beta_0)\ln\left(d_L^{1265}2^{n_L/4}\right)\leqslant\sqrt{(1-\beta_0)\ln(d_L)}$$

et donc, d'après le théorème 2.24,

$$\beta\leqslant 1+\frac{\ln\left((1-\beta_0)\ln(d_L)\right)}{384\ln\left(d_L^{1265}2^{n_L/4}\right)}\leqslant 1+\frac{\ln\left((1-\beta_0)\ln(d_L)\right)}{487296\ln\left(d_L\right)}.$$

Si $1-\beta_0\geqslant\left(\frac{1}{5076\cdot1536}\right)^2\frac{1}{\ln(d_L)}$, comme la région sans zéro du 2.16 implique l'inégalité $1-\beta\geqslant\frac{1}{4\ln(d_L)}$, on a

$$\beta\leqslant 1+\frac{\ln\left((1-\beta_0)\ln(d_L)\right)}{m\ln(d_L)}$$

pour $m\geqslant -4\ln\left((1-\beta_0)\ln(d_L)\right)$; on peut prendre n'importe quel $m\geqslant 133$, et nous prendrons $m=487296$ à nouveau, pour obtenir la majoration annoncée sans hypothèse sur β_0. Soit $B=-\frac{\ln((1-\beta_0)\ln(d_L))}{487296\ln(d_L)}$. Alors

$$\sum_{|\rho-1|<1}|k_{1,x}(\rho)|\leqslant\frac{1}{x^{2B}}\int_B^1\frac{\mathrm{d}n(t,1)}{t^2}\leqslant\frac{2}{Bx^{2B}}\ln(d_L),$$

nous permettant d'estimer la somme sur les zéros :

$$\sum_{\rho\neq\beta_0}|k_{1,x}(\rho)|\leqslant 884\ln(d_L)+\frac{1}{\ln(2)}(\ln(d_L))^2((1-\beta_0)\ln(d_L))^{\frac{1}{243648}\frac{\ln(x)}{\ln(d_L)}}.$$

Pour résumer, on a, en utilisant ce qui précède et (3.2),

$$\begin{aligned}\sum_{\mathfrak{p}\in\Pi_C}\ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p}))\geqslant\frac{|C|}{|G|}\Big(&\frac{(\ln(x))^2}{10}\min(1,(1-\beta_0)\ln(x))\\&-\frac{3}{2}(\ln(d_L))^2((1-\beta_0)\ln(d_L))^{\frac{1}{243648}\frac{\ln(x)}{\ln(d_L)}}\\&-884\ln(d_L)-\left(2\frac{\ln(d_L)}{\ln(x)}+4n_L\right)\frac{(\ln(x))^2}{x^2-1}\Big).\end{aligned}$$

À présent, posons $x = d_L^{243648}$. Alors, toutes les contributions négatives ci-dessus sont supérieures à $-\frac{1}{80}x^2 \min(1, (1-\beta_0)\ln(x))$, et on a :

$$\sum_{\mathfrak{p}\in\Pi_C} \ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p})) \geqslant \frac{|C|}{|G|}\frac{(\ln(x))^2}{20}\min(1,(1-\beta_0)\ln(x)) > 0.$$

Ceci prouve que l'ensemble des idéaux premiers de Π_C tels que $\hat{k}_{1,x}(\mathrm{N}(\mathfrak{p})) \neq 0$ est non vide : il existe un idéal premier $\mathfrak{p}$ tel que $\left[\frac{L/K}{\mathfrak{p}}\right] = C$, et tel que $\mathrm{N}(\mathfrak{p}) \leqslant x^4 = d_L^{974592}$ soit un nombre premier.

Si $\sqrt{1-\beta_0} \leqslant \frac{1}{1536\ln\left(d_L^7 2^{n_L/4} e^{26n_L+32}\right)}$ **:** dans ce cas,

$$\ln\left(1536(1-\beta_0)\ln\left(d_L^7 2^{n_L/4}e^{26n_L+32}\right)\right) \leqslant \frac{1}{2}\ln\left(1-\beta_0\right),$$

et par conséquent, par le théorème 2.24,

$$\beta \leqslant 1 + \frac{1}{485760}\frac{\ln(1-\beta_0)}{\ln(d_L)}$$

pour tout zéro $\rho = \beta + i\gamma \neq \beta_0$ of ζ_L tel que $|\gamma| \leqslant 1$. Alors,

$$\begin{aligned}
k_{2,x}(1) - \sum_\rho |k_{2,x}(\rho)| &= k_{2,x}(1) - k_{2,x}(\beta_0) - \sum_{|\mathrm{Im}(\rho)|<1} |k_{2,x}(\rho)| - \sum_{|\mathrm{Im}(\rho)|\geqslant 1} |k_{2,x}(\rho)| \\
&\geqslant \frac{x^2}{10}\min(1,(1-\beta_0)\ln(x)) - x^2(1-\beta_0)^{\frac{1}{485760}\frac{\ln(x)}{\ln(d_L)}} n(1) \\
&\quad - \int_1^\infty \frac{\mathrm{d}n(u)}{x^{u^2-2}} \\
&\geqslant \frac{x^2}{10}\min(1,(1-\beta_0)\ln(x)) - 244x^2(1-\beta_0)^{\frac{1}{485760}\frac{\ln(x)}{\ln(d_L)}}\ln(d_L) \\
&\quad - 306x\ln(d_L),
\end{aligned}$$

ce qui induit finalement, en combinant (3.3) et (3.4), l'estimation finale que nous voulions :

$$\begin{aligned}
\sum_{\substack{\mathfrak{p}\in\Pi_C \\ \mathrm{N}(\mathfrak{p})<x^{10}}} \ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p})) \geqslant \frac{|C|}{|G|}\Big(&\frac{x^2}{10}\min(1,(1-\beta_0)\ln(x)) \\
&- 244x^2(1-\beta_0)^{\frac{1}{485760}\frac{\ln(x)}{\ln(d_L)}}\ln(d_L) \\
&- 742x\ln(d_L) - 3301x^{3/4}\sqrt{\ln(x)}\Big)
\end{aligned}$$

Posons $c = 2812632$ et $x = d_L^c$. Alors, toutes les contributions négatives ci-dessus sont supérieures à $-\frac{1}{60}x^2 \min(1, (1-\beta_0)\ln(x))$, et on a :

$$\sum_{\substack{\mathfrak{p}\in\Pi_C \\ \mathrm{N}(\mathfrak{p})<x^{10}}} \ln(\mathrm{N}(\mathfrak{p}))\hat{k}_{2,x}(\mathrm{N}(\mathfrak{p})) \geqslant \frac{|C|}{|G|}\frac{x^2}{20}\min(1, (1-\beta_0)\ln(x)) > 0.$$

Ceci prouve que l'ensemble des idéaux premiers de Π_C tels que $\mathrm{N}(\mathfrak{p}) < x^{10}$ est non vide : il existe un idéal premier $\mathfrak{p}$ tel que $\left[\frac{L/K}{\mathfrak{p}}\right] = C$, et tel que $\mathrm{N}(\mathfrak{p}) \leqslant x^{10} = d_L^{28126320}$ soit un nombre premier. Le théorème 3.1 est donc, finalement, vrai pour toute valeur du zéro de Siegel potentiel.

Deuxième partie

Problème de Lehmer elliptique

Chapitre 4

Intersection arithmétique

« Il m'avait semblé seulement que je sentais, confiné au fond de mon intellect, le germe obscur d'une idée supérieure à toutes les formules de bonne femme dont j'avais récemment parcouru le dictionnaire. Mais ce n'était que l'idée d'une idée, quelque chose d'infiniment vague. »
Charles Baudelaire, *Le Spleen de Paris*

4.1 Motivation

La géométrie d'Arakelov est un ensemble de techniques géométriques consacrées à l'étude de problèmes diophantiens, nées du vœu de transposer des résultats connus pour des courbes algébriques définies sur des corps de fonctions au cas des corps de nombres (tels que la conjecture de Mordell, désormais un théorème de Faltings, qui énonce que l'ensemble des points rationnels d'une courbe de genre au moins deux est fini).

Les définitions et propriétés élémentaires de l'intersection arithmétique sont, ici, données dans le cas général d'une surface arithmétique, afin que le lecteur puisse adapter à sa convenance notre étude à d'autres situations (bien que notre manuscrit n'invoque la théorie de l'intersection arithmétique que sur des surfaces elliptiques). Rappelons sa définition.

Définition 4.1 (Surface arithmétique)**.** Une surface arithmétique est un morphisme propre et plat entre deux schémas $\mathcal{X} \to B$, où $\mathcal{X}$ est régulier et B le spectre de l'anneau des entiers d'un corps de nombres K, de sorte que la fibre générique X est une courbe géométriquement connexe.

Conformément à cette définition, B désignera toujours, dans ce chapitre, le spectre de l'anneau des entiers d'un corps de nombres K.

Une façon naïve de définir l'intersection de deux diviseurs sur une surface arithmétique, que nous n'adopterons pas sans quelques ajustements mais qui n'est pas dépourvue d'intérêt pour autant, est de regarder au-dessus de chaque fibre si les diviseurs se coupent (avec multiplicité), et de sommer la contribution en chaque intersection pour obtenir leur nombre d'intersection global. Plus précisément, si $\mathcal{X} \to B$ est une surface arithmétique et $\mathcal{D}_1$, $\mathcal{D}_2$ deux diviseurs irréductibles et distincts, d'équations locales f_1 et f_2 en $x \in \mathcal{X}$ (c'est-à-dire : ce sont des uniformisantes de $\mathscr{O}_{\mathcal{X},x}(-\mathcal{D}_1)_x$ et $\mathscr{O}_{\mathcal{X},x}(-\mathcal{D}_2)_x$ respectivement), on définit l'intersection locale en x (ou indice de multiplicité), qu'on note

$$i_x(\mathcal{D}_1, \mathcal{D}_2), \tag{4.1}$$

comme étant la longueur du $\mathscr{O}_{\mathcal{X},x}$-module $\mathscr{O}_{\mathcal{X},x}/(f_1, f_2)$. On somme alors les intersections locales en tous les points x, pondérées avec le logarithme du cardinal du corps résiduel en x, pour obtenir l'intersection globale $\mathcal{D}_1 \cdot \mathcal{D}_2$ (pour deux diviseurs distincts, il n'y a qu'un nombre fini d'intersections locales non nulles). Ceci définit par linéarité, *si l'on impose à $\mathcal{D}_2$ d'être vertical*, un accouplement bilinéaire sur l'ensemble des diviseurs, symétrique si l'on prend également $\mathcal{D}_1$ vertical, et invariant par relation d'équivalence linéaire « à gauche » : si $\mathcal{D}_1$ est linéairement équivalent à $\mathcal{D}'_1$, alors $\mathcal{D}_1 \cdot \mathcal{D}_2 = \mathcal{D}'_1 \cdot \mathcal{D}_2$. Pour les détails, voir par exemple [Lan88], chapitre III, ou [Liu02] section 9.1. Il nous manque toutefois une propriété importante, à cause de la proposition suivante :

Proposition 4.2 (Intersection avec une section, [Liu02], proposition IX.1.30)**.** *Soit $\mathcal{X} \to B$ une surface arithmétique de fibre générique X. Pour tout point fermé $P \in X$ d'adhérence $\mathcal{P}$ dans $\mathcal{X}$ et pour tout point fermé $\mathfrak{p} \in B$, on a :*

$$\mathcal{P} \cdot \mathcal{X}_\mathfrak{p} = [K(P) : K(B)] \ln(|k(P)|),$$

où $\mathcal{X}_\mathfrak{p}$ est la fibre de $\mathcal{X}$ au-dessus de $\mathfrak{p}$.

Outre la conséquence utile qu'une section coupe nécessairement chaque fibre en un point rationnel et lisse, on a l'information moins heureuse qu'on ne peut pas avoir l'invariance par équivalence linéaire : on a $\mathcal{P} \cdot \mathcal{X}_\mathfrak{p} \neq 0$ alors que $\mathcal{X}_\mathfrak{p}$ est un diviseur principal. C'est pourtant une propriété qu'on attend d'une « bonne » théorie de l'intersection, mais ce défaut n'est pas tant une surprise que cela : dans le cas des corps de fonctions, notre base B correspondrait à une courbe affine et avec une telle base, nos variétés ne seraient pas complètes. Dans le cas affine, on recourt à la géométrie projective pour formuler convenablement une théorie de l'intersection. Ici, au moins formellement, on sait comment « compléter » la base B : en y adjoignant les places infinies M_K^∞. Il faudrait alors pouvoir étendre $\mathcal{X}$ en un schéma complet sur $B \cup M_K^\infty$, qui comprendrait de nouveaux diviseurs, ne seraient-ce que les fibres de la projection $\mathcal{X} \to B$ au-dessus des places infinies. C'est ce qui motive l'introduction des diviseurs d'Arakelov dans la section suivante.

4.2 Intersection locale

Par commodité, on note dorénavant $\sigma : K \hookrightarrow \mathbb{C}$ les plongements de K dans $\mathbb{C}$, et $\sigma : L \hookrightarrow \mathbb{C}$ les morphismes de corps $\sigma : L \to \mathbb{C}$ qui fixent K (ce dernier aspect est donc désormais implicite). On suppose que $\mathcal{X}$ est une surface arithmétique de genre $g > 0$.

Définition 4.3 (Diviseur d'Arakelov)**.** Soit $\mathcal{X} \to B$ une surface arithmétique.

1. Un diviseur d'Arakelov sur $\mathcal{X}$ est une combinaison linéaire formelle à coefficients entiers de sous-schémas fermés irréductibles de dimension 1 (c'est-à-dire des diviseurs de Weil) plus une contribution $\sum_{\sigma:K\hookrightarrow\mathbb{C}} \alpha_\sigma F_\sigma$, où les α_σ sont réels, et les F_σ des symboles formels associés aux « fibres à l'infini », nommément $\mathcal{X}_\sigma = (\mathcal{X} \otimes_{\sigma,B} \mathbb{C})(\mathbb{C})$. Il y a une structure naturelle de groupe sur l'ensemble des diviseurs d'Arakelov, noté $\widehat{\mathrm{Div}}(\mathcal{X})$.
2. À toute fonction rationnelle non nulle f définie sur $\mathcal{X}$, on peut associer un diviseur d'Arakelov $(f) = (f)_{\mathrm{fin}} + (f)_\infty$, où $(f)_{\mathrm{fin}}$ est le diviseur de f au sens traditionnel, et
$$(f)_\infty = -\sum_{\sigma:K\hookrightarrow\mathbb{C}} \left(\int_{\mathcal{X}_\sigma} \ln(|f|_\sigma)\mu_\sigma \right) F_\sigma, \tag{4.2}$$
où μ_σ est la (1,1)-forme fondamentale sur $\mathcal{X}_\sigma$ (définie plus tard, voir (4.4)). Un tel diviseur est un diviseur principal d'Arakelov.
3. Deux diviseurs d'Arakelov sont linéairement équivalents si leur différence est un diviseur principal d'Arakelov. On note $\widehat{\mathrm{Cl}}(\mathcal{X})$ le groupe d'Arakelov des diviseurs de $\mathcal{X}$ modulo la relation d'équivalence linéaire.

Remarque 4.4. La contribution à l'infini $-\int_{\mathcal{X}_\sigma} (\ln(|f|_\sigma)\mu_\sigma)\, F_\sigma$ est supposée être le pendant archimédien de la contribution de la fibre au-dessus d'un idéal premier $\mathfrak{p}$ qui est de la forme $\sum_\Gamma \mathrm{ord}_\Gamma(f) \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))\Gamma$, où Γ parcourt l'ensemble des composantes irréductibles de $\mathcal{X}_\mathfrak{p}$ et ord_Γ est la valuation discrète sur le germe en Γ (c'est-à-dire l'union des germes de tous les points sur Γ). La fibre « formelle » à l'infini F_σ doit être interprétée comme une fibre « infiniment dégénérée », où chaque point $P \in \mathcal{X}_\sigma$ est une composante irréductible, de sorte que la valuation v_P de f le long de cette « composante » est donnée par la valuation $\mathrm{ord}_P(f) = -\ln(|f(P)|_\sigma)$. Intégrer sur $\mathcal{X}_\sigma$ donne la valuation sur toute la fibre.

Nous remotiverons la définition d'un diviseur principal au sens d'Arakelov plus tard, quand nous présenterons l'intersection arithmétique globale du point de vue des fibrés munis de métriques hermitiennes. Bien entendu, le groupe des diviseurs de Weil s'injecte dans le groupe des diviseurs d'Arakelov, en prenant pour nulles les contributions aux places infinies. On introduit à présent les prérequis nécessaires à la

définition de l'intersection en une place infinie. Aux places infinies, les fibres seront des surfaces de Riemann compactes, et la notion de proximité v-adique passe donc par des fonctions analytiques.

Soit X une surface de Riemann compacte de genre $g > 0$. L'espace vectoriel $\Gamma(X, \Omega^1)$ est de dimension g, muni d'un produit scalaire hermitien donné par

$$\langle \omega | \omega' \rangle = \frac{i}{2} \int_X \omega \wedge \bar{\omega}' \tag{4.3}$$

Soit $(\omega_1, \ldots, \omega_g)$ une base orthonormée de $\Gamma(X, \Omega^1)$. On pose

$$\mu = \frac{i}{2g} \sum_{k=1}^{g} \omega_k \wedge \bar{\omega}_k. \tag{4.4}$$

La (1,1)-forme μ ne dépend pas du choix de la base orthonormée, et elle est d'intégrale égale à 1. Enfin, on pose $\partial\bar{\partial} f = \frac{\partial^2 f}{\partial z \partial \bar{z}} \mathrm{d}z \wedge \mathrm{d}\bar{z}$ pour toute fonction f de classe C^∞, où z est une coordonnée locale.

Théorème 4.5 (Fonction de Green-Arakelov)**.** *Il existe une unique fonction $G : X \times X \to \mathbb{R}_+$ vérifiant les trois propriétés suivantes :*

1. *La fonction $(P, Q) \to (G(P, Q))^2$ est de classe C^∞ sur $X \times X$, et G ne s'annule que sur la diagonale. Pour $P \in X$ fixé, U un voisinage ouvert de P et z une coordonnée locale sur U, on peut écrire $\ln(G(P, Q)) = \ln(|z(Q)|) + f(Q)$ pour $P \neq Q \in U$, où f est une fonction C^∞.*
2. *Pour tout $P \in X$, on a $\partial_Q \bar{\partial}_Q \left(\ln(G(P, Q))^2\right) = 2i\pi\mu(Q)$ pour $Q \neq P$.*
3. *Pour tout $P \in X$, on a $\int_X \ln(G(P, Q))\mu(Q) = 0$.*

On note $g = \ln(G)$, et on l'appelle fonction de Green, ou de Green-Arakelov.

La démonstration de leur existence, d'abord établie dans [Ara74], provient de méthodes issues de la théorie des équations aux dérivées partielles, et ne donne pas de moyen de les construire explicitement.

Remarque 4.6. Si $D = \sum_P m_P(P)$ est un diviseur de X et Q un point, on pose $g(D, Q) = \sum_P m_P g(P, Q)$. Il est immédiat que $\partial\bar{\partial} g(D, \cdot) = i\pi \deg(D)\mu$.

Le laplacien défini par rapport à la forme μ est l'opérateur de $\mathrm{C}^\infty(X)$ tel que $i\pi\Delta(f)\mu = \partial\bar{\partial} f$. Utilisant la formule de Stokes, on montre que si $f \in \mathrm{C}^\infty(X)$ est d'intégrale nulle sur X, alors

$$f(P) = \int_X (-g(P, Q))\Delta(f(Q))\mathrm{d}\mu(Q) \tag{4.5}$$

pour tout $Q \in X$. On peut en déduire que si $0 = \lambda_0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdot \leqslant \lambda_n \leqslant \cdots$ sont les valeurs propres du laplacien Δ de $\mathrm{L}^2(X, \mu)$, et $(\varphi_n)_{n \geqslant 0}$ une base orthonormée de $\mathrm{L}^2(X, \mu)$, alors nous avons au moins formellement un développement de Fourier

$$g(P, Q) \sim -\sum_{n=1}^{\infty} \frac{1}{\lambda_n} \varphi_n(P) \overline{\varphi_n(Q)}.$$

Pour réellement écrire une égalité entre ces deux membres, il est nécessaire de convoler g avec une fonction bien choisie : on utilisera cette approche pour démontrer le lemme d'Elkies pondéré dans le chapitre 6. On en tire, par ailleurs, la symétrie de g en P et Q.

Définition 4.7 (Intersections locales)**.** Soient $\mathcal{X} \to B$ une surface arithmétique, $\mathcal{D}_1$ et $\mathcal{D}_2$ deux diviseurs irréductibles et distincts de $\mathcal{X}$, et v une place de K. Alors,

— si v est une place ultramétrique, associée à l'idéal premier $\mathfrak{p}$, on pose

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\mathfrak{p}} = \sum_{x \in \mathcal{X}_{\mathfrak{p}}} i_x(\mathcal{D}_1, \mathcal{D}_2) \ln(|k(x)|),$$

où l'indice i_x a été introduit en (4.1) et la somme est sur les points fermés ;

— si v est une place archimédienne, associée au plongement $\sigma : K \hookrightarrow \mathbb{C}$, $\mathcal{D}_1$ un diviseur horizontal et $\mathcal{D}_2$ une section $\mathrm{Spec}(\mathcal{O}_K) \to \mathcal{X}$, on pose

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_\sigma = -n_v g_\sigma(D_1^\sigma, D_2^\sigma),$$

où $n_v = [K_v : \mathbb{Q}_v]$, g_σ est la fonction de Green-Arakelov sur $\mathcal{X}_\sigma$ étendue par linéarité grâce à la remarque 4.6, et $D^\sigma = \mathcal{D} \otimes_{\sigma, B} \mathbb{C}$ pour tout $\mathcal{D}$ (cette intersection n'est donc pas nécessairement positive, même pour des diviseurs effectifs) ;

— si v est une place archimédienne, et si $\mathcal{D}_1$ ou $\mathcal{D}_2$ est un diviseur de Weil vertical, on pose

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = 0;$$

— si v est une place archimédienne, $\mathcal{D}_1$ un diviseur horizontal et F_σ une fibre à l'infini, on pose

$$\langle \mathcal{D}_1, F_\sigma \rangle_v = \begin{cases} \deg(\mathcal{D}_{1|K}) & \text{si } v \text{ est associée au plongement } \sigma; \\ 0 & \text{sinon.} \end{cases}$$

Remarque 4.8. Il y a plusieurs normalisations possibles ; dans [Lan88], la fonction g_σ est normalisée de sorte que $g_\sigma = 2\lambda_v$, où λ_v est une fonction de Néron, tandis qu'avec notre définition nous aurons $g_\sigma = -\lambda_v$ dans la section 5.4.

Remarque 4.9. Voici comment traduire, plus concrètement, l'intersection de deux points algébriques en une place finie. D'après [Lan88] (propriété « INT 3 » page 73), la somme des intersections en toutes les places finies de deux diviseurs horizontaux donnés par les adhérences $\mathcal{P}_1$, $\mathcal{P}_2$ de deux points fermés $P_1, P_2 \in X$ égale :

$$\sum_{\mathfrak{p}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\mathfrak{p}} = \sum_{\sigma : L \hookrightarrow \bar{L}} \mathrm{ord}_{P_1^\sigma}(\mathcal{P}_2) \ln(|k(P_1^\sigma)|), \tag{4.6}$$

où $L = K(P_1)$. Autrement dit, comme $\mathcal{P}_2 \otimes \bar{K}_{\mathfrak{p}}$ se décompose en somme de conjugués P_2^τ, la quantité $\mathrm{ord}_{P_1^\sigma}(\mathcal{P}_2)$ est strictement positive si, et seulement si un des conjugués P_2^τ coïncide avec P_1^σ modulo un idéal maximal.

Si les définitions semblent très différentes dans les cas ultramétriques et archimédiens, elles sont pourtant reliées par de nombreuses propriétés communes (dans les deux cas, par exemple, l'intersection mesure essentiellement le logarithme de la distance v-adique sur $X(\bar{K}_v)$). C'est probablement la recherche d'une intersection vérifiant les propriétés suivantes qui a motivé la définition de l'intersection en une place archimédienne à l'aide des fonctions de Green-Arakelov.

Proposition 4.10 ([Lan88], III.5)**.** *Pour toute place v, la restriction de l'intersection locale aux diviseurs de Weil sur $\mathcal{X} \to B$ de degré nul vérifie les trois propriétés suivantes :*

1. *Elle est bilinéaire et symétrique.*
2. *Si $\mathcal{D}_1$ est l'adhérence d'un diviseur principal $\mathrm{div}(f) \in \mathrm{Div}(X)$, et $\mathcal{D}_2$ un diviseur de Weil de degré nul dont le support est génériquement disjoint de celui de $\mathcal{D}_1$, on a*
$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = -n_v \ln(|f(\mathcal{D}_{2|K})|_v),$$
où $f(D) = \prod_i f(P_i)^{n_i}$ pour tout diviseur $D = \sum_i n_i(P_i) \in \mathrm{Div}^0(X)$ dont le support est disjoint de celui de $\mathrm{div}(f)$.
3. *Pour $P_0 \in X(K) \setminus \mathrm{supp}\left(\mathcal{D}_{|K}\right)$ fixé, d'adhérence $\mathcal{P}_0$ dans $\mathcal{X}$, l'application $\mathcal{X}(\mathcal{O}_K) \setminus \mathrm{supp}(\mathcal{D}) \to \mathbb{R}$ définie par*
$$\mathcal{P} \mapsto \langle \mathcal{D}, \mathcal{P} - \mathcal{P}_0 \rangle_v$$
est continue (pour la topologie v-adique) et localement bornée.

On voit un autre rapprochement dans l'annexe A.2, entre l'intersection en une place archimédienne et l'intersection en une place de mauvaise réduction multiplicative.

4.3 Intersection globale

En sommant l'ensemble des intersections locales, on obtient une intersection globale qui s'étend, en vérité, à l'ensemble des diviseurs d'Arakelov.

Théorème 4.11 (Intersection globale)**.** *Il existe un accouplement bilinéaire symétrique* $\langle \cdot, \cdot \rangle : \widehat{\mathrm{Div}(\mathcal{X})} \times \widehat{\mathrm{Div}(\mathcal{X})} \to \mathbb{R}$*, dit accouplement d'intersection. Il se factorise à travers la relation d'équivalence linéaire, et définit donc un accouplement d'intersection* $\widehat{\mathrm{Cl}(\mathcal{X})} \times \widehat{\mathrm{Cl}(\mathcal{X})} \to \mathbb{R}$*. Si* $\mathcal{D}_1$ *et* $\mathcal{D}_2$ *sont deux diviseurs d'Arakelov sans composante commune, on a* $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \sum_{v \in M_K} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v$*.*

Voyons, dans les grandes lignes, comment nous avons réussi à retrouver l'invariance par relation d'équivalence linéaire : si $(f) = (f)_{\mathrm{fin}} + (f)_\infty$ est un diviseur principal d'Arakelov et $\mathcal{D}$ une section non contenue dans le support de f, alors :

$$\begin{aligned}\langle (f), \mathcal{D} \rangle &= \sum_{v \in M_K^0} \langle (f)_{\mathrm{fin}}, \mathcal{D} \rangle_v + \sum_{v \in M_K^\infty} \langle (f)_{\mathrm{fin}}, \mathcal{D} \rangle_v + \sum_{v \in M_K^\infty} \langle (f)_\infty, \mathcal{D} \rangle_v \\ &= \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f_{|\mathcal{D}}) \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) + \sum_{\sigma : K \hookrightarrow \mathbb{C}} g_\sigma((f)_{\mathrm{fin}}, D^\sigma) - \sum_{\sigma : K \hookrightarrow \mathbb{C}} \left(\int_{\mathcal{X}_\sigma} \ln(|f|_\sigma) \mu_\sigma \right),\end{aligned}$$

et il nous reste à calculer $g_\sigma((f)_{\mathrm{fin}}, D^\sigma)$: comme $\partial\bar{\partial} g_\sigma((f)_{\mathrm{fin}}, \cdot) = \partial\bar{\partial} \ln(|f|_\sigma) = 0$ hors de $(f)_{\mathrm{fin}}$ (voir la remarque 4.6), on a $g_\sigma((f)_{\mathrm{fin}}, D^\sigma) = \ln(|f(D^\sigma)|_\sigma) + c$ pour une certaine constante c, qu'on détermine après intégration de l'égalité établie à l'instant pour trouver $c = -\int_{\mathcal{X}_\sigma} \ln(|f|_\sigma)\mu$. Reporter cette expression de $g_\sigma((f)_{\mathrm{fin}}, D^\sigma)$ ci-dessus permet d'obtenir zéro par la formule du produit (qui est donc l'ingrédient essentiel qui manquait, lorsqu'on se contentait des places finies, pour avoir l'invariance par relation d'équivalence linéaire).

Remarque 4.12. Par la deuxième propriété de la proposition 4.10, la restriction de ce même accouplement d'intersection aux diviseurs de Weil de degré nul vérifie également l'invariance par relation d'équivalence linéaire au sens classique.

Remarque 4.13. Selon nos affinités et nos besoins, on peut adopter un autre point de vue, plus proche des diviseurs de Cartier (et permettant, peut-être, de mieux comprendre ce qu'il se passe aux places infinies), même si on peut s'en passer dans ce texte. En effet, on peut aussi décrire les fonctions de Green-Arakelov en disant que si D_1, D_2 sont deux points de X, alors $g(D_1, D_2)$ est le logarithme de la norme en D_1 de la section constante 1 de $\mathcal{O}_X(D_2)$, où la norme est induite par le produit scalaire (4.3) sur $\mathcal{O}_X(D_2)$. Ceci fournit à $\mathcal{O}_{\mathcal{X}_v}(D)$ une métrique hermitienne pour tout point D de $\mathcal{X}_v$ (v archimédienne), puis pour tout diviseur D de $\mathcal{X}_v$ par tensorisation. Pour la partie arithmétique : si $\mathcal{D} = \mathcal{D}_f + \mathcal{D}_\infty$ est un diviseur d'Arakelov, où $\mathcal{D}_f$ est un diviseur de Weil et $\mathcal{D}_\infty$ à support dans les fibres F_σ, on définit $\mathcal{O}_{\mathcal{X}}(\mathcal{D})$ comme le fibré en droites traditionnel $\mathcal{O}_{\mathcal{X}}(\mathcal{D}_f)$ muni des métriques hermitiennes induites sur $\mathcal{X}_v$:

si $\mathcal{D}_\infty = \sum_{v \in M_K^\infty} r_v F_v$, on multiplie la métrique sur les $\mathcal{O}_{\mathcal{X}_v}(\mathcal{D}_f)$ par $\exp(-r_v)$. Voyons comment décrire l'intersection à présent, partant de ce point de vue : si $\mathcal{D}_1$ est l'image d'une section $s : B \to \mathcal{X}$, alors $s^*(\mathcal{O}_\mathcal{X}(\mathcal{D}_2))$ est un module projectif de rang 1 sur $\mathcal{O}_K$, muni de métriques hermitiennes aux places infinies. Soit $s_0 \in s^*(\mathcal{O}_X(\mathcal{D}_2))$ non nul. On peut prendre pour définition de l'intersection de $\mathcal{D}_1 = s(B)$ et $\mathcal{D}_2$:

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \deg(s^*(\mathcal{O}_\mathcal{X}(\mathcal{D}_2))) = \ln\left(\operatorname{card}\left(\frac{s^*(\mathcal{O}_\mathcal{X}(\mathcal{D}_2))}{(s_0)}\right)\right) - \sum_{v \in M_K^\infty} n_v \ln(|s_0|_v). \quad (4.7)$$

Un avantage de cette définition (qui ne dépend pas du choix de s_0, et coïncide avec la précédente : voir [Lan88], théorème IV.3.4) est qu'elle convient y compris pour $\mathcal{D}_1$ et $\mathcal{D}_2$ qui admettent une composante commune, et ne dépend clairement pas de la classe d'isomorphisme de $\mathcal{O}_\mathcal{X}(\mathcal{D}_2)$ (en tant que fibré muni de métriques hermitiennes).

Ceci étant dit, on peut justifier la définition de la partie infinie d'un diviseur principal d'Arakelov (f) : la multiplication par f induit un isomorphisme de fibrés $\mathcal{O}_\mathcal{X}((f)_{\text{fin}}) \to \mathcal{O}_\mathcal{X}$. On choisit alors $(f)_\infty$ de sorte que cet isomorphisme soit également une isométrie $\mathcal{O}_\mathcal{X}((f)) \to \mathcal{O}_\mathcal{X}$ aux places infinies : ceci fournira immédiatement l'invariance par équivalence linéaire. D'après la discussion qui précède, ceci impose $(f)_\infty = -\sum_{v \in M_K^\infty} n_v \left(\int_{\mathcal{X}_v} \ln(|f|_v)\mu\right) F_v$.

Pour garder en tête la base de la surface arithmétique, on annote parfois le nombre d'intersection $\langle \cdot, \cdot \rangle_K$: cela permet de s'y retrouver quand on considère l'intersection de points algébriques (au lieu des points rationnels vus comme sections) ou qu'on fait des changements de base. La proposition suivante permet de constater qu'en un certain sens, l'intersection arakelovienne et le changement de base commutent.

Proposition 4.14 (Changement de base, [Lan88], théorème IV.1.2)**.** *Soit $\mathcal{X} \to B$ une surface arithmétique de fibre générique X. Considérons une extension de corps finie L/K et notons $\mathcal{X}'$ la désingularisation minimale de $X \otimes_K \operatorname{Spec}(L)$. Alors, si r est le morphisme canonique $\mathcal{X}' \to \mathcal{X}$, on a, pour tous diviseurs $\mathcal{D}_1$, $\mathcal{D}_2$ de $\mathcal{X}$:*

$$\langle r^*(\mathcal{D}_1), r^*(\mathcal{D}_2) \rangle_L = [L : K] \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_K. \quad (4.8)$$

Remarque 4.15. Dans le cas des courbes de genre un, cette proposition se généralise : si $f : X \to X'$ est une isogénie, elle ne s'étend pas nécessairement en un morphisme $\mathcal{X} \to \mathcal{X}'$; il faut éclater un certain nombre (fini) de points fermés de $\mathcal{X}$. Dans ce cas, pour tous diviseurs $\mathcal{D}_1, \mathcal{D}_2$ de $\mathcal{X}'$, on a $\langle f^*(\mathcal{D}_1), f^*(\mathcal{D}_2) \rangle = \deg(f) \cdot \langle \mathcal{D}_1, \mathcal{D}_2 \rangle$ (voir [Szp90], lemme 1).

Remarque 4.16. Pour tout diviseur $\mathcal{D}_1$, il existe une extension finie L/K telle que $\mathcal{D}_1$ se « décompose » sur L en somme de sections et de composantes de fibres. On peut donc de la sorte définir l'intersection $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle$ pour tout $\mathcal{D}_1$ grâce à la définition (4.7) et à la formule du changement de base.

Mentionnons le résultat suivant, qui est très pratique pour calculer les auto-intersections :

Théorème 4.17 (Formule d'adjonction,[Lan88], corollaire 5.5)**.** *Soit $\mathcal{X} \to B$ une surface arithmétique et $\mathcal{Q} : \mathrm{Spec}(\mathcal{O}_L) \to \mathcal{X}$ un diviseur horizontal. Notant $\mathrm{K}_{\mathcal{X}/B}$ le diviseur canonique (d'Arakelov) de $\mathcal{X}/B$, on a :*

$$\langle \mathcal{Q}, \mathrm{K}_{\mathcal{X}/B} \rangle_K + \langle \mathcal{Q}, \mathcal{Q} \rangle_K = \mathrm{d}_{\mathcal{Q}/L} - \sum_{v \in M_K^\infty} n_v \sum_{\substack{\sigma,\tau : L \hookrightarrow \mathbb{C} \\ \sigma,\tau | v \\ \sigma \neq \tau}} g_v(Q^\sigma, Q^\tau), \tag{4.9}$$

où $\mathrm{d}_{\mathcal{Q}/L} \geqslant 0$ est le logarithme du discriminant de $\mathcal{Q}/L$ (voir [Lan88], page 97, pour une définition). En particulier, si $L = K$, le membre de droite est nul et on a l'égalité $\langle \mathcal{Q}, \mathcal{Q} \rangle_K = -\langle \mathcal{Q}, \mathrm{K}_{\mathcal{X}/B} \rangle_K$.

Concluons ce chapitre sur un résultat classique.

Théorème 4.18 (Théorème de l'indice de Hodge, [Fal84], théorème 4)**.** *Le nombre d'intersection est semi-défini négatif sur l'espace des diviseurs d'Arakelov qui sont combinaisons linéaires de composantes irréductibles des fibres aux places finies, et les multiples (rationnels) des fibres sont les seuls diviseurs de cet espace à être d'auto-intersection nulle. La signature de la forme induite par le nombre d'intersection n'a qu'un seul signe « + ».*

On peut réécrire matriciellement ce théorème : soit M la matrice d'incidence $((\langle \Gamma_i, \Gamma_j \rangle))_{0 \leqslant i,j \leqslant r}$, où les Γ_i sont les différentes composantes irréductibles d'une fibre à une place finie, à des multiplicités notées n_i. D'après le théorème de l'indice de Hodge, la forme quadratique $X \mapsto {}^t XMX$ est semi-définie négative sur $\mathbb{Q}$, et son noyau est de dimension un, engendré par le vecteur $(n_0, \ldots, n_r)$. En particulier, tous les mineurs de M sont inversibles.

On utilisera ce théorème dans la section A.2, alors qu'on voudra exprimer un certain diviseur vertical comme combinaison linéaire des composantes irréductibles des fibres ; les coefficients de cette combinaison seront solutions d'un système linéaire dont l'inversibilité sera assurée par le théorème de l'indice de Hodge.

Chapitre 5

Courbes elliptiques

« Arithmétique ! algèbre ! géométrie ! trinité grandiose ! triangle lumineux ! Celui qui ne vous a pas connues est un insensé ! »
Comte de Lautréamont, *Les Chants de Maldoror* (Éloge des mathématiques)

5.1 Définitions, propriétés générales

Une courbe elliptique est essentiellement une cubique lisse dans le plan projectif. Afin de minimiser les dépendances en la courbe elliptique dans les résultats que l'on veut démontrer, on introduit dans cette section et les suivantes les propriétés les plus intrinsèques possible ; ceci permet par exemple de limiter la dépendance en l'équation de la courbe elliptique, *etc.* Nous exposons plus précisément les propriétés liées aux fibres d'un « bon » modèle d'une courbe elliptique (puisque les fibres jouent un rôle de premier plan dans les calculs d'intersections locales que nous avons en ligne de mire), donc liées aux types de réduction possibles d'une courbe elliptique, sans oublier de définir les notions et quantités qui apparaîtront dans l'inégalité (4).

Définition 5.1 (Courbe elliptique)**.** Une courbe elliptique est une paire (E, O), où E est une courbe projective lisse de genre un et O un point de E. La courbe elliptique est définie sur K si la courbe et le point sont définis sur K.

Si on veut une description plus concrète, le théorème de Riemann-Roch permet de démontrer que pareille courbe est isomorphe à une cubique lisse donnée par une équation de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{5.1}$$

où O est envoyé sur le « point à l'infini » [0,1,0] ou, si K est de caractéristique différente de 2 ou 3 (on travaillera essentiellement sur un corps de nombres),

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Définition 5.2. Soit E une courbe elliptique sur un corps de nombres K. Si E a pour équation (5.1), où tous les coefficients a_i sont entiers, on appelle

$$W = \mathrm{Proj}\left(\frac{\mathcal{O}_K[X,Y,Z]}{Y^2Z + (a_1X + a_3Z)YZ - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)}\right)$$

un modèle de Weierstrass pour E ; c'est un schéma sur $B = \mathrm{Spec}(\mathcal{O}_K)$.

Soient E/K une courbe elliptique et O son point rationnel fixé. Le théorème de Riemann-Roch, encore une fois, permet de démontrer que l'application

$$\kappa \ : \begin{cases} E & \to & \mathrm{Pic}^0(E) \\ P & \mapsto & (P) - (O) \end{cases}$$

est un isomorphisme. La loi de groupe sur $\mathrm{Pic}^0(E)$ en induit donc une sur E, d'élément neutre O. L'addition est caractérisée par $P+Q = R$ si, et seulement si $(P)+(Q)$ est linéairement équivalent à $(R) + (O)$. Pour tout P, on note $[-1]P$ l'inverse de P pour la loi $+$, c'est-à-dire le point tel que $([-1]P) + (P)$ soit linéairement équivalent à $2(O)$.

Théorème 5.3 ([HS00], théorème A.4.4.2)**.** *Soit E une courbe elliptique. Les applications $(P,Q) \mapsto P+Q$ et $P \mapsto [-1]P$ définies ci-dessus donnent à E une structure de groupe algébrique abélien, d'élément neutre O.*

Les points rationnels P, Q, $R \in E(K)$ sont colinéaires dans $\mathbb{P}^2$ si, et seulement si $P + Q + R = O$. Ce phénomène est illustré par la figure 5.2.

Pour tout n entier, on note $[n]$ l'application qui à P associe $[n]P = P + \cdots + P$ (n fois) si n est positif, et $[n]P = [-n]([-1]P)$ sinon. Ces endomorphismes sont les *multiplications par des entiers*. On note $E[n]$ leur noyau.

Définition 5.4 (Discriminant)**.** Soit E/K une courbe elliptique d'équation (5.1). Son discriminant $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ est défini par l'égalité

$$\Delta = \frac{1}{16}\mathrm{disc}\left(4(x^3 + a_2x^2 + a_4x + a_6) + (a_1x + a_3)^2\right)$$

pour K de caractéristique différente de 2 (pour K de caractéristique 2, on réduit modulo 2 le polynôme de $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ obtenu par le calcul de discriminant ci-dessus).

FIGURE 5.1 – Courbe elliptique d'équation projective $Y^2Z = X^3 + Z^3$ (vue d'artiste).

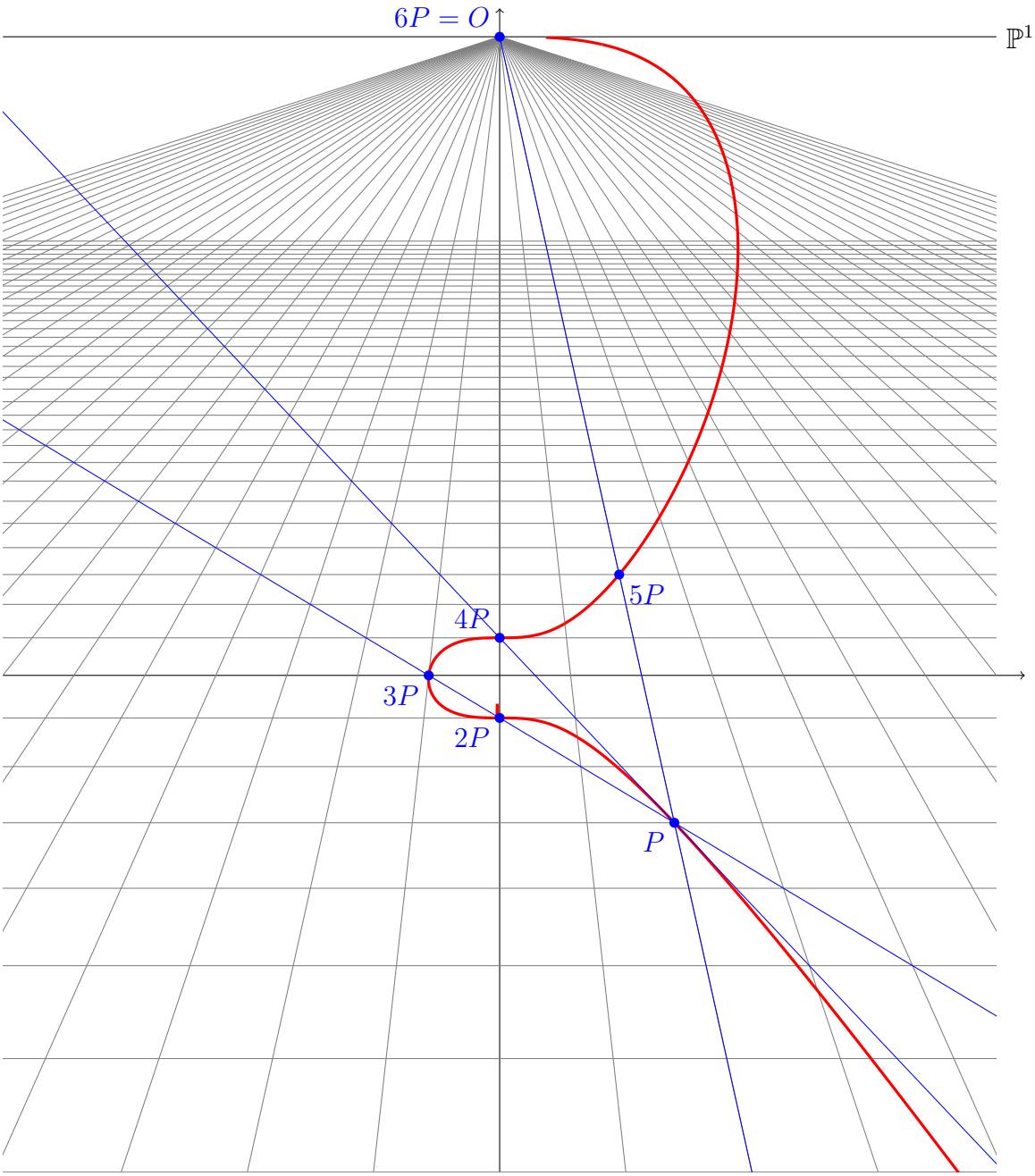
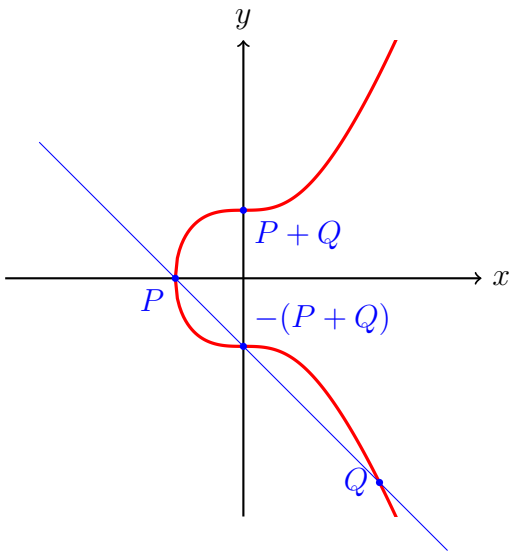


FIGURE 5.2 – Loi de groupe sur une courbe elliptique.



La lissité de E est équivalente à la non-annulation de Δ, et fait du discriminant une quantité tout à fait digne d'intérêt, comme nous le verrons.

La classe d'isomorphisme sur $\bar{K}$ d'une courbe elliptique E/K est caractérisée par une fraction rationnelle en les coefficients d'une équation intégrale de E, qu'on appelle le j-invariant et qu'on note $j_E \in K$. Nous n'aurons pas besoin de définition plus précise dans notre exposé ; le lecteur intéressé peut se tourner vers [Sil09] par exemple.

En vue d'appliquer la théorie de l'intersection arithmétique, exposée brièvement dans le chapitre précédent, aux courbes elliptiques, il convient de décrire la forme des fibres aux places finies et « à l'infini ». La proposition suivante permet d'y voir plus clair pour les fibres infinies ; nous verrons le cas de certaines fibres finies dans la proposition 5.13.

Proposition 5.5 (Uniformisation complexe,[Sil94], corollaire I.4.3)**.** *Soit $E/\mathbb{C}$ une courbe elliptique. Alors il existe un nombre complexe τ dans le demi-plan supérieur, qu'on peut même prendre dans le domaine $|\mathrm{Re}(\tau)| \leqslant \frac{1}{2}$, $\mathrm{Im}(\tau) \geqslant \frac{\sqrt{3}}{2}$, tel que les points complexes de E soient paramétrés par l'isomorphisme de groupes algébriques*

$$\varphi \ : \begin{cases} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \to & E(\mathbb{C}) \\ z & \mapsto & (\mathscr{P}_\tau(z), \mathscr{P}'_\tau(z)) \end{cases},$$

où $\mathscr{P}_\tau$ est la fonction de Weierstrass définie par la formule :

$$\mathscr{P}_\tau(z) = \frac{1}{z^2} + \sum_{\omega \in (\mathbb{Z}+\tau\mathbb{Z})\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Si on pose $\Delta(z) = (2\pi)^{12} e^{2i\pi z} \prod_{n=1}^{\infty} (1 - e^{2i\pi z n})^{24}$, alors $\Delta(\tau)$ est, à un facteur numérique près, égal à Δ_E.

Remarque 5.6. On peut aussi décrire la structure de l'ensemble des points rationnels d'une courbe elliptique E définie sur un corps de nombres K : on sait que $E(K)$ est un groupe abélien de type fini ; c'est le célèbre théorème de Mordell-Weil. Hélas, déterminer le rang, des générateurs ou le sous-groupe de torsion est pour l'instant un problème ouvert.

5.2 Mauvaise réduction et modèle minimal régulier

En arithmétique, l'utilité du recours à la réduction modulo un idéal premier n'est plus à justifier. Il est naturel de se demander si une courbe elliptique réduite en un certain idéal premier (c'est-à-dire, prosaïquement, en réduisant modulo un idéal premier une équation de Weierstrass qui définit la courbe) reste une courbe elliptique. Une telle réduction est effectivement possible, puisqu'un changement de variable adéquat permet de se ramener à une équation de la forme (5.1) où les coefficients a_i sont des entiers algébriques, mais il va de soi que l'information obtenue sera nulle si le choix de l'équation est mauvais : si E est le lieu d'annulation d'un certain polynôme à coefficients entiers, alors multiplier par deux le polynôme donne encore une équation qui décrit E, mais sa réduction modulo un idéal premier divisant 2 a pour équation $0 = 0$. On évite ces anomalies en privilégiant des équations de Weierstrass dites « minimales ». On suppose dans cette section que K est un corps de nombres.

Définition 5.7 (Modèle de Weierstrass minimal)**.** Soit E/K une courbe elliptique. Pour tout $\mathfrak{p}$, soit $v_\mathfrak{p}$ la valuation discrète de l'anneau local $\mathcal{O}_{K,\mathfrak{p}}$. Soit W un modèle de Weierstrass de E, de discriminant Δ. On dit que W est minimal en $\mathfrak{p}$ si $v_\mathfrak{p}(\Delta)$ est la plus petite valeur possible parmi les valuations des discriminants de toutes les équations intégrales de E. Il existe toujours un tel modèle minimal en une place donnée.

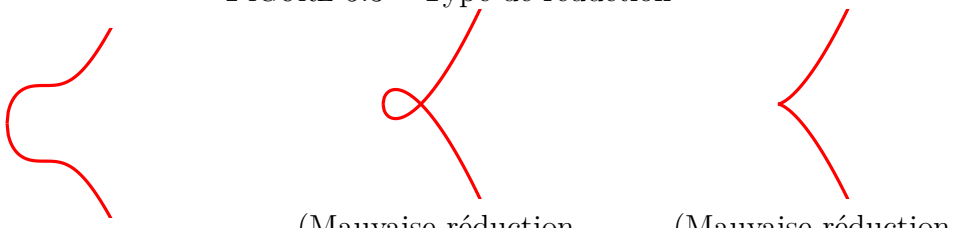
On est maintenant paré pour parler correctement de réduction en une place finie.

Proposition 5.8 (Bonne, mauvaise réduction, [Liu02], lemme 10.2.1)**.** *Soient E/K une courbe elliptique, $\mathfrak{p}$ un idéal maximal de K de corps résiduel k, et $W_\mathfrak{p}$ la fibre*

spéciale d'un modèle de Weierstrass pour E minimal en $\mathfrak{p}$; il s'agit d'une cubique géométriquement irréductible. Soit $W_{\mathfrak{p}}^0$ sa partie lisse. Alors, une de ces propriétés est vérifiée :

1. *La fibre $W_{\mathfrak{p}}$ est lisse sur k, c'est donc une courbe elliptique sur k : on dit que E/K a bonne réduction en $\mathfrak{p}$.*
2. *La fibre $W_{\mathfrak{p}}$ admet un unique point singulier p qui est rationnel sur k. Soit $\pi : W'_{\mathfrak{p}} \to W_{\mathfrak{p}}$ sa normalisation. Alors $W'_{\mathfrak{p}} \simeq \mathbb{P}^1_k$. De plus, on est dans un de ces trois cas de figure :*
   (a) *L'image réciproque $\pi^{-1}(p)$ contient exactement deux points k-rationnels, et $W_{\mathfrak{p}}^0 \simeq \mathbb{A}^1_k \setminus \{0\}$: on parle alors de mauvaise réduction multiplicative déployée.*
   (b) *L'image réciproque $\pi^{-1}(p)$ est un point de degré (séparable) 2 sur k : on parle alors de mauvaise réduction multiplicative non déployée.*
   (c) *L'image réciproque $\pi^{-1}(p)$ est un point k-rationnel, et $W_{\mathfrak{p}}^0 \simeq \mathbb{A}^1_k$: on parle de mauvaise réduction additive.*

FIGURE 5.3 – Type de réduction



(Bonne réduction) (Mauvaise réduction multiplicative) (Mauvaise réduction additive)

Proposition 5.9 (Réduction semi-stable, [Sil09], proposition VII.5.4)**.** *Soit E/K une courbe elliptique et $\mathfrak{p}$ un idéal premier de K.*

- *si $K'/K_{\mathfrak{p}}$ est une extension non ramifiée, alors le type de réduction de E sur $K_{\mathfrak{p}}$ (bonne, multiplicative, additive) est le même que le type de réduction de E sur K' ;*
- *si $K'/K_{\mathfrak{p}}$ est une extension finie et E une courbe elliptique à réduction bonne ou multiplicative sur $K_{\mathfrak{p}}$, alors le type de réduction est le même sur K' ;*
- *il existe une extension finie $K'/K_{\mathfrak{p}}$ telle que E a bonne ou mauvaise réduction multiplicative sur K'.*

Une courbe elliptique qui a bonne réduction ou mauvaise réduction multiplicative en toute place est dite semi-stable. S'il existe une extension K'/K telle que E/K' ait bonne réduction, on dit que E/K a potentiellement bonne réduction (on définit de même une courbe potentiellement semi-stable).

La proposition ci-dessus dit donc que toute courbe elliptique est potentiellement semi-stable, et une courbe elliptique n'ayant que des places de bonne ou de mauvaise réduction additive a potentiellement bonne réduction partout. Les deux quantités définies précédemment, le discriminant et le j-invariant de la courbe elliptique, donnent des informations décisives sur la réduction d'une courbe elliptique.

Définition 5.10 (Discriminant minimal)**.** Soit E/K une courbe elliptique sur un corps de nombres. Pour chaque place v associée à un idéal premier $\mathfrak{p}$, soit $N_\mathfrak{p}$ le plus petit exposant tel que $\mathfrak{p}^{N_\mathfrak{p}}$ soit le discriminant minimal en $\mathfrak{p}$ d'une équation intégrale de E. On définit le discriminant minimal de E/K par la formule :

$$\Delta(E/K) = \prod_{\mathfrak{p}} \mathfrak{p}^{N_\mathfrak{p}}.$$

Le produit est bien fini, puisque $\Delta(E/K)$ divise un discriminant (Δ) associé à une équation intégrale de E, donc admet un nombre fini de diviseurs premiers.

Proposition 5.11. *Soit E/K une courbe elliptique de discriminant minimal $\Delta(E/K)$. Alors E a bonne réduction en un idéal maximal $\mathfrak{p}$ si, et seulement si $\mathfrak{p}$ ne divise pas $\Delta(E/K)$.*

L'étude du j-invariant affine l'état de l'art exposé dans la proposition 5.9.

Proposition 5.12. *Soient E une courbe elliptique définie sur un corps de nombres K et $\mathfrak{p}$ un idéal maximal de K. Alors,*

- *le j-invariant de E vérifie $|j_E|_\mathfrak{p} \leqslant 1$ si, et seulement si E a potentiellement bonne réduction en $\mathfrak{p}$;*
- *le j-invariant de E vérifie $|j_E|_\mathfrak{p} > 1$ si, et seulement si E a mauvaise réduction multiplicative en $\mathfrak{p}$;*

On a même mieux que cela : d'une part, quand $|j_E|_\mathfrak{p} > 1$, une uniformisation bien utile peut rendre la fibre spéciale plus facile à étudier.

Proposition 5.13 (Uniformisation de Tate, [Sil94], sections V.3 et V.5)**.** *Soient E une courbe elliptique sur un corps de nombres K et v une place ultramétrique telle que $|j_E|_v^{-1} < 1$ (donc v est une place de mauvaise réduction multiplicative). Pour toute extension algébrique L/K_v, il existe un isomorphisme*

$$L^*/q^\mathbb{Z} \simeq E(L),$$

où $|q|_v = |j_E|_v^{-1}$, donné par des séries v-adiques convergentes, et cet isomorphisme commute avec l'action du groupe de Galois absolu de K_v.

Remarque 5.14. L'uniformisation complexe ressemble beaucoup à celle p-adique si l'on constate qu'après exponentiation, $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ est isomorphe à $\mathbb{C}^*/q^\mathbb{Z}$ avec $q = e^{2i\pi\tau}$.

D'autre part, dans le cas où $|j_E|_\mathfrak{p} \leqslant 1$, on peut déterminer une extension où E passe de bonne réduction en puissance à bonne réduction en acte.

Proposition 5.15 ([Sil94], proposition IV.10.3)**.** *Soit K un corps local de caractéristique résiduelle p, et E/K une courbe elliptique de j-invariant entier. Pour tout entier $m \geqslant 3$ premier à p, la courbe elliptique E a bonne réduction sur $K(E[m])$.*

Ainsi, si E est une courbe elliptique définie sur un *corps de nombres* K, ayant potentiellement bonne réduction partout, adjoindre les coordonnées des points de 3-torsion à K permet d'obtenir de la bonne réduction partout, sauf peut-être en les places de caractéristique résiduelle 3. On y remédie en ajoutant, encore, les coordonnées des points de 4-torsion. Autrement dit, si E est une courbe elliptique ayant potentiellement bonne réduction en toute place de K, alors E a bonne réduction en toute place de $K(E[12])$.

Si E admet des places de mauvaise réduction, la géométrie d'Arakelov nous encourage à choisir des modèles de E dont les fibres sont aussi simples à étudier que possible (notamment au niveau de la description de leurs composantes irréductibles). Une telle exigence est remplie par le modèle minimal régulier d'une courbe elliptique.

Définition 5.16 (Modèle minimal régulier, [Liu02], définition 9.4.34)**.** Soit E/K une courbe elliptique. Il existe une unique surface arithmétique $\mathcal{E} \to B$ minimale (c'est-à-dire, *pour une surface de genre au moins un*, qu'elle ne contient pas de diviseur d'auto-intersection -1) dont la fibre générique est isomorphe à E. On l'appelle modèle minimal régulier de E.

Le modèle minimal régulier d'une courbe elliptique est obtenu par désingularisation minimale d'un de ses modèles de Weierstrass.

Une propriété importante du modèle minimal régulier est que ses sections décrivent exactement les points rationnels de E : on a $\mathcal{E}(\mathcal{O}_K) \simeq E(K)$. Pour tous les détails sur la structure des fibres du modèle minimal régulier, on renvoie le lecteur à la section A.1.

Comme on le sait grâce au théorème de classification de Kodaira-Néron (théorème A.2), le discriminant minimal $\Delta(E/K)$, obtenu en regardant localement les meilleures équations de Weierstrass de E, est lié au modèle minimal régulier. Définissons une dernière quantité liée à une courbe elliptique, et dont les diviseurs premiers sont des idéaux de mauvaise réduction ; il s'agit du conducteur, qui intervient comme on l'a vu en introduction dans la minoration (4).

Définition 5.17 (Conducteur)**.** Soit E/K une courbe elliptique, de modèle minimal régulier $\mathcal{E} \to B$. Notons $m_\mathfrak{p}$ le nombre de composantes irréductibles de la fibre $\mathcal{E}_\mathfrak{p}$.

On définit la norme N_E du conducteur de E/K par la formule :

$$\ln(N_E) = \sum_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}}(E/K) \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})),$$

où $\mathfrak{f}_{\mathfrak{p}}(E/K)$ est défini par ce qu'on appelle la formule de Ogg :

$$\mathfrak{f}_{\mathfrak{p}}(E/K) = v_{\mathfrak{p}}(\Delta(E/K)) + 1 - m_{\mathfrak{p}}.$$

En particulier, $\mathfrak{f}_{\mathfrak{p}}(E/K) \geqslant 1$ si, et seulement si E/K a mauvaise réduction en $\mathfrak{p}$, donc la somme ci-dessus est finie, et la norme du conducteur est bien définie.

5.3 Cas de la multiplication complexe

Définition 5.18 (Multiplications complexes)**.** Soit $E/\mathbb{C}$ une courbe elliptique. On dit que E admet des multiplications complexes si $\mathbb{Z} \subsetneq \mathrm{End}(E)$, c'est-à-dire s'il existe d'autres endomorphismes que les multiplications par des entiers.

Si $E/\mathbb{C}$ est une courbe elliptique, on sait ([Sil09], VI.5.5) que $\mathrm{End}(E) \otimes \mathbb{Q}$ est isomorphe soit à $\mathbb{Q}$ (si $\mathrm{End}(E)$ ne contient que les multiplications $[n]$ par des entiers), soit à un corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$, et dans ce cas $\mathrm{End}(E)$ est un ordre de ce corps : il existe un unique entier $f \geqslant 1$, appelé le conducteur de $\mathrm{End}(E)$ (à ne pas confondre avec le conducteur de E, définition 5.17), tel que :

$$\mathrm{End}(E) = \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

On dit alors que E admet des multiplications complexes par le corps $\mathbb{Q}(\sqrt{d})$, ou par l'anneau $\mathbb{Z}+f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ si cette précision est nécessaire. Il existe toujours une courbe elliptique isogène à E telle que son anneau d'endomorphismes soit exactement $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. On suppose donc, dans le reste de cette section, que $\mathrm{End}(E) = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Attention toutefois, parce qu'il existe deux façons de plonger $\mathrm{End}(E)$ dans $\mathbb{C}$: précisons ce que nous entendons par toutes ces égalités.

Proposition 5.19 ([Sil94], proposition II.1.1)**.** *Soit $E/\mathbb{C}$ une courbe elliptique à multiplications complexes par l'anneau $A \subseteq \mathbb{C}$. Il existe un unique isomorphisme $[\cdot] : A \xrightarrow{\sim} \mathrm{End}(E)$ tel que pour tout $\omega \in \Omega_E$, on ait :*

$$\forall \alpha \in A, \quad [\alpha]^*\omega = \alpha\omega.$$

On a énoncé qu'une courbe elliptique à multiplications complexes a d'autres endomorphismes que les multiplications par des entiers ; parmi ces multiplications complexes, certaines vont ici être privilégiées : les endomorphismes de Frobenius.

Théorème 5.20 (Relèvement du Frobenius, [ST61], III.13, théorème 1)**.** *Soit E une courbe elliptique à multiplications complexes par $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, définie sur un corps de nombres K. Supposons que K contient $\mathbb{Q}(\sqrt{d})$. Pour tout idéal premier $\mathfrak{p}$ de K de bonne réduction, il existe une unique isogénie $\mathrm{F}_\mathfrak{p} : E \to E$ définie sur K qui induit, modulo $\mathfrak{p}$, l'exponentiation à la puissance $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$ sur la réduction de la courbe elliptique. On l'appelle endomorphisme de Frobenius de E associé à $\mathfrak{p}$, et il est de degré $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$.*

En d'autres termes, il est possible de relever le Frobenius modulo $\mathfrak{p}$ sur une courbe elliptique à multiplications complexes. Enfin, il est intéressant de remarquer qu'admettre « beaucoup » d'endomorphismes est une telle contrainte que le type de réduction de E est alors figé :

Théorème 5.21 ([Sil94], théorèmes II.6.1 et II.6.4)**.** *Soit L un corps de nombres, et E/L une courbe elliptique à multiplications complexes. Alors j_E est un entier algébrique, et par conséquent E a potentiellement bonne réduction en tout idéal premier de L.*

5.4 Intersection sur une surface elliptique

Dans cette section, on poursuit l'étude de l'intersection arithmétique entamée dans le chapitre 4, en l'appliquant aux surfaces arithmétiques de genre un, ou plus précisément au modèle minimal régulier d'une courbe elliptique.

L'existence des fonctions de Green-Arakelov, que nous avons introduite dans le théorème 4.5, peut heureusement être rendue explicite dans le cas des surfaces arithmétiques de genre un grâce aux fonctions de Néron.

Définition 5.22 (Fonction de Néron)**.** Soit v une place archimédienne. Fixons un isomorphisme entre $E(\bar{K}_v)$ et $\mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$, où τ_v est un nombre complexe de partie imaginaire strictement positive. La fonction $\lambda_v : \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z}) \setminus \{0\} \to \mathbb{R}$ est définie par la formule :

$$\lambda_v(z) = -\frac{1}{2}B_2\left(\frac{\ln(|u|_v)}{\ln(|q|_v)}\right)\ln(|q|_v) - \ln(|1-u|_v) - \sum_{n=1}^{\infty}\ln\left(\left|(1-q^n u)\left(1-\frac{q^n}{u}\right)\right|_v\right),$$

où $u = e^{2i\pi z}$, $q = e^{2i\pi\tau_v}$, tandis que $B_2(x) = (x-[x])^2 - (x-[x]) + \frac{1}{6}$ est le deuxième polynôme de Bernoulli étendu par 1-périodicité.

Remarque 5.23. Une autre expression équivalente est

$$\lambda_v(z) = -\ln\left(\left|e^{-\frac{1}{2}z\eta(z)}\sigma(z)\Delta(z)^{\frac{1}{12}}\right|_v\right),$$

où la fonction Δ a été définie dans la proposition 5.5, et σ, η deux fonctions méromorphes qui se définissent à partir des fonctions $\mathscr{P}$ de Weierstrass (voir [Sil94], propositions I.5.2 et I.5.4 pour une définition de η et σ, puis le théorème VI.3.2 pour cette identité de λ_v).

Remarque 5.24. La fonction $u \mapsto \frac{1}{2}B_2\left(\frac{\ln(|u|)}{\ln(|q|)}\right)$ permet de décrire la fonction de Green-Arakelov sur $\mathbb{R}/\mathbb{Z}$ pour la mesure de Haar, donc cette définition n'est pas complètement *ad hoc*.

On peut montrer que λ_v ne dépend pas du choix de τ_v. On a alors $g_v(P,Q) = -\lambda_v(P-Q)$ pour $P, Q \in E(\bar{K}_v)$. Suivant la définition 4.7 (ou, si l'on veut, la remarque 4.16), l'intersection de deux diviseurs horizontaux irréductibles $\mathcal{P}_1$ et $\mathcal{P}_2$ en une place archimédienne v est donnée par la formule :

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v = n_v \sum_{\sigma,\tau} \lambda_v \left(P_1^\sigma - P_2^\tau\right),$$

où, donc, $\mathcal{P}_1 \otimes_{v,B} \mathbb{C} = \sum_\sigma (P_1^\sigma)$ et de même pour $\mathcal{P}_2$.

Remarque 5.25. Selon la notation qui s'avère être la plus agréable, on notera indifféremment $\langle P, Q\rangle$, $\langle \mathcal{P}, \mathcal{Q}\rangle$ ou $\langle (\mathcal{P}), (\mathcal{Q})\rangle$ pour P et Q des points de $E(\bar{K})$ d'adhérences $\mathcal{P}$ et $\mathcal{Q}$. Si une différence $\mathcal{P} - \mathcal{O}$ apparaît dans un calcul d'intersection, il n'y a pas d'ambiguïté : ce sera *systématiquement* la différence des diviseurs $(\mathcal{P})$ et $(\mathcal{O})$ (et non pas la différence pour la loi de groupe sur la courbe elliptique).

5.5 Hauteurs

Si K est un corps de nombres, on rappelle que M_K est l'ensemble de ses places ($M_K^0 \subseteq M_K$ se restreint aux places ultramétriques, et M_K^∞ aux places archimédiennes), et que pour tout $v \in M_K$, la valeur absolue associée à v est notée $|\cdot|_v$ (normalisée par $|p|_v = \frac{1}{p}$ si v divise p, et prolongeant la valeur absolue usuelle de $\mathbb{Q}$ si v divise ∞). Alors, pour tout point $P = (x_0 : \cdots : x_n)$ de l'espace projectif $\mathbb{P}^n(K)$, la hauteur naïve de P est définie par

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \ln(\max_{0 \leqslant i \leqslant n}(|x_i|_v)).$$

Si x est un nombre algébrique, on pose $h(x) = h([x:1])$. On vérifie que $h(P)$ ne dépend ni du choix des coordonnées projectives de P, ni du choix du corps de rationalité K. Il fait alors sens de définir la fonction h sur une courbe elliptique dès qu'on l'a plongée dans $\mathbb{P}^2$ grâce au choix d'une équation de Weierstrass.

La hauteur apparaît régulièrement dans les résultats qui cherchent à estimer la complexité arithmétique des nombres, ainsi que dans plusieurs théorèmes de transcendance ; le lecteur intéressé peut par exemple se tourner vers les lemmes de Siegel, dont on trouve une formulation dans le lemme 2.2 de [Lau83]. Dans le cas des courbes elliptiques, il sera bien commode de pouvoir estimer des quantités liées à la courbe elliptique en fonction de la hauteur de son j-invariant. Selon les situations et les auteurs, une autre hauteur apparaît avec pertinence : il s'agit de la hauteur de Faltings h_{F^+}, qui est notamment d'une importance centrale dans la démonstration de la conjecture de Mordell, et qu'on peut définir pour une courbe elliptique par la formule :

$$h_{F^+}(E/K) = \frac{1}{12[K:\mathbb{Q}]}\left(\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))) - \sum_{v\in M_K^\infty} n_v \ln(|(2\pi)^{-12}\Delta(\tau_v)|(2\mathrm{Im}(\tau_v))^6)\right), \tag{5.2}$$

où la fonction Δ est celle définie en la proposition 5.5, et τ_v est un nombre complexe du demi-plan supérieur tel que $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$; cette formule est donnée dans la proposition X.1.1 de [CS86]. Nous voulons simplement en profiter pour montrer au lecteur que même si nous allons recourir à la hauteur du j-invariant dans l'inégalité de notre théorème principal, il peut se ramener sans difficulté à la hauteur de Faltings de la courbe elliptique, grâce à la proposition suivante.

Proposition 5.26. *Soit E/K une courbe elliptique. On peut écrire son j-invariant comme le quotient de deux idéaux premiers entre eux, $(j_E) = \mathfrak{A}\mathfrak{D}^{-1}$, où $\mathfrak{D}^{-1}$ est un diviseur de l'idéal $\Delta(E/K)$ (il y a même égalité dans le cas d'une courbe elliptique semi-stable). Posons $\mathfrak{Y}(E/K) = \Delta(E/K)\mathfrak{D}^{-1}$. La hauteur de son j-invariant et sa hauteur de Faltings sont alors reliées par les inégalités :*

$$-6\ln(1+h(j_E)) - 14 \leqslant 12h_{F^+}(E/K) - h(j_E) \leqslant \frac{1}{[K:\mathbb{Q}]}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{Y})) + 2{,}83.$$

Démonstration. Par uniformisation complexe, il existe un nombre complexe τ_v tel que $|\mathrm{Re}(\tau_v)| \leqslant \frac{1}{2}$, $\mathrm{Im}(\tau_v) \geqslant \frac{\sqrt{3}}{2}$ et $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$. On sait alors montrer d'une part, en recourant par exemple à [HS88] (lemme 2.2) et à [BP05] (lemme 24), que :

$$-6 \leqslant \max(\ln(|j_E|_v),0) - 2\pi\mathrm{Im}(\tau_v) \leqslant 2{,}304,$$

et d'autre part, assez simplement, comme $\mathrm{Im}(\tau_v) \geqslant \frac{\sqrt{3}}{2}$,

$$\left|-2\pi\mathrm{Im}(\tau_v) - \ln(|(2\pi)^{-12}\Delta(\tau_v)|)\right| \leqslant 24\sum_{n=1}^{\infty}\ln\left(1+e^{-\sqrt{3}\pi n}\right) \leqslant 0{,}12. \tag{5.3}$$

Partant de la formule (5.2), on obtient :

$$\frac{1}{[K:\mathbb{Q}]}\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K)))+h_\infty(j_E)-\frac{6}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty}n_v\ln(\ln(\max(|j_E|_v,e)))\\ -14\leqslant 12h_{F^+}(E/K),$$

où l'on note $h_\infty(j_E)=\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty}n_v\max(\ln(|j_E|_v),0)$ par commodité, et :

$$12h_{F^+}(E/K)\leqslant\frac{1}{[K:\mathbb{Q}]}\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K)))+h_\infty(j_E)+2{,}83.$$

Il est facile de montrer que :

$$\frac{1}{[K:\mathbb{Q}]}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{D}))+h_\infty(j_E)=h(j_E),$$

et que :

$$\begin{aligned}\sum_{v\in M_K^\infty}n_v\ln(\ln(\max(|j_E|_v,e)))&=\ln\prod_{v\in M_K^\infty}(\ln(\max(|j_E|_v,e)))^{n_v}\\&\leqslant\ln\left(\sum_{v\in M_K^\infty}\frac{\ln(\max(|j_E|_v,e))}{[K:\mathbb{Q}]}\right)^{[K:\mathbb{Q}]}\\&\leqslant[K:\mathbb{Q}]\ln\left(1+\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty}\ln(\max(|j_E|_v,1))\right)\\&\leqslant[K:\mathbb{Q}]\ln(1+h(j_E)),\end{aligned}$$

grâce à l'inégalité arithmético-géométrique, et on en déduit finalement les inégalités désirées. □

Remarque 5.27. D'après [CS86], page 258, on peut montrer que si $\mathfrak{p}$ est un idéal premier de K, alors $v_\mathfrak{p}(\mathfrak{Y})<12+12v_\mathfrak{p}(2)+6v_\mathfrak{p}(3)$.

Ces considérations étant dorénavant mises de côté, on peut définir la hauteur de Néron-Tate sur une courbe elliptique, ou hauteur canonique (parce qu'elle s'avère être la partie quadratique de toute fonction de hauteur définie sur la courbe elliptique). Si, à présent, on considère une courbe elliptique E, plongée dans $\mathbb{P}^2$ par le choix d'un modèle de Weierstrass défini sur K, alors on définit la hauteur de Néron-Tate d'un point P de $E(\bar{K})$ par la formule :

$$\hat{h}(P)=\lim_{n\to+\infty}\frac{h([2^n]P)}{4^n}.$$

Comme nous le verrons grâce au lien entre hauteur et intersection, la hauteur de Néron-Tate admet elle aussi une décomposition en termes locaux, à l'instar de la hauteur naïve. En attendant on résume, dans la proposition suivante, les propriétés de $\hat{h}$ qui nous serviront.

Proposition 5.28 ([HS00], théorèmes B.4.1 et B.5.6)**.** *La hauteur de Néron-Tate $\hat{h} : E(\bar{K}) \to \mathbb{R}$ vérifie les propriétés suivantes :*

- *la valeur de $\hat{h}(P)$, pour $P \in E(\bar{K})$, ne dépend pas du corps de rationalité de P considéré ;*
- *elle est invariante par conjugaison : si $P \in E(\bar{K})$ et $\sigma : K(P) \hookrightarrow \bar{K}$ est un plongement, alors $\hat{h}(P) = \hat{h}(P^\sigma)$;*
- *elle induit une forme quadratique définie positive sur $E(\bar{K}) \otimes \mathbb{Q}$, donc également un produit scalaire $(\cdot|\cdot)$ défini par la formule*

$$(P|Q) = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right);$$

- *pour tout endomorphisme non nul ϕ de la courbe elliptique E et tout point $P \in E(\bar{K})$, on a $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$.*

On se permettra, par la suite, d'amalgamer l'accouplement bilinéaire défini ci-dessus sur $E(\bar{K})$ et celui défini sur $\mathrm{Div}^0(E)$ par $((P)-(O)|(Q)-(O)) = (P|Q)$ puis étendu par linéarité. Cet accouplement a également une interprétation géométrique arakelovienne. Avant de la nommer, on fait une courte digression nécessaire.

Soit $\mathcal{X} \to B$ une surface arithmétique. Pour un diviseur $\mathcal{D} \in \mathrm{Div}(\mathcal{X})$ de degré nul, il existe un diviseur vertical $[\mathcal{D}] \in \mathrm{Div}(\mathcal{X}) \otimes \mathbb{Q}$, unique modulo les fibres, tel que l'intersection de $\mathcal{D} + [\mathcal{D}]$ avec tout diviseur vertical soit nulle. Si $\mathcal{X} \to B$ est lisse, alors $[\mathcal{D}] = 0$ pour tout diviseur $\mathcal{D} \in \mathrm{Div}(\mathcal{X})$ de degré nul. En effet, il suffit dans ce cas de le vérifier pour chaque fibre, laquelle est un diviseur principal (celui d'une uniformisante), donc son intersection avec $\mathcal{D}$ est nulle d'après la remarque 4.12.

Le point de départ de la démonstration de l'inégalité (4) est alors le théorème suivant.

Théorème 5.29 (Faltings-Hriljac, [Fal84] et [Hri85])**.** *Soit E une courbe elliptique définie sur un corps de nombres K, et $\mathcal{E} \to B$ son modèle minimal régulier. Alors, pour tous diviseurs D_1 et $D_2 \in \mathrm{Div}(E)$ de degré nul, à support dans des points de $E(L)$ et dont on note $\mathcal{D}_1$ et $\mathcal{D}_2$ l'adhérence dans $\mathcal{E}$, on a*

$$\langle \mathcal{D}_1 + [\mathcal{D}_1], \mathcal{D}_2 + [\mathcal{D}_2] \rangle_K = -2[L : \mathbb{Q}](D_1|D_2).$$

On a donc fait le lien entre la hauteur de Néron-Tate sur une courbe elliptique et l'intersection arithmétique. Si $\mathcal{D}_1 = \mathcal{D}_2$, on se retrouve avec une auto-intersection. Les théorèmes 5.29 et 4.17 permettent d'écrire une autre relation entre hauteur canonique et intersection.

Corollaire 5.30. *Soit E une courbe elliptique définie sur un corps de nombres K ayant bonne réduction partout, et $\mathcal{E} \to B$ son modèle minimal régulier, de section neutre $\mathcal{O}$. Alors, pour tout point $Q \in E(\bar{K})$ d'adhérence $\mathcal{Q}$ dans $\mathcal{E}$, on a :*

$$\hat{h}(Q) = \frac{\langle \mathcal{Q}, \mathcal{O} \rangle_K}{[K(Q) : \mathbb{Q}]}. \tag{5.4}$$

Démonstration. Notons $L = K(Q)$. On se ramène par changement de base au cas où $\mathcal{Q}$ est une section d'un modèle minimal régulier $\mathcal{E}'/\mathcal{O}_L$; ceci n'affecte pas le calcul de $\hat{h}(Q)$, car la hauteur est invariante par extension de corps. Donc $\langle \mathcal{Q}, \mathcal{Q} \rangle_L = -\langle \mathcal{Q}, \mathrm{K}_{\mathcal{E}'/\mathcal{O}_L} \rangle_L$ par la formule d'adjonction énoncée dans le théorème 4.17, et il est démontré dans [Szp90], théorème 2, que si E a réduction semi-stable, alors :

$$\langle \mathcal{Q}, \mathrm{K}_{\mathcal{E}'/\mathcal{O}_L} \rangle_L = \frac{1}{12} \ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta(E/L))|). \tag{5.5}$$

Ici, $\Delta(E/L) = \mathcal{O}_L$, donc finalement l'auto-intersection de toute section de $\mathcal{E}' \to \mathrm{Spec}(\mathcal{O}_L)$ est nulle. De fait, en appliquant le théorème 5.29 aux diviseurs $D_1 = D_2 = (Q) - (O')$ (on a noté $\mathcal{O}'$ la section neutre de $\mathcal{E}' \to \mathrm{Spec}(\mathcal{O}_L)$), on obtient :

$$2[L : \mathbb{Q}]\hat{h}(Q) = -\langle \mathcal{Q} - \mathcal{O}', \mathcal{Q} - \mathcal{O}' \rangle_L = -\langle \mathcal{Q}, \mathcal{Q} \rangle_L - \langle \mathcal{O}', \mathcal{O}' \rangle_L + 2\langle \mathcal{Q}, \mathcal{O}' \rangle_L = 2\langle \mathcal{Q}, \mathcal{O}' \rangle_L.$$

On a le résultat voulu grâce à la formule du changement de base (4.8). En effet, comme la hauteur canonique est invariante par conjugaison,

$$\begin{aligned} 2[L : \mathbb{Q}]\hat{h}(Q) &= 2[K : \mathbb{Q}] \sum_{\sigma : L \hookrightarrow \mathbb{C}} \hat{h}(Q^\sigma) = \frac{2}{[L : K]} \sum_{\sigma : L \hookrightarrow \mathbb{C}} \langle \mathcal{Q}^\sigma, \mathcal{O}' \rangle_L \\ &= \frac{2}{[L : K]} \langle r^*(\mathcal{Q}), r^*(\mathcal{O}) \rangle_L = 2\langle \mathcal{Q}, \mathcal{O} \rangle_K. \end{aligned}$$

□

En vérité, le raisonnement ci-dessus permet d'obtenir une expression de la hauteur en terme d'intersection arithmétique y compris dans le cas d'une courbe elliptique semi-stable, mais pour ne pas perdre de vue le théorème principal, je reporte la démonstration d'une telle expression à l'annexe A.2.

Chapitre 6

Démonstration du théorème principal

« Ô miracle ! ô jouissance du philosophe qui vérifie l'excellence de sa théorie ! »
Charles Baudelaire, *Le Spleen de Paris*

L'objectif de ce chapitre est de démontrer le théorème annoncé dans l'introduction. Comme l'expliquent les remarques à suivre, on peut considérablement relaxer les hypothèses et les données sur la courbe elliptique à connaître.

Théorème 6.1. *Soit $K/\mathbb{Q}$ une extension galoisienne finie de degré n_K et de discriminant absolu d_K. Soit E/K une courbe elliptique à multiplications complexes par l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, et dont le conducteur est de norme N_E. Pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on a :*

$$\hat{h}(P) \geqslant \frac{1}{c_{K,E}} \frac{1}{D} \left(\frac{\ln(\ln(4D))}{\ln(4D)} \right)^3,$$

où :

$$c_{K,E} = 5 \cdot 2^{28} \sqrt{6n_K} (59{,}07 + 276{,}48 \ln(|d_K|) + n_K (2911{,}6 + 550{,}1 \ln(6N_E) + 138{,}3 \ln(-4d)))^6 \cdot (3{,}89 + 0{,}13 h(j_E))^3.$$

si HRG est vraie, et :

$$c_{K,E} = 8\sqrt{3n_K} \exp\left[(|d_K|^{384} d^{92n_K} (6N_E)^{382n_K} 192^{384n_K})^{2709} \exp(387(4992n_K + 33)) \right] \times \left(728 + 10^{-4751} \exp\left[(|d_K|^{384} d^{92n_K} (6N_E)^{382n_K} 192^{384n_K})^{2709} \exp(387(4992n_K + 33)) \right] \right) \times (3{,}89 + 0{,}13 h(j_E))^3$$

sinon.

Remarque 6.2. Si l'extension $K/\mathbb{Q}$ n'est pas supposée galoisienne, on se ramène au cas galoisien en remplaçant K par l'extension composée $\hat{K}$ de tous les conjugués de K sur $\mathbb{Q}$. Le degré $n_{\hat{K}}$ et le discriminant $d_{\hat{K}}$ de $\hat{K}$ sont alors liés aux quantités correspondantes de K par les formules $n_{\hat{K}} | n_K!$ et $d_{\hat{K}} | d_K^{n_{\hat{K}}} | d_K^{n_K!}$ (voir [Tôy55]). Dans certains cas, selon la complexité du groupe de Galois, on peut affiner l'inégalité ; par exemple, si $K = \mathbb{Q}(\sqrt[n]{2})$ pour $n \geqslant 2$, alors $n_{\hat{K}} \leqslant \varphi(n)n$ et $\ln(d_{\hat{K}}) \leqslant n \ln(2n)$.

Remarque 6.3. On peut relâcher le nombre de données nécessaires à la description de l'inégalité : il est démontré dans [Col98] que la hauteur de Faltings de la courbe elliptique, et donc $h(j_E)$ également, peut être minorée par une fonction affine en $\ln(-4d)$ (mais le coefficient directeur n'est pas explicite), et on peut majorer de la même manière $\ln(6N_E)$: en effet, réutiliser (5.2) et (5.3) permet de démontrer que

$$h_{F^+}(E/K) \geqslant \frac{1}{12[K:\mathbb{Q}]} \ln(N_E),$$

et la proposition 5.26 montre comment relier, si besoin, la hauteur de Faltings h_{F^+} et la hauteur de j_E. On peut donc, en fin de compte, obtenir une minoration ne dépendant que de K et de $h(j_E)$, et même une minoration ne dépendant que de K et de d, car la hauteur de j_E est également majorée en fonction de d (voir par exemple la section 4 de [Hab10] si HRG).

Remarque 6.4. Un certain nombre de modifications est possible : la démonstration montre que la constante $c_{K,E}$ peut être modifiée si K contient $\mathrm{End}(E) \otimes \mathbb{Q}$ (le terme $\ln(-4|d_K|d)$ peut être remplacé par $\ln(|d_K|)$) ou si E a bonne réduction en toute place de K (le terme $6N_E$ peut être remplacé par 1, et plusieurs constantes peuvent être choisies plus petites). On peut voir ces améliorations à partir du lemme 6.13.

6.1 Premières réductions

On effectue un changement de base adéquat $\mathrm{Spec}(\mathcal{O}_{K'}) \to B$, de sorte que :
- K' contient $\mathrm{End}(E) \otimes \mathbb{Q}$;
- E a bonne réduction en toute place de K', ceci étant possible parce que le j-invariant de E est un entier algébrique, donc la courbe a potentiellement bonne réduction en toute place ;
- K' est une extension normale de $\mathbb{Q}$.

On prend pour cela $K' = K \cdot (\mathrm{End}(E) \otimes \mathbb{Q}) \cdot K(E[12])$, qui reste galoisien sur $\mathbb{Q}$ si K l'est. Notons que ce changement de base n'affecte pas le calcul de la hauteur de Néron-Tate, qui ne dépend pas du corps de rationalité du point considéré. Dans cette section, on n'utilisera l'accouplement d'intersection que sur $\mathcal{E} \to \mathrm{Spec}(\mathcal{O}_{K'})$, on peut donc poser $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{K'}$ sans risque de confusion. Soient $L = K'(P)$ et $D = [L : K']$.

Soient $s \geqslant 3$ un réel dont on fixera la valeur ultérieurement, et $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers rationnels inférieurs à s qui se décomposent complètement dans K'. Pour tout $p \in \Pi_s$ on associe un idéal premier $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ divisant p, puis une isogénie $\mathrm{F}_p : E \to E$ qui induit, modulo $\mathfrak{p}$, l'exponentiation à la puissance p sur la réduction de la courbe elliptique, dont l'existence est assurée par le fait que E est à multiplications complexes d'après le théorème 5.20. On sait, en particulier, que F_p est de degré p.

Montrons d'abord qu'on peut se ramener au cas où tous les conjugués de $\mathrm{F}_p(P)$ par les K'-plongements de L dans $\mathbb{C}$ sont distincts. Ceci permet de faire l'économie du lemme combinatoire 4.2 de [Lau83] sur le nombre de conjugués qui coïncident.

Lemme 6.5. *Nous pouvons supposer que $K'(\mathrm{F}_p(P)) = L$ pour tout $p \in \Pi_s$. En particulier, on a toujours $\mathrm{F}_p(P)^\sigma \neq \mathrm{F}_p(P)^\tau$ pour $\sigma, \tau \in \mathrm{Hom}_{K'}(L, \mathbb{C})$ distincts.*

Démonstration. Les lemmes 3.2 et 3.3 de [Rat04] s'adaptent à notre situation, et montrent qu'on peut supposer que soit $K'(\mathrm{F}_p(P)) = L$, soit $[L : K'(\mathrm{F}_p(P))] = p$ pour tout $p \in \Pi_s$. Démontrons qu'on peut même s'affranchir du second cas pour démontrer l'inégalité (6.1) pour tout point d'ordre infini de degré D, à l'aide d'une récurrence sur D ; notons que si $L = K'$, alors il n'y a rien à dire.

S'il existe $p \in \Pi_s$ tel que $[L : K'(\mathrm{F}_p(P))] = p$, alors l'hypothèse de récurrence assure que l'inégalité (6.1) est vérifiée pour $\mathrm{F}_p(P)$, et on a :

$$\hat{h}(P) = \frac{1}{p}\hat{h}(\mathrm{F}_p(P)) \geqslant \frac{1}{p[K'(\mathrm{F}_p(P)) : K']} f([K'(\mathrm{F}_p(P)) : K']) = \frac{1}{D} f([K'(\mathrm{F}_p(P)) : K']),$$

où $f(x) = \frac{1}{c_{K,E}} \frac{1}{x} \left(\frac{\ln(\ln(4x))}{\ln(4x)}\right)^3$ définit une application décroissante pour $x \geqslant 1$, d'où l'inégalité (6.1) pour P. □

Il était déjà démontré, dans le lemme 4.2 de [Lau83], que les « orbites » par $\mathrm{Hom}_{K'}(L, \mathbb{C})$ des différents $\mathrm{F}_p(P)$ ne se recoupent pas (et même des différents $\phi(P)$, pour $\phi \in \mathrm{End}(E)$). Conjointement au lemme précédent, on en déduit :

Corollaire 6.6. *Nous pouvons supposer que pour tous $p, p' \in \Pi_s$ et $\sigma, \tau \in \mathrm{Hom}_{K'}(L, \mathbb{C})$ tels que $(\sigma, p) \neq (\tau, p')$, on a $\mathrm{F}_p(P)^\sigma \neq \mathrm{F}_{p'}(P)^\tau$.*

Si P est un point de torsion, ce corollaire n'est plus nécessairement valable. C'est le seul endroit où l'on utilise le fait que P soit d'ordre infini.

6.2 Contribution positive des places finies

Soient m_1, …, m_r des entiers naturels ; on étend les morphismes F_p en des morphismes de $\mathcal{E}$ dans $\mathcal{E}$, et on considère le diviseur de Weil de $\mathcal{E}$ suivant :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - D \cdot (\mathcal{O})),$$

où, pour uniformiser les notations, on a posé $p_0 = 1$ et $\mathrm{F}_1 = \mathrm{Id}$. C'est par l'intermédiaire de ce diviseur qu'on compte calculer la hauteur de P. Le point de départ est le théorème 5.29 : comme $\mathcal{L}$ est de degré nul, on a :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j \left(\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + D^2 \langle \mathcal{O}, \mathcal{O} \rangle - D \langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle \right).$$

En vertu du corollaire 5.30 et de la proposition 5.28, on a

$$\langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle = D n_{K'} (p_i + p_j) \hat{h}(P), \text{ et } \langle \mathcal{O}, \mathcal{O} \rangle = 0,$$

donc :

$$2D^2 n_{K'} \left(\sum_{i=0}^{r} m_i \right) \left(\sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant \sum_{0 \leqslant i,j \leqslant r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle.$$

Il nous reste à estimer les termes de la forme $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle$. Si $i = j$, alors la formule d'adjonction (4.9) et l'identité (5.5) montrent que la contribution des auto-intersections provient des places archimédiennes :

$$\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_i}(\mathcal{P}) \rangle \geqslant \sum_{v \in M_{K'}^{\infty}} \sum_{\substack{\sigma,\tau : L \hookrightarrow \mathbb{C} \\ \sigma,\tau|v \\ \sigma \neq \tau}} n_v \lambda_v \left(\mathrm{F}_{p_i}(\mathcal{P})^{\sigma} - \mathrm{F}_{p_i}(\mathcal{P})^{\tau} \right). \tag{6.1}$$

Ainsi, en écrivant la décomposition locale du nombre d'intersection pour $i \neq j$ et en utilisant (6.1) ci-dessus pour $i = j$, on a :

$$\begin{aligned} 2D^2 n_{K'} \left(\sum_{i=0}^{r} m_i \right) \left(\sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant & \sum_{v \in M_{K'}^{0}} \sum_{1 \leqslant i \neq j \leqslant r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle_v \\ & + \sum_{v \in M_{K'}^{\infty}} \sum_{\substack{1 \leqslant i,j \leqslant r \\ \sigma,\tau : L \hookrightarrow \mathbb{C} \\ \sigma,\tau|v \\ (i,\sigma) \neq (j,\tau)}} n_v m_i m_j \lambda_v (\mathrm{F}_{p_i}(\mathcal{P})^{\sigma} - \mathrm{F}_{p_j}(\mathcal{P})^{\tau}) \end{aligned} \tag{6.2}$$

Avant de poursuivre, notons que l'expression ci-dessus est homogène en les m_i, si bien qu'on peut les supposer rationnels en toute généralité. Par densité et continuité, on peut même supposer dorénavant que $m_i \in \mathbb{R}_+$.
Il reste à estimer chacune des sommes du membre de droite. On commence par celle indexée par les places finies, où on tire profit de la propriété des relèvements du Frobenius.

Lemme 6.7. *On a, en conservant les notations précédentes,*

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}}\sum_{v\in M^0_{K'}} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Démonstration. Intéressons-nous d'abord aux intersections avec $\mathcal{P}$: démontrons que pour tout $\sigma : L \hookrightarrow \mathbb{C}$, tout $p \in \Pi_s$ et tout idéal premier $\mathfrak{p}$ au-dessus de p, il existe $\tau : L \hookrightarrow \mathbb{C}$ tel que $\mathrm{F}_p(\mathcal{P})^\sigma \equiv \mathcal{P}^\tau \mod \mathfrak{p}$. Il suffit pour cela de montrer que pour $x \in \mathcal{O}_{L,\mathfrak{P}}$ (où $\mathfrak{P}|\mathfrak{p}$),

$$\mathfrak{p} \text{ divise } \prod_{\tau:L\hookrightarrow\mathbb{C}} ((x^p)^\sigma - x^\tau) \in K',$$

puisque F_p induit l'endomorphisme de Frobenius modulo $\mathfrak{p}$ sur les coordonnées de $\mathcal{P}$ (si $\mathcal{P}$ se réduit en O, alors le résultat est trivial).

Or, si $x \in \mathcal{O}_{L,\mathfrak{P}}$ et

$$\mu(X) = \prod_{\tau:L\hookrightarrow\mathbb{C}} (X - x^\tau),$$

alors $\mu(X) \in K'[X]$: il s'agit du polynôme minimal de x (sur K') à la puissance $[L : K'(x)]$. Ses coefficients sont donc fixés par σ, et :

$$\mu(\sigma(X^p)) \equiv \sigma(\mu(X)^p) \mod \mathfrak{p},$$

puis, après évaluation en x, $\mu(\sigma(x^p)) \equiv 0 \mod \mathfrak{p}$, démontrant le résultat désiré. On obtient donc, partant de l'égalité (4.6),

$$\sum_{p\in\Pi_s}\sum_{v\in M^0_{K'}} \langle \mathrm{F}_p(\mathcal{P}), \mathcal{P}\rangle_v \geqslant \sum_{p\in\Pi_s}\sum_{\mathfrak{p}|p}\sum_{\sigma} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) = [L:\mathbb{Q}] \sum_{p\in\Pi_s} \ln(p).$$

On minore trivialement les intersections locales restantes, qui sont positives. □

On doit dorénavant estimer les intersections locales aux places archimédiennes.

Lemme 6.8 (Lemme d'Elkies pondéré)**.** *Soit v une place archimédienne, et soient P_1, …, P_N des points distincts de $E(L)$ tels que $P_i^\sigma \neq P_j^\tau$ pour tous $(i,\sigma) \neq (j,\tau)$. Soient m_1, …, m_N des réels strictement positifs qui vérifient $3\sum_{i=1}^N m_i^2 < 2D\left(\sum_{i=1}^N m_i\right)^2$. Alors,*

$$\sum_{\substack{1\leqslant i,j\leqslant N\\ (i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geqslant -D\sum_{i=1}^N m_i^2 \cdot \left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=1}^N m_i\right)^2}{\sum_{i=1}^N m_i^2} - 2\right) + \frac{1}{12}J_v + \frac{27}{10}\right),$$

où l'on note $J_v = \max(\ln(|j_E|_v), 0)$.

Le lemme d'Elkies est démontré dans [BP05] dans le cas où $L = K'$ et $m_i = 1$ pour tout i. La démonstration s'adapte presque trivialement à notre situation.

Démonstration. La preuve nécessite quelques notations issues de la théorie de Fourier : on note Γ_E le groupe des caractères de $E(\mathbb{C})$, c'est-à-dire l'ensemble des morphismes de groupe de $E(\mathbb{C})$ dans le groupe des nombres complexes de module 1. On définit la transformée de Fourier, définie sur Γ_E, d'une application intégrable $f : E(\mathbb{C}) \to \mathbb{C}$ par la formule

$$\hat{f}(\chi) = \int_{E(\mathbb{C})} f(P)\bar{\chi}(P)\mathrm{d}P.$$

Les autres définitions familières se transposent : on a des produits scalaires

$$< f, g >_{E(\mathbb{C})} = \int_{E(\mathbb{C})} f(P)\bar{g}(P)\mathrm{d}P, \quad < \hat{f}, \hat{g} >_{\Gamma_E} = \sum_{\chi\in\Gamma_E} \hat{f}(\chi)\bar{\hat{g}}(\chi),$$

qui sont en vérité égaux quand les deux quantités sont définies (c'est la formule de Parseval), et un produit de convolution

$$f * g(P) = \int_{E(\mathbb{C})} f(Q)g(P-Q)\mathrm{d}Q.$$

Sous de bonnes hypothèses, une telle fonction f est caractérisée par sa transformée de Fourier, puisqu'on peut écrire la formule d'inversion $f(P) = \sum\limits_{\chi\in\Gamma_E} \hat{f}(\chi)\chi(P)$.
Partant de la preuve de la proposition 2.4 de [BP05], les mêmes calculs aboutissent à :

$$\sum_{\substack{1\leqslant i,j\leqslant N\\(i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geqslant \sum_{\substack{1\leqslant i,j\leqslant N\\ \sigma,\tau: L\hookrightarrow\mathbb{C}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) - D\sum_{i=1}^N m_i^2 \lambda_t(O) - \left[D^2\left(\sum_{i=1}^N m_i\right)^2 - D\left(\sum_{i=1}^N m_i^2\right)\right] t, \quad (6.3)$$

où $t > 0$ est un paramètre quelconque, λ_t est le produit de convolution de λ_v avec le noyau de la chaleur $g_t(P) = \sum\limits_{\chi\in\Gamma_E} \exp\left(-\frac{t}{\hat{\lambda_v}(\chi)}\right)\chi(P)$; remarquons que la transformée de Fourier de g_t se lit dans sa définition : on a $\widehat{g_t}(\chi) = \exp\left(-\frac{t}{\hat{\lambda_v}(\chi)}\right)$.

Posons $m = D\sum\limits_{i=1}^N m_i$. Une observation cruciale concerne la première somme du membre de droite : si on note δ la mesure de probabilité qui donne la masse $\frac{m_i}{m}$ à P_i^σ pour tout $\sigma : L \hookrightarrow \mathbb{C}$, alors

$$\frac{1}{m^2}\sum_{\substack{1\leqslant i,j\leqslant N\\ \sigma,\tau: L\hookrightarrow\mathbb{C}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) = \iint_{E(\mathbb{C})\times E(\mathbb{C})} \lambda_t(P-Q)\delta(P)\delta(Q)\mathrm{d}P\mathrm{d}Q = < \lambda_t * \delta, \delta >_{E(\mathbb{C})},$$

et donc, par la formule de Parseval,

$$\frac{1}{m^2}\sum_{\substack{1\leqslant i,j\leqslant N\\ \sigma,\tau:L\hookrightarrow\mathbb{C}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) = \sum_{\chi\in\Gamma_E} \widehat{\lambda_t * \delta}(\chi)\bar{\hat{\delta}}(\chi) = \sum_{\chi\in\Gamma_E} \widehat{\lambda_t}(\chi)|\hat{\delta}(\chi)|^2$$
$$= \sum_{\chi\in\Gamma_E} \widehat{\lambda_v}(\chi)\widehat{g_t}(\chi)|\hat{\delta}(\chi)|^2.$$

Le terme principal de la somme est positif ; seule la positivité de $\widehat{\lambda_v}(\chi)$ est non triviale, et provient du fait qu'il s'agit de l'inverse d'une valeur propre du laplacien sur $E(\mathbb{C})$ (voir [BP05], proposition 2.2). Alors, la première somme du membre de droite de (6.3) est positive. En utilisant le lemme A.6 de [BP05] pour majorer $\lambda_t(O)$ (pour $t<1$), on a :

$$\frac{1}{D}\sum_{\substack{1\leqslant i,j\leqslant N\\ (i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geqslant -\left(\sum_{i=1}^N m_i^2\right)\left(\frac{1}{2}\ln\left(\frac{1}{t}\right) + \frac{1}{12}\max(\ln(|j_E|_v),0) + \frac{11}{5}\right)$$
$$- \left[D\left(\sum_{i=1}^N m_i\right)^2 - \left(\sum_{i=1}^N m_i^2\right)\right] t,$$

d'où le résultat en posant

$$t = \frac{\sum_{i=1}^N m_i^2}{2\left[D\left(\sum_{i=1}^N m_i\right)^2 - \left(\sum_{i=1}^N m_i^2\right)\right]} < 1,$$

qui est le réel maximisant le terme de droite. □

À présent, pour $i \geqslant 1$, posons $m_i = 1$, et choisissons $m_0 < 2r + \sqrt{4r^2 + r(2r-3)}$ si $D = 1$: cette inégalité est équivalente à la condition d'application du lemme d'Elkies pondéré (pour $D \geqslant 2$, elle est trivialement toujours vérifiée). On a alors, en injectant dans (6.2) les résultats des lemmes 6.7 (pour les places finies) et 6.8 (pour les places infinies) :

$$\hat{h}(P) \geqslant \frac{1}{D}\frac{m_0\sum_{i=1}^r \ln(p_i) - (m_0^2+r)\left(\frac{1}{2}\ln\left(2D\frac{(m_0+r)^2}{m_0^2+r} - 2\right) + \frac{1}{12}h(j_E) + \frac{27}{10}\right)}{2\left(m_0 + \sum_{i=1}^r p_i\right)(m_0+r)}. \quad (6.4)$$

Il est temps de simplifier la minoration en estimant les sommes indexées par les nombres premiers. On suppose dans un premier temps que HRG est vraie, pour simplifier les calculs. La version inconditionnelle est démontrée dans la dernière section du chapitre.

Lemme 6.9. *Soit $K/\mathbb{Q}$ une extension galoisienne. On a, en admettant HRG, pour tout $s \geqslant 10^5$,*

$$\left|\mathrm{card}(\Pi_s) - \frac{1}{n_K}\mathrm{Li}(s)\right| \leqslant \frac{\alpha_K}{n_K}\sqrt{s}\ln(s),$$

$$\left|\sum_{p\in\Pi_s}\ln(p) - \frac{s}{n_K}\right| \leqslant \frac{\beta_K}{n_K}\sqrt{s}(\ln(s))^2, \text{ et}$$

$$\sum_{p\in\Pi_s} p \leqslant \frac{1}{2n_K}\left[1+\frac{3}{\ln(s)}\right]\frac{s^2}{\ln(s)} + \frac{5}{3}\frac{\alpha_K}{n_K}s^{3/2}\ln(s),$$

où, pour $s \geqslant 10^5$,

$$\frac{s}{\ln(s)} \leqslant \mathrm{Li}(s) \leqslant \left[1+\frac{1{,}3}{\ln(s)}\right]\frac{s}{\ln(s)},$$

et :

$$\alpha_K = 59{,}07 + 1{,}44\ln(|d_K|) + 4{,}35n_K,$$

$$\beta_K = 8{,}72 + 0{,}47\ln(|d_K|) + 3{,}30n_K.$$

Démonstration. L'inégalité (2.40) et le théorème 1.8 donnent exactement les deux premières inégalités. La dernière s'obtient facilement en partant d'une transformation d'Abel :

$$\sum_{p\in\Pi_s} p = \int_1^s t\mathrm{d}\pi(t) = s\pi(s) - \int_2^s \pi(t)\mathrm{d}t,$$

où $\pi(s) = \mathrm{card}(\Pi_s)$, qu'on vient d'estimer. Le calcul de la dernière intégrale provient donc essentiellement des estimations de $\int_2^s \frac{t^a}{(\ln(t))^b}\mathrm{d}t$ pour $b > 0$ et $a > -1$, affinées avec une intégration par parties et une relation de Chasles (en scindant l'intégrale en $\sqrt{s}$). □

Remarque 6.10. Des calculs plus lourds, mais sans différence conceptuelle, permettent de démontrer que pour tout entier naturel non nul f, on a

$$\sum_{p\in\Pi_s} p^f \leqslant \frac{1}{n_K}\left[\frac{1}{f+1} + \frac{\gamma_{f,K}}{\ln(s)}\right]\frac{s^{f+1}}{\ln(s)},$$

où $\gamma_{f,K} = 2954 + \left(396 + \frac{2212}{(2f+3)^2}\right)\ln(d_K) + \left(1980 + \frac{10822}{(2f+3)^2}\right)n_K$. La majoration moins bonne que celle du lemme (pour $f = 1$) provient d'estimations moins fines dans le calcul de $\int_2^s \frac{t^{f-1/2}}{\ln(t)}\mathrm{d}t$.

On peut simplifier les inégalités.

Lemme 6.11. *Conservons les notations du lemme précédent, et soit $\varepsilon \in]0,1[$. Alors, sous réserve de la justesse de HRG,*

— *si* $\ln(s) \geqslant 4\ln\left(4\sqrt{\frac{\beta_K}{\varepsilon}e}\ln(4\sqrt{\frac{\beta_K}{\varepsilon}})\right)$, *on a* $\sum_{p\in\Pi_s}\ln(p) \geqslant \frac{1-\varepsilon}{n_K}s$;

— *si* $\ln(s) \geqslant 4\ln\left(4\sqrt{\frac{\alpha_K}{\varepsilon}e}\ln(4\sqrt{\frac{\alpha_K}{\varepsilon}})\right)$, *on a* $\mathrm{card}(\Pi_s) \geqslant (1-\varepsilon)\mathrm{Li}(s) \geqslant \frac{1-\varepsilon}{n_K}\frac{s}{\ln(s)}$.

En particulier, si $s \geqslant 2^{16}\left(\frac{\alpha_K}{\varepsilon}\right)^4$, *ces deux inégalités sont vérifiées.*

Démonstration. Il suffit de résoudre l'inégalité $\frac{s}{n_K} - \frac{\beta_K}{n_K}\sqrt{s}(\ln(s))^2 \geqslant (1-\varepsilon)\frac{s}{n_K}$, et donc d'utiliser le corollaire B.3 (deuxième point, avec $\alpha = \frac{1}{4}$ et $b = \sqrt{\frac{\beta_K}{\varepsilon}}$), pour obtenir la première inégalité voulue, et on procède de même pour la deuxième inégalité. □

Remarque 6.12. Sous la même condition, on a également $\mathrm{card}(\Pi_s) \leqslant \frac{1+\varepsilon}{n_K}\mathrm{Li}(s)$ et $\sum_{p\in\Pi_s} p \leqslant \frac{1}{n_K}\left(\frac{1}{2} + \frac{5\varepsilon}{3} + \frac{3}{\ln(s)}\right)\frac{s^2}{\ln(s)}$.

Soit $m_0 = \sqrt{r}$. On suppose désormais avoir choisi $s \geqslant 10^5$ tel que

$$\sqrt{s\ln(s)} \geqslant 8\sqrt{\frac{3n_{K'}}{2}\left(1 + \frac{1{,}3}{5\ln(10)}\right)}\left(\frac{1}{2}\ln(4Ds) + \frac{1}{12}h(j_E) + 2\right).$$

Ceci est vérifié pour, par exemple (voir corollaire B.3),

$$s \geqslant \max\left(\frac{36n_{K'}\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)^2}{\ln\left(36n_{K'}\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)^2\right)}\sqrt{e}, 36n_{K'}\sqrt{e}\ln(36n_{K'})\right).$$

Prenons donc $s = 2^{20}\alpha_{K'}^4\left[\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right]^2 \cdot \left[\ln\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)\right]^{-1}$. L'inégalité dessus, ainsi que les estimations données par le lemme 6.9 pour $\varepsilon = \frac{1}{2}$ amènent à la minoration suivante :

$$\hat{h}(P) \geqslant \frac{1}{4Dn_{K'}}\frac{s}{\frac{1}{\sqrt{n_{K'}}}\frac{s^2}{\ln(s)}\left(\frac{8}{5\sqrt{n_{K'}}} + \frac{4}{3\sqrt{3e}}\right)\left(\frac{1}{\sqrt{e}} + \frac{4}{3\sqrt{n_{K'}}}\right)\sqrt{\frac{s}{\ln(s)}}} \geqslant \frac{1}{20\sqrt{n_{K'}}D}\left(\frac{\ln(s)}{s}\right)^{3/2},$$

d'où le résultat annoncé dans le théorème 6.1, avec $n_{K'}$ et $\ln(|d_{K'}|)$ au lieu de n_K et $\ln(|d_K|)$: il est important de noter que $D \leqslant [K(P):K]$, et que l'application

$$x \mapsto \frac{1}{x}\left(\frac{\ln\left(4xe^{4+\frac{h(j_E)}{6}}\right)}{\ln\left(\ln\left(4xe^{4+\frac{h(j_E)}{6}}\right)\right)}\right)^3$$

est décroissante pour $x \geqslant 1$, on peut donc bien substituer D par $[K(P) : K]$ dans l'inégalité ci-dessus (avant de la modifier pour l'avoir telle qu'énoncée dans le théorème 6.1).

Pour l'énoncé avec n_K et $\ln(|d_K|)$, on utilise les majorations du lemme suivant.

Lemme 6.13. *On a* $n_{K'} \leqslant 192 n_K$ *et*

$$\ln(|d_{K'}|) \leqslant 384 \ln(|d_K|) + 96 n_K \ln(-d) + 382 n_K \ln(6N_E) + 384 n_K \ln(192),$$

où d *est le discriminant absolu de* $\mathrm{End}(E) \otimes \mathbb{Q}$ *et* N_E *la norme du conducteur de* E.

Démonstration. Commençons par démontrer la première inégalité : on a bien entendu $n_{K'} \leqslant 2[K(\sqrt{d}, E[12]) : K(\sqrt{d})] n_K$, et l'action de $\mathrm{Gal}(K(\sqrt{d}, E[12])/K(\sqrt{d}))$ sur $E[12]$ commute avec les éléments de $\mathrm{End}(E) = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, donc induit une injection

$$\mathrm{Gal}(K(\sqrt{d}, E[12])/K(\sqrt{d})) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/12\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}(E[12]) \simeq \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{12\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}\right)^{\times}.$$

Donc $[K(\sqrt{d}, E[12]) : K(\sqrt{d})] \leqslant 96$, le pire cas étant celui où 2 et 3 sont tous les deux inertes dans $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

La deuxième inégalité, qui lie les différents discriminants, provient des relations de divisibilité entre des discriminants de corps de nombres et celui de leur extension composée, décrites dans l'article [Tôy55]. Puisque K' s'obtient en composant K, $\mathrm{End}(E) \otimes \mathbb{Q}$ et $K(E[12])$, on a :

$$\begin{aligned}\ln(|d_{K'}|) \leqslant \frac{n_{K'}}{n_K} \ln(|d_K|) + \frac{n_{K'}}{2} \ln(-d) \\ + \frac{n_{K'}}{[K(E[12]) : \mathbb{Q}]} \left([K(E[12]) : K] \ln(|d_K|) + \ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K})) \right),\end{aligned}$$

où $\Delta_{K(E[12])/K}$ est le discriminant relatif de l'extension $K(E[12])/K$. Or, la proposition C.1.5 de [HS00] démontre que l'extension $K(E[12])/K$ ne se ramifie au plus qu'en les places de mauvaise réduction et celles de caractéristiques résiduelles 2 et 3. La proposition 5 de [Ser81] établit l'inégalité :

$$\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K})) \leqslant [K(E[12]) : \mathbb{Q}] \left(1 - \frac{1}{192}\right) \sum_{\substack{\mathfrak{p} | p \\ \mathfrak{p} \text{ ram.}}} \ln(p) + [K(E[12]) : \mathbb{Q}] \ln(192),$$

parce que $[K(E[12]) : K] \leqslant 192$. On en déduit que

$$\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K})) \leqslant 191 n_K \ln(6N_E) + 192 n_K \ln(192),$$

d'où le résultat. □

Ceci démontre le théorème principal conditionnel complètement.

6.3 Minoration inconditionnelle

Pour s'affranchir de l'hypothèse de Riemann généralisée, peu de choses sont à modifier : le fil de la démonstration reste le même. Seules les estimations des lemmes 6.9 et 6.11 sont à adapter (et, de fait, le choix de s en bout de course).

Lemme 6.14. *Soit $K/\mathbb{Q}$ une extension galoisienne, et soit β_0 l'éventuel zéro de Siegel de ζ_K. Notons $M_K = \exp(110000 n_K (\ln(9d_K^8))^2)$. On a, pour tout $s \geqslant M_K$,*

$$\left|\mathrm{card}(\Pi_s) - \frac{1}{n_K}\left(\mathrm{Li}(s) - \frac{s^{\beta_0}}{\ln(s^{\beta_0})}\right)\right| \leqslant \frac{3{,}37\cdot 10^{13}}{n_K} s \exp\left(-\frac{1}{12}\sqrt{\frac{\ln(s)}{n_K}}\right),$$

$$\left|\sum_{p\in\Pi_s} \ln(p) - \frac{s}{n_K}\left(1 - \frac{s^{\beta_0-1}}{\beta_0}\right)\right| \leqslant \frac{3{,}5\cdot 10^{12}}{n_K} s \exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right), \text{ et}$$

$$\sum_{p\in\Pi_s} p \leqslant \frac{s^2}{2n_K\ln(s)}\left[1 + \frac{1{,}00001}{\ln(s)} + 4{,}24\cdot 10^{13}\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right) + \frac{8}{\beta_0(\beta_0+1)}\frac{1}{s^{1-\beta_0}}\right],$$

où, pour $s \geqslant M_K$,

$$\frac{s}{\ln(s)} \leqslant \mathrm{Li}(s) \leqslant \left[1 + \frac{1{,}00001}{\ln(s)}\right]\frac{s}{\ln(s)}.$$

Les termes contenant β_0 peuvent être supprimés en l'absence de zéro de Siegel.

Démonstration. Les deux premières inégalités proviennent du théorème 1.7 et de l'inégalité (2.41) ; la deuxième inégalité est même valable pour $s \geqslant \sqrt{M_K}$. La troisième inégalité se calcule par une autre transformation d'Abel, puisqu'on a :

$$\sum_{p\in\Pi_s} p = \frac{s\theta(s)}{\ln(s)} - \int_2^s \theta(x)\left(\frac{1}{\ln(x)} - \frac{1}{(\ln(x))^2}\right)\mathrm{d}x,$$

où $\theta(s) = \sum_{p\in\Pi_s} \ln(p)$. On suppose à présent $s \geqslant M_K$, en minorant trivialement par zéro l'intégrande sur l'intervalle $[2, \sqrt{s}]$. La seule difficulté inédite réside dans l'estimation suivante, nécessaire à cause de l'intégration du terme d'erreur du théorème de Chebotarev inconditionnel, et qu'on obtient par intégration par parties :

$$\int_{\sqrt{s}}^s x\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(x)}{n_K}}\right)\mathrm{d}x \leqslant \left(1 + \frac{1}{8\sqrt{n_K\ln(s)}}\right)\frac{s^2}{2}\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right). \qquad \square$$

Remarque 6.15. Utilisant le lemme 2.17 et le corollaire 2.26, on peut fournir une majoration de la somme des nombres premiers de Π_s qui ne dépend pas de β_0, toujours pour $s \geqslant M_K$:

$$\sum_{p\in\Pi_s} p \leqslant \frac{s^2}{2n_K\ln(s)}\left[1{,}00001 + 6{,}37\exp\left(\frac{12|d_K|^{2709}e^{387(26n_K+32)}}{n_K} - \frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right)\right].$$

On a utilisé la majoration $s^{\beta_0-1} \leqslant \exp\left(\frac{1}{16^2(1-\beta_0)n_K}\right)\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right)$ (si β_0 n'existe pas, l'inégalité ci-dessus reste évidemment valable).

Lemme 6.16. *Conservons les notations du lemme précédent, et soit $\varepsilon \in]0,1[$. Posons $B_K = 3072|d_K|^{2709}e^{387(26n_K+32)}$. Alors,*

— *si $s \geqslant \left(\frac{2,2}{\varepsilon}\right)^{B_K}\exp\left(64n_K\left(\ln\left(\frac{7\cdot 10^{12}}{\varepsilon}\right)\right)^2\right)$, on a $\sum\limits_{p\in\Pi_s}\ln(p) \geqslant \frac{1-\varepsilon}{n_K}s$.*

— *si $s \geqslant \left(\frac{2}{\varepsilon}\right)^{B_K}\exp\left(\frac{\varepsilon}{1{,}685\cdot 10^{13}}\right)$, on a $\mathrm{card}(\Pi_s) \geqslant \frac{1-\varepsilon}{n_K}\frac{s}{\ln(s)}$.*

Démonstration. Supposons d'abord que le zéro de Siegel β_0 existe pour ζ_K. Alors, l'inégalité $\sum\limits_{p\in\Pi_s}\ln(p) \geqslant \frac{1-\varepsilon}{n_K}s$ est vraie sous l'hypothèse suffisante que :

$$\varepsilon \geqslant \frac{1}{\beta_0 s^{1-\beta_0}} + 3{,}5\cdot 10^{12}\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right).$$

Dans ce cas, cette inégalité est vérifiée si $s \geqslant \max\left[\left(\frac{2}{\beta_0\varepsilon}\right)^{\frac{1}{1-\beta_0}}, \exp\left(64n_K\left(\ln\left(\frac{7\cdot 10^{12}}{\varepsilon}\right)\right)^2\right)\right]$. Le corollaire 2.26 permet de majorer β_0, d'où l'inégalité requise. Si β_0 n'existe pas, il suffit de prendre $s \geqslant \exp\left(64n_K\left(\ln\left(\frac{3{,}5\cdot 10^{12}}{\varepsilon}\right)\right)^2\right)$, donc la borne du premier cas convient encore. On procède de même pour la deuxième estimation. □

Reprenons la démonstration esquissée dans la troisième section, jusqu'à l'inégalité (6.4), avec encore une fois le choix $m_0 = \sqrt{r}$ (rappelons que $r = \mathrm{card}(\Pi_s)$). Notons que $X \mapsto \frac{X}{\exp\left(\frac{1}{12}\sqrt{\frac{X}{n_{K'}}}\right)}$ décroît à partir de $X \geqslant 576n_{K'}$, donc en particulier

$$\frac{\ln(s)}{\exp\left(\frac{1}{12}\sqrt{\frac{\ln(s)}{n_{K'}}}\right)} \leqslant \frac{\ln(M_{K'})}{\exp\left(\frac{1}{12}\sqrt{\frac{\ln(M_{K'})}{n_{K'}}}\right)} \leqslant \frac{\ln(M_{K'})}{\exp(40\sqrt{\ln(|d_{K'}|)})} \leqslant 298.$$

On suppose avoir choisi $s \geqslant \max\left[M_{K'}, \left(\frac{2,2}{\varepsilon}\right)^{B_{K'}}\exp\left(64n_{K'}\left(\ln\left(\frac{7\cdot 10^{12}}{\varepsilon}\right)\right)^2\right)\right]$ tel que :

$$\sqrt{s\ln(s)} \geqslant 8\sqrt{300n_{K'}}\left(\frac{1}{2}\ln(4Ds) + \frac{1}{12}h(j_E) - 13\right).$$

Ceci est vérifié pour

$$s \geqslant \max\left(\frac{19200n_{K'}\left(\ln\left(4De^{2h(j_E)-26}\right)\right)^2}{\ln\left(19200n_{K'}\left(\ln\left(4De^{2h(j_E)-26}\right)\right)^2\right)}\sqrt{e}, 19200n_{K'}\sqrt{e}\ln(19200n_{K'})\right).$$

On remplace l'emploi du lemme 6.11, que nous avions appliqué avec $\varepsilon = \frac{1}{2}$, par l'application du lemme 6.16 que nous venons de démontrer. Alors, prenant

$$s = \left[\ln\left(4De^{4+2h(j_E)}\right)\right]^2 \left[\ln\left(\ln\left(4De^{4+2h(j_E)}\right)\right)\right]^{-1} \exp\left(1{,}5B_{K'}\right),$$

l'inégalité (6.4) amène à la minoration suivante :

$$\hat{h}(P) \geqslant \frac{1}{4\sqrt{n_{K'}}D} \frac{1}{13\left(13{,}14 + 6{,}37 \cdot 10^{-4754}\exp\left(B_{K'}\right)\right)} \left(\frac{\ln(s)}{s}\right)^{3/2},$$

d'où le résultat annoncé dans le théorème 6.1, avec $n_{K'}$ et $\ln(|d_{K'}|)$ au lieu de n_K et $\ln(|d_K|)$; là encore, on peut bien substituer D par $[K(P) : K]$ dans l'inégalité ci-dessus. On utilise le lemme 6.13 pour conclure.

Annexe A

Hauteur sur une courbe elliptique semi-stable

A.1 Classification de Kodaira-Néron

Pour formuler au mieux le théorème de classification, introduisons encore une notation.

Proposition A.1. *Soient E/K une courbe elliptique de modèle minimal régulier $\mathcal{E} \to B$, dont on note la section neutre $\mathcal{O}$, W un modèle de Weierstrass de E, et $\mathfrak{p}$ un idéal maximal de $\mathfrak{p}$. On note $E_{0,\mathfrak{p}}(K) \subseteq E(K)$ l'ensemble des points K-rationnels dont la réduction modulo $\mathfrak{p}$ dans W est un point non singulier. Alors $E_{0,\mathfrak{p}}(K)$ est également l'ensemble des points rationnels dont l'image dans $\mathcal{E}_\mathfrak{p}$ est dans la même composante irréductible que $\mathcal{O}(\mathfrak{p})$. On l'appelle donc « composante identité ».*

Théorème A.2 (Classification de Kodaira-Néron, [Sil94], théorème IV.8.2)**.** *Soit E/K une courbe elliptique de modèle minimal régulier $\mathcal{E} \to B$ et $\mathfrak{p}$ un idéal maximal de K. La fibre $\mathcal{E}_\mathfrak{p}$ a une des formes suivantes (les multiplicités des composantes sont indiquées dans le tableau de la figure A.1) :*

- *type* I_0 *: la fibre $\mathcal{E}_\mathfrak{p}$ est une courbe elliptique ;*
- *type* I_1 *: la fibre $\mathcal{E}_\mathfrak{p}$ est une courbe rationnelle avec un nœud ;*
- *type* I_n*, $n \geqslant 2$: la fibre $\mathcal{E}_\mathfrak{p}$ est l'union de n droites (projectives) qui s'arrangent selon un polygone ;*
- *type* II *: la fibre $\mathcal{E}_\mathfrak{p}$ est une courbe rationnelle avec une pointe ;*
- *type* III *: la fibre $\mathcal{E}_\mathfrak{p}$ consiste en deux courbes rationnelles qui se coupent tangentiellement en un point ;*
- *type* IV *: la fibre $\mathcal{E}_\mathfrak{p}$ est l'union de trois droites qui se coupent en un seul point ;*
- *type* I_0^* *: la fibre $\mathcal{E}_\mathfrak{p}$ est une droite de multiplicité 2 coupé par quatre droites de multiplicité 1 ;*

— *type* I_n^* *: la fibre* $\mathcal{E}_\mathfrak{p}$ *est une « chaîne » de* $n+1$ *droites de multiplicité 2, avec deux droites de multiplicité 1 qui coupent chacune des droites aux extrémités ;*
— *type* IV^* *: la fibre* $\mathcal{E}_\mathfrak{p}$ *consiste en sept droites agencées comme dans le tableau ci-contre ;*
— *type* III^* *: la fibre* $\mathcal{E}_\mathfrak{p}$ *consiste en huit droites agencées comme dans le tableau ci-contre ;*
— *type* III^* *: la fibre* $\mathcal{E}_\mathfrak{p}$ *consiste en neuf droites agencées comme dans le tableau ci-contre.*

Le cas I_0 *correspond au cas de bonne réduction,* I_n *au cas de mauvaise réduction multiplicative, et tous les autres cas sont de type additif.*

Nous utiliserons la notation de Kodaira dans ce chapitre.

Remarque A.3. Pour chaque type de réduction, si on note Γ_i les composantes irréductibles de la fibre $\mathcal{E}_\mathfrak{p}$ et n_i leurs multiplicités, alors le théorème de l'indice de Hodge assure que $n_i\langle\Gamma_i,\Gamma_i\rangle = -\sum_{j\neq i} n_j\langle\Gamma_i,\Gamma_j\rangle$, et la classification de Kodaira-Néron nous permet de calculer le membre de droite dans chaque cas, pour trouver *a posteriori* que les composantes irréductibles ont pour auto-intersection -2. Ce n'est cependant qu'un raccourci pour retrouver ce fait bien connu qu'on utilise dans le corollaire A.8 ; sachant qu'on démontre justement le théorème de classification par ces calculs d'intersections, le serpent se mordrait la queue si nous n'avions pas un autre recours pour les calculer : la formule d'adjonction, que nous n'avons formulée que pour les sections d'une surface arithmétique.

Remarque A.4. L'uniformisation de Tate exposée dans la proposition 5.13 permet de réinterpréter l'isomorphisme $E(K)/E_{0,\mathfrak{p}}(K) \simeq \mathbb{Z}/n\mathbb{Z}$ dans le cas de mauvaise réduction multiplicative, suivant la remarque IV.9.6 de [Sil94] : soit E/K une courbe elliptique sur un corps de nombres et $\mathfrak{p}$ un idéal premier de mauvaise réduction multiplicative. On note $r_\mathfrak{p}$ la composition des applications

$$E(\bar{K}_\mathfrak{p}) \simeq \bar{K}_\mathfrak{p}^*/q^\mathbb{Z} \to \mathbb{Q}/\mathbb{Z},$$

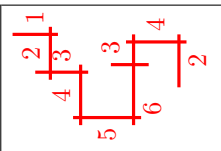
où la dernière application est $u \mapsto \frac{\ln(|u|_v)}{\ln(|q|_v)}$. On l'appelle morphisme de rétraction (et le cercle $\mathbb{Q}/\mathbb{Z}$ est le squelette de E).

L'isomorphisme $K_\mathfrak{p}^*/q^\mathbb{Z} \simeq E(K_\mathfrak{p})$, où $|q|_\mathfrak{p} = |j_E|_\mathfrak{p}^{-1}$, identifie les sous-groupes $\mathcal{O}_{K_\mathfrak{p}}$ et $E_0(K_\mathfrak{p})$, et induit des isomorphismes

$$E(K_\mathfrak{p})/E_0(K_\mathfrak{p}) \simeq K_\mathfrak{p}^*/q^\mathbb{Z}\mathcal{O}_{K_\mathfrak{p}}^* \simeq \mathbb{Z}/n\mathbb{Z},$$

où le deuxième isomorphisme est induit par la valuation $v_\mathfrak{p}$ et $n = v_\mathfrak{p}(q) = v_\mathfrak{p}(\Delta)$. De là, on parvient à l'égalité $r_\mathfrak{p}(P) = \frac{u(P)}{n} \bmod \mathbb{Z}$, où $u(P)$ est l'image de P dans $E(K_\mathfrak{p})/E_{0,\mathfrak{p}}(K_\mathfrak{p}) \simeq \mathbb{Z}/n\mathbb{Z}$.

FIGURE A.1 – Classification de Kodaira-Néron.

Kodaira	I_0	$\mathrm{I}_n, n \geqslant 1$	II	III	IV	I_0^*	I_n^*	IV^*	III^*	II^*
Néron	A	B_n	C_1	C_2	C_3	C_4	$\mathrm{C}_{5,n}$	C_6	C_7	C_8
Fibre										
$\mathcal{E}_{\mathrm{p}}^0(k)$	$\tilde{E}(k)$	k^*	k	k	k	k	k	k	k	k
Nbre comp.	1	n	1	2	3	5	$5+n$	7	8	9
$v_{\mathrm{p}}(\Delta(E/K))$	0	n	2	3	4	6	$6+n$	8	9	10
$\frac{E(K)}{E_{0,\mathrm{p}}(K)}$	0	$\frac{\mathbb{Z}}{n\mathbb{Z}}$	0	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$	$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ (n pair) $\frac{\mathbb{Z}}{4\mathbb{Z}}$ (n impair)	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	0

Corollaire A.5. *Soit E/K une courbe elliptique semi-stable, et $\Delta(E/K)$ son discriminant minimal. Alors :*

$$\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))) = \sum_{\mathfrak{p}} \delta_{\mathfrak{p}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})),$$

où $\delta_{\mathfrak{p}}$ est le nombre de points singuliers dans la fibre $\mathcal{E}_{\mathfrak{p}}$ du modèle minimal régulier.

Démonstration. On le voit immédiatement en regardant la structure des fibres spéciales dans le cas I_n de mauvaise réduction multiplicative, en notant que $v_{\mathfrak{p}}(\Delta(E/K))$ égale le nombre de composantes irréductibles de la fibre $\mathcal{E}_{\mathfrak{p}}$, qui est également le nombre de points singuliers. □

En particulier, le discriminant minimal d'une courbe elliptique semi-stable reste traçable par extension de corps, comme on pouvait le présager (puisque le type de réduction ne change pas dans le cas semi-stable).

Corollaire A.6. *Soient E/K une courbe elliptique semi-stable, L une extension finie de K, et $\mathfrak{p}$ un idéal premier de mauvaise réduction multiplicative sur K. Alors :*

$$\sum_{\mathfrak{P}|\mathfrak{p}} n_{\mathfrak{P}} \ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta(E/L))|_{\mathfrak{P}}) = [L:K] n_{\mathfrak{p}} \ln(|\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))|_{\mathfrak{p}}).$$

En particulier, $\ln(\mathrm{N}_{L/\mathbb{Q}}(\Delta(E/L))) = [L:K]\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K)))$.

Démonstration. Le modèle minimal régulier sur $\mathcal{O}_L$ est obtenu en résolvant les points doubles de $\mathcal{X} \times_{\mathcal{O}_K} \mathrm{Spec}(\mathcal{O}_L)$. D'après [Liu02], corollaire 10.3.25, un point double sur la fibre de $\mathcal{X} \times_{\mathcal{O}_K} \mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_L)$ au-dessus de l'idéal maximal $\mathfrak{P}$ se résout par un éclatement en $e_{\mathfrak{P}} - 1$ composantes irréductibles de multiplicité 1 et isomorphes à des droites $\mathbb{P}^1_{k(\mathfrak{P})}$ d'auto-intersection -2, où $k(\mathfrak{P})$ est le corps résiduel de $\mathfrak{P}$ et $e_{\mathfrak{P}}$ l'indice de ramification de $\mathfrak{P}$ sur K. Ceci prouve le résultat, conjointement à la formule du corollaire précédent : on a en effet,

$$\begin{aligned}\sum_{\mathfrak{P}|\mathfrak{p}} n_{\mathfrak{P}} \ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_{\mathfrak{P}}) &= -\sum_{\mathfrak{P}|\mathfrak{p}} \delta_{\mathfrak{P}} \ln(\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P})) = -\delta_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} \ln(\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P})) \\ &= -\delta_{\mathfrak{p}} \ln(\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p})) = -\delta_{\mathfrak{p}}[L:K]\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) \\ &= [L:K] n_{\mathfrak{p}} \ln(|\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))|_{\mathfrak{p}}).\end{aligned}$$ □

A.2 Hauteurs locales, et cas d'un point algébrique

Par souci d'intelligibilité je traite d'abord le cas, certes général, d'une courbe elliptique avec tous types de réduction, mais en me restreignant aux points rationnels. Le théorème 5.29 nous permet alors de retrouver l'expression de la hauteur d'un

point rationnel en facteurs locaux dont la valeur dépend, essentiellement, du type de réduction du point ; on parle simplement de décomposition en hauteurs locales. En effet, appliquant ce théorème avec $D_1 = D_2 = (P) - (O)$, où $P \in E(K)$, on a :

$$\begin{aligned}\hat{h}(P) &= -\frac{1}{2[K:\mathbb{Q}]}\langle \mathcal{P} - \mathcal{O} + [\mathcal{P} - \mathcal{O}], \mathcal{P} - \mathcal{O} + [\mathcal{P} - \mathcal{O}]\rangle \\ &= -\frac{1}{2[K:\mathbb{Q}]}\langle \mathcal{P} - \mathcal{O} + [\mathcal{P} - \mathcal{O}], \mathcal{P} - \mathcal{O}\rangle,\end{aligned}$$

puisque $\langle \mathcal{P} - \mathcal{O} + [\mathcal{P} - \mathcal{O}], [\mathcal{P} - \mathcal{O}]\rangle = 0$ par définition de $[\mathcal{P} - \mathcal{O}]$. Donc finalement, après développement :

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]}\left(\langle \mathcal{P}, \mathcal{O}\rangle - \frac{1}{2}\langle \mathcal{P} - \mathcal{O}, [\mathcal{P} - \mathcal{O}]\rangle - \langle \mathcal{O}, \mathcal{O}\rangle - \langle \mathcal{P}, \mathcal{P}\rangle\right).$$

Pour que cette formule soit utilisable, on doit d'une part calculer les auto-intersections, puis d'autre part déterminer $[\mathcal{P} - \mathcal{O}]$ et calculer son intersection avec $\mathcal{P} - \mathcal{O}$. À ce stade, néanmoins, on peut déjà deviner pourquoi la hauteur peut s'écrire en termes locaux qui dépendent de la composante où P se réduit modulo chaque idéal premier : cela provient du second nombre d'intersection.

Supposons provisoirement avoir déterminé $[\mathcal{P} - \mathcal{O}]$: si $\Gamma_{i,\mathfrak{p}}$ est une composante de la fibre $\mathcal{E}_\mathfrak{p}$ (sous-entendu que $\Gamma_{0,\mathfrak{p}}$ contient $\mathcal{O}(\mathfrak{p})$), on note $a_{i,\mathfrak{p}}$ la multiplicité à laquelle elle apparaît dans $[\mathcal{P} - \mathcal{O}]$; il est facile de montrer qu'on peut toujours prendre $a_{0,\mathfrak{p}} = 0$. Alors, en utilisant la classification de Néron-Kodaira, ainsi que le fait qu'un point rationnel de E se réduit nécessairement en un point lisse (donc, en particulier, en une unique composante de multiplicité un ; voir 4.2), on obtient sans peine la formule :

$$\frac{1}{2}\langle \mathcal{P} - \mathcal{O}, [\mathcal{P} - \mathcal{O}]\rangle_K = \frac{1}{2}\langle \mathcal{P}, [\mathcal{P} - \mathcal{O}]\rangle_K = \sum_\mathfrak{p} \frac{a_{j_\mathfrak{p},\mathfrak{p}}}{2}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})),$$

où $j_\mathfrak{p}$ est l'indice de la composante où P se réduit modulo $\mathfrak{p}$. En effet, en décomposant l'intersection globale en somme d'intersections locales et en développant autant que possible, on se ramène exclusivement à des calculs d'intersections de la forme $a_{j,\mathfrak{p}}\langle \mathcal{P}, \Gamma_{j,\mathfrak{p}}\rangle_\mathfrak{p}$, qui sont nuls sauf pour $j = j_\mathfrak{p}$.

Il reste à déterminer $a_{j_\mathfrak{p},\mathfrak{p}}$; si $P \in E_{0,\mathfrak{p}}(K)$, alors $\mathcal{P} - \mathcal{O}$ est d'intersection nulle avec tous les diviseurs verticaux contenus dans $\mathcal{E}_\mathfrak{p}$, donc on peut prendre

$$\mathrm{supp}([\mathcal{P} - \mathcal{O}]) \cap \mathrm{supp}(\mathcal{E}_\mathfrak{p}) = \emptyset,$$

et en particulier $a_{j_\mathfrak{p},\mathfrak{p}} = 0$. Supposons à présent que la fibre $\mathfrak{p}$ admet au moins deux composantes, que l'on note $\Gamma_{0,\mathfrak{p}}, \ldots, \Gamma_{n_\mathfrak{p}-1,\mathfrak{p}}$, et que P n'appartient pas à $E_{0,\mathfrak{p}}(K)$. Si M est la matrice $((\langle \Gamma_{i,\mathfrak{p}}, \Gamma_{j,\mathfrak{p}}\rangle))_{1\leqslant i,j\leqslant n_\mathfrak{p}-1}$, alors cette matrice est inversible par le

théorème 4.18, et $a_{j_\mathfrak{p},\mathfrak{p}}$ est le coefficient $(j_\mathfrak{p}, j_\mathfrak{p})$ de $-M^{-1}$. On le voit en résolvant le système matriciel équivalent à

$$\langle \mathcal{P} - \mathcal{O} + \sum_{\mathfrak{p}'} \sum_{j'} a_{j',\mathfrak{p}'} \Gamma_{j',\mathfrak{p}'}, \Gamma_{j,\mathfrak{p}} \rangle = 0$$

pour tous j et $\mathfrak{p}$. Pour résumer,

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \left(\langle \mathcal{P}, \mathcal{O} \rangle_K + \frac{1}{2} \sum_{\mathfrak{p}} a_{j_\mathfrak{p},\mathfrak{p}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) - \langle \mathcal{O}, \mathcal{O} \rangle - \langle \mathcal{P}, \mathcal{P} \rangle \right).$$

Lemme A.7. *Soient E/K une courbe elliptique de modèle minimal régulier $\mathcal{E} \to B$ et P un point rationnel. Soit $\mathfrak{p}$ un idéal premier de mauvaise réduction. Si $P \in E_{0,\mathfrak{p}}(K)$, on peut prendre $a_{j_\mathfrak{p},\mathfrak{p}} = 0$. Sinon, selon le type de réduction :*

Type	I_n	III	IV	I_0^*	IV^*	III^*	I_n^*
$a_{j_\mathfrak{p},\mathfrak{p}}$	$\frac{j_\mathfrak{p}(n-j_\mathfrak{p})}{n}$	$\frac{1}{2}$	$\frac{1}{3}$	1	$\frac{4}{3}$	$\frac{3}{2}$	1 *si* $P(\mathfrak{p}) \in \Gamma_1$ $1+\frac{n}{4}$ *sinon*

Dans tous les cas non mentionnés (I_0, II, II^**), on a nécessairement $P \in E_{0,\mathfrak{p}}(K)$.*

Démonstration. C'est une simple conséquence du calcul de la matrice M citée ci-dessus et de son inverse ; les auto-intersections valent -2 d'après la remarque A.3. On résume la situation dans la figure A.3, où les composantes sont numérotées (arbitrairement) en commençant par les composantes de multiplicité un, sauf dans le cas I_n^* où la numérotation importe (figure A.2). □

Dans le cas semi-stable, on obtient alors une expression limpide de la hauteur.

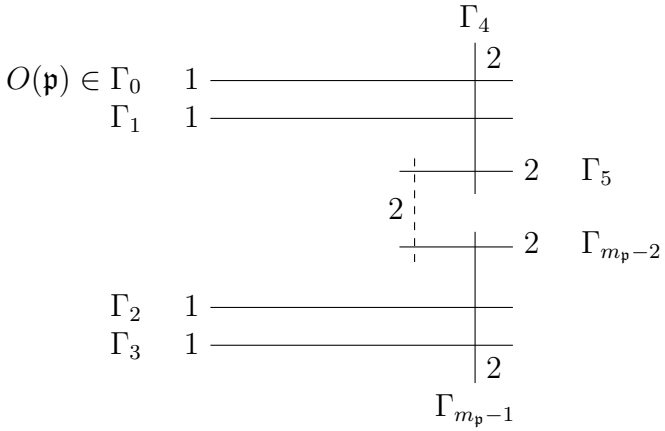
Théorème A.8. *Soient E/K une courbe elliptique semi-stable, et* M *l'ensemble des idéaux premiers de mauvaise réduction (multiplicative). Alors, pour tout $P \in E(K)$,*

$$[K:\mathbb{Q}]\hat{h}(P) = \langle P, O \rangle_K - \frac{1}{2} \sum_{\mathfrak{p} \in \mathrm{M}} [K_\mathfrak{p} : \mathbb{Q}_p] B_2\left(r_\mathfrak{p}(P)\right) \ln(|\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))|_\mathfrak{p}),$$

où $r_\mathfrak{p}$ est le morphisme de rétraction de la remarque A.4.

Démonstration. C'est une conséquence immédiate du lemme précédent et de la formule (5.5), valable pour une courbe elliptique semi-stable, qui détermine les deux auto-intersections ; on remplace d'abord $\frac{j_\mathfrak{p}}{n}$, où $j_\mathfrak{p}$ est la composante du polygone où P se réduit, par $\frac{j_\mathfrak{p}}{v_\mathfrak{p}(\Delta(E/K))}$ grâce à la classification de Kodaira-Néron (figure A.1), puis par $r_\mathfrak{p}(P)$ par la remarque A.4. □

FIGURE A.2 – Structure de la fibre dans le cas I_n^* (un point rationnel se réduit en Γ_i pour $i \in \{0,1,2,3\}$, et $m_\mathfrak{p} = 5+n$).



Remarque A.9. En pratique, dans le cas de mauvaise réduction de type additif, on préfère remplacer P par $[12]P$ dans notre étude. En effet, comme le groupe des composantes est nécessairement, dans ce cas, de cardinal inférieur ou égal à 4 (donc divisant 12), on se ramène ainsi au cas où le point est dans la composante neutre.

Corollaire A.10 (Hauteurs locales)**.** *Soit E/K une courbe elliptique semi-stable. Pour toute place v, il existe des fonctions $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$ vérifiant les propriétés suivantes :*

- *elles sont continues sur $E(K_v) \setminus \{O\}$ et bornées sur le complément de tout voisinage v-adique de O (pour la topologie la plus fine sur $E(K_v)$ qui rend toutes les applications $E(K_v) \setminus \{\text{pôles de } f\} \to \mathbb{R}, P \mapsto |f(P)|_v$, pour $f \in K(E)$, continues) ;*
- *la limite $\lim_{P\to O} \left(\lambda_v(P) - \frac{\langle P,O\rangle_v}{n_v}\right)$ existe ;*
- *fixons une équation de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ sur K_v, de discriminant Δ ; alors, pour tout $P \in E(K_v)$ tel que $[2]P \neq O$,*

$$\lambda_v([2]P) = 4\lambda_v(P) - \ln(|(2y + a_1x + a_3)(P)|_v) + \frac{1}{4}\ln(|\Delta|_v)$$

(autrement dit, λ_v est « presque » quadratique) ;

et telles que pour tout $P \in E(K_v) \setminus \{O\}$,

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K} n_v\lambda_v(P).$$

Les fonctions λ_v ne dépendent pas de l'équation de Weierstrass choisie. On les appelle hauteurs locales de Néron-Tate.

FIGURE A.3 – Matrice d'incidence selon chaque type de réduction.

Type	M	$-M^{-1}$
I_n	$\begin{pmatrix} -2 & 1 & 0 & \cdots & 0 \\ 1 & -2 & 1 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & 1 & -2 & 1 \\ 0 & \cdots & 0 & 1 & -2 \end{pmatrix}$	j-ième ligne $\to \frac{1}{n}\begin{pmatrix} n-j \\ 2(n-j) \\ \vdots \\ j(n-j) \\ \vdots \\ 2j \\ j \end{pmatrix}_{1\leqslant j\leqslant n-1}$
III	(-2)	$\left(\frac{1}{2}\right)$
IV	$\begin{pmatrix} -2 & 1 \\ 1 & -2 \end{pmatrix}$	$\frac{1}{3}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
I_0^*	$\begin{pmatrix} -2 & 0 & 0 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & 0 & -2 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix}$	$\frac{1}{2}\begin{pmatrix} 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 4 \end{pmatrix}$
IV^*	$\begin{pmatrix} -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 0 & 0 & 1 \\ 1 & 0 & 0 & -2 & 0 & 1 \\ 0 & 1 & 0 & 0 & -2 & 1 \\ 0 & 0 & 1 & 1 & 1 & -2 \end{pmatrix}$	$\frac{1}{3}\begin{pmatrix} 4 & 2 & 3 & 5 & 4 & 6 \\ 2 & 4 & 3 & 4 & 5 & 6 \\ 3 & 3 & 6 & 6 & 6 & 9 \\ 5 & 4 & 6 & 10 & 8 & 12 \\ 4 & 5 & 6 & 8 & 10 & 12 \\ 6 & 6 & 9 & 12 & 12 & 18 \end{pmatrix}$
III^*	$\begin{pmatrix} -2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & -2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -2 \end{pmatrix}$	$\frac{1}{2}\begin{pmatrix} 3 & 2 & 4 & 4 & 5 & 3 & 6 \\ 2 & 4 & 4 & 6 & 6 & 4 & 8 \\ 4 & 4 & 8 & 8 & 10 & 6 & 12 \\ 4 & 6 & 8 & 12 & 12 & 8 & 16 \\ 5 & 6 & 10 & 12 & 15 & 9 & 18 \\ 3 & 4 & 6 & 8 & 9 & 7 & 12 \\ 6 & 8 & 12 & 16 & 18 & 12 & 24 \end{pmatrix}$
I_n^*	$\begin{pmatrix} -2 & 0 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & -2 & 0 & 0 & \cdots & \cdots & 0 & 1 \\ 0 & 0 & -2 & 0 & \ddots & 0 & \vdots & 1 \\ 1 & 0 & 0 & -2 & 1 & \ddots & \vdots & 0 \\ 0 & \vdots & \ddots & 1 & -2 & \ddots & 0 & \vdots \\ \vdots & \vdots & 0 & \ddots & \ddots & \ddots & 1 & 0 \\ \vdots & 0 & \cdots & \cdots & 0 & \ddots & -2 & 1 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 1 & -2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 1 & \cdots & \cdots & \cdots & 1 \\ \frac{1}{2} & \frac{m_\mathfrak{p}-1}{4} & \frac{m_\mathfrak{p}-3}{4} & 1 & \frac{3}{2} & 2 & \cdots & \frac{m_\mathfrak{p}-3}{2} \\ \frac{1}{2} & \frac{m_\mathfrak{p}-3}{4} & \frac{m_\mathfrak{p}-1}{4} & 1 & \frac{3}{2} & 2 & \cdots & \frac{m_\mathfrak{p}-3}{2} \\ 1 & 1 & 1 & 2 & \cdots & \cdots & \cdots & 2 \\ \vdots & \frac{3}{2} & \frac{3}{2} & \vdots & 3 & \cdots & \cdots & 3 \\ \vdots & 2 & 2 & \vdots & \vdots & 4 & \cdots & 4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \frac{m_\mathfrak{p}-3}{2} & \frac{m_\mathfrak{p}-3}{2} & 2 & 3 & 4 & \cdots & m_\mathfrak{p}-4 \end{pmatrix}$ (on a $n = m_\mathfrak{p} - 5 = v_\mathfrak{p}(\Delta(E/K)) - 6$)

Démonstration. Il suffit de poser

$$\lambda_v(P) = \frac{\langle P, O\rangle_v}{n_v} - B_2(r_v(P))\ln(|\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))|_v)$$

pour v une place finie de mauvaise réduction multiplicative, et $\lambda_v(P) = n_v^{-1}\langle P, O\rangle_v$ sinon. La décomposition en termes locaux et la deuxième propriété sont alors évidentes par définition et par le théorème A.8, tandis que la première propriété provient essentiellement de la proposition 4.10. La démonstration de la troisième propriété est plus fastidieuse, on peut la trouver dans [Sil09] : voir la démonstration du théorème VI.4.2. On peut aussi consulter la démonstration du théorème principal de [BM12], qui utilise essentiellement la même approche que nous (attention, cependant, à la différence de normalisation dans la définition de l'intersection locale). □

Remarque A.11. Comparons les expressions des hauteurs locales archimédiennes

$$\lambda_v(z) = -\frac{1}{2}B_2\left(\frac{\ln(|u|_v)}{\ln(|q|_v)}\right)\ln(|q|_v) - \ln(|1-u|_v) - \sum_{n=1}^{\infty}\ln\left(\left|(1-q^n u)\left(1-q^n u^{-1}\right)\right|_v\right),$$

où $u = e^{2i\pi z}$, $q = e^{2i\pi\tau_v}$, avec τ_v tel que $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$, et des hauteurs locales aux places finies de mauvaise réduction multiplicative

$$\lambda_v(P) = -\frac{1}{2}B_2\left(\frac{\ln(|u|_v)}{\ln(|q|_v)}\right)\ln(|q|_v) - \ln(|1-u|_v) - \sum_{n=1}^{\infty}\ln\left(\left|(1-q^n u)\left(1-q^n u^{-1}\right)\right|_v\right),$$

où u est un représentant de l'image de P dans $\bar{K}_v^*/q^{\mathbb{Z}}$ et $q = |j_E|_v^{-1}$ (si on prend u tel que $0 \leqslant -\ln(|u|_v) < -\ln(|q|_v)$, alors on retrouve l'expression du théorème A.8). Les deux formules, d'une ressemblance troublante, disent plus ou moins la même chose : la hauteur locale d'un point P ne dépend que de son image dans $\bar{K}_v^*/q^{\mathbb{Z}}$, le cas de potentiellement bonne réduction étant mis de côté. Ou encore : on a vu que dans le cas de mauvaise réduction multiplicative, $\frac{\ln(|u|_v)}{\ln(|q|_v)}$ indique la composante irréductible où P se réduit modulo l'idéal associé à v. Ce rappel et la proximité entre les formules donnant la hauteur locale, aussi bien aux places finies et infinies, rejoignent la remarque 4.4, et nous font comprendre qu'en un sens, la hauteur locale archimédienne d'un point dépend uniquement de la composante irréductible où elle se réduit.

Ainsi la hauteur canonique admet, à l'instar de la hauteur naïve, une décomposition en termes locaux, qui ont l'avantage de toujours conserver l'interaction entre la géométrie de la courbe elliptique (à travers sa loi de groupe) et la complexité arithmétique (locale) des points de cette même courbe. Cette décomposition était déjà connue, bien entendu, on la retrouve par exemple dans [Sil94], chapitre VI, où leur existence est démontrée y compris dans le cas de mauvaise réduction additive,

ou dans [HS00], chapitre B.8, dans le cadre des variétés abéliennes. Mais l'approche arakelovienne a l'avantage de relier la hauteur d'un point *algébrique* à des termes locaux (les intersections) évalués en ce point algébrique, là où les hauteurs locales se restreignent aux points rationnels sur K (ou, du moins, sur K_v). J'espère donc que cette interprétation permettra de généraliser quelques résultats sur la hauteur de points rationnels qui utilisent les hauteurs locales (voir par exemple [HS88], [HS99], [Pet06]...) au cas des points algébriques, comme illustré au chapitre 6.

En reproduisant pas à pas les démonstrations du corollaire 5.30 et du théorème A.8, on obtient une expression plus générale de la hauteur dans le cas de courbes elliptiques semi-stables.

Corollaire A.12. *Soient E une courbe elliptique semi-stable définie sur un corps de nombres K et $\mathcal{E} \to B$ son modèle minimal régulier, de section neutre $\mathcal{O}$. Notons M_K les places de mauvaise réduction (multiplicative). Alors, pour tout point $Q \in E(\bar{K})$ d'adhérence $\mathcal{Q}$ dans $\mathcal{E}$, on a :*

$$\hat{h}(Q) = \frac{1}{[K(Q):\mathbb{Q}]}\left(\langle \mathcal{Q}, \mathcal{O}\rangle_K - \frac{1}{2}\sum_{\mathfrak{p}\in \mathrm{M}_K}[K_\mathfrak{p}:\mathbb{Q}_p]\sum_{\sigma: L\hookrightarrow\mathbb{C}} B_2\left(r_\mathfrak{p}(Q^\sigma)\right)\ln(|\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))|_\mathfrak{p})\right).$$

Démonstration. On se ramène encore une fois au cas d'une section à l'aide d'un changement de base $\mathrm{Spec}(\mathcal{O}_L) \to B$, où $L = K(Q)$. Pour alléger les notations, soient $\Delta = \Delta(E/L)$, $n_\mathfrak{P} = [L_\mathfrak{P} : \mathbb{Q}_p]$, et notons M_L l'ensemble des idéaux premiers de L de mauvaise réduction multiplicative ; d'après la proposition 5.9, ils divisent les idéaux premiers de M_K. Reprenant les raisonnements des démonstrations du corollaire 5.30 et du théorème A.8, on a :

$$[L:\mathbb{Q}]\hat{h}(Q) = \langle \mathcal{Q}, \mathcal{O}'\rangle_L - \frac{1}{2}\sum_{\mathfrak{P}\in \mathrm{M}_L} n_\mathfrak{P} B_2\left(r_\mathfrak{P}(Q)\right)\ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_\mathfrak{P})$$

puis :

$$\begin{aligned}
2[L:\mathbb{Q}]\hat{h}(Q) &= 2[K:\mathbb{Q}]\sum_{\sigma: L\hookrightarrow\mathbb{C}}\hat{h}(Q^\sigma)\\
&= \frac{2}{[L:K]}\sum_{\sigma: L\hookrightarrow\mathbb{C}}\left(\langle \mathcal{Q}^\sigma, \mathcal{O}'\rangle_L - \frac{1}{2}\sum_{\mathfrak{P}\in \mathrm{M}_L} n_\mathfrak{P} B_2\left(r_\mathfrak{P}(Q^\sigma)\right)\ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_\mathfrak{P})\right)\\
&= 2\langle \mathcal{Q}, \mathcal{O}\rangle_K - \frac{1}{[L:K]}\left(\sum_{\sigma: L\hookrightarrow\mathbb{C}}\sum_{\mathfrak{P}\in \mathrm{M}_L} n_\mathfrak{P} B_2\left(r_\mathfrak{P}(Q^\sigma)\right)\ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_\mathfrak{P})\right),
\end{aligned}$$

et il reste à calculer cette double somme. On remarque que si l'on note $j_\mathfrak{P}^\sigma$ l'indice de la composante où se réduit Q^σ modulo $\mathfrak{P}$, et si $\mathfrak{P}\cap\mathcal{O}_K = \mathfrak{p}$, alors notant u^σ l'image de $Q^\sigma \in E(\bar{L}_\mathfrak{P})$ dans $\bar{L}_\mathfrak{P}^*/q^\mathbb{Z}$ avec $|q|_\mathfrak{P} = |j_E|_\mathfrak{P}^{-1}$, on a :

$$r_\mathfrak{P}(Q^\sigma) = \frac{\ln(|u^\sigma|_\mathfrak{P})}{\ln(|q|_\mathfrak{P})} = \frac{\ln(|u^\sigma|_\mathfrak{p})}{\ln(|q|_\mathfrak{p})} = r_\mathfrak{p}(Q^\sigma),$$

d'après la démonstration du corollaire A.6 et la définition de $r_{\mathfrak{p}}$. Donc :

$$\sum_{\mathfrak{P}\in \mathrm{M}_L} n_{\mathfrak{P}} B_2\left(r_{\mathfrak{P}}(Q^\sigma)\right) \ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_{\mathfrak{P}}) = \sum_{\mathfrak{p}\in \mathrm{M}_K} B_2\left(r_{\mathfrak{p}}(Q^\sigma)\right) \sum_{\mathfrak{P}|\mathfrak{p}} n_{\mathfrak{P}} \ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|_{\mathfrak{P}}).$$

On conclut encore une fois grâce au corollaire A.6. □

Remarque A.13. N'ayant pas de prise sur l'évolution du discriminant minimal par extension de corps dans le cas général, je ne sais pas généraliser cette formule au cas où il existerait une place de réduction de type additif. Peut-être faudrait-il s'affranchir de faire une extension dans la démonstration du corollaire ci-dessus, afin de préserver le discriminant minimal, mais dans ce cas les fonctions de Green-Arakelov qui interviennent dans la formule d'adjonction, les calculs de $[\mathcal{P} - \mathcal{O}]$ et des auto-intersections (puis, dans une moindre mesure, le discriminant de $\mathcal{P}/L$) compliquent la tâche... D'autant plus qu'un point algébrique peut se réduire en un point singulier du modèle minimal régulier, et donc compliquer l'analyse qui précède la démonstration du théorème A.8.

Annexe B

Fonctions de Lambert

La fonction $\text{ʍ} : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & xe^x \end{cases}$ admet le tableau de variations suivant :

x	$-\infty$		-1		$+\infty$
$\text{ʍ}'(x)$		$-$	0	$+$	
$\text{ʍ}(x)$	0	↘	$-\frac{1}{e}$	↗	$+\infty$

Elle définit donc deux applications réciproques $\mathrm{w}_1 : \left]-\frac{1}{e}, +\infty\right[\to]-1, +\infty[$ et $\mathrm{w}_{-1} : \left]-\frac{1}{e}, 0\right[\to]-\infty, -1[$, la première étant strictement croissante et la seconde strictement décroissante. Leurs comportements asymptotiques sont connus.

Proposition B.1 ([CGH+96], (4.18))**.** *Les fonctions* w_1 *et* w_{-1} *vérifient les comportements asymptotiques suivants :*

$$\mathrm{w}_{-1}(x) = \ln(-x) - \ln(-\ln(-x)) + O\left(\frac{\ln(-\ln(-x))}{\ln(-x)}\right), \quad x \to 0, \text{ et}$$

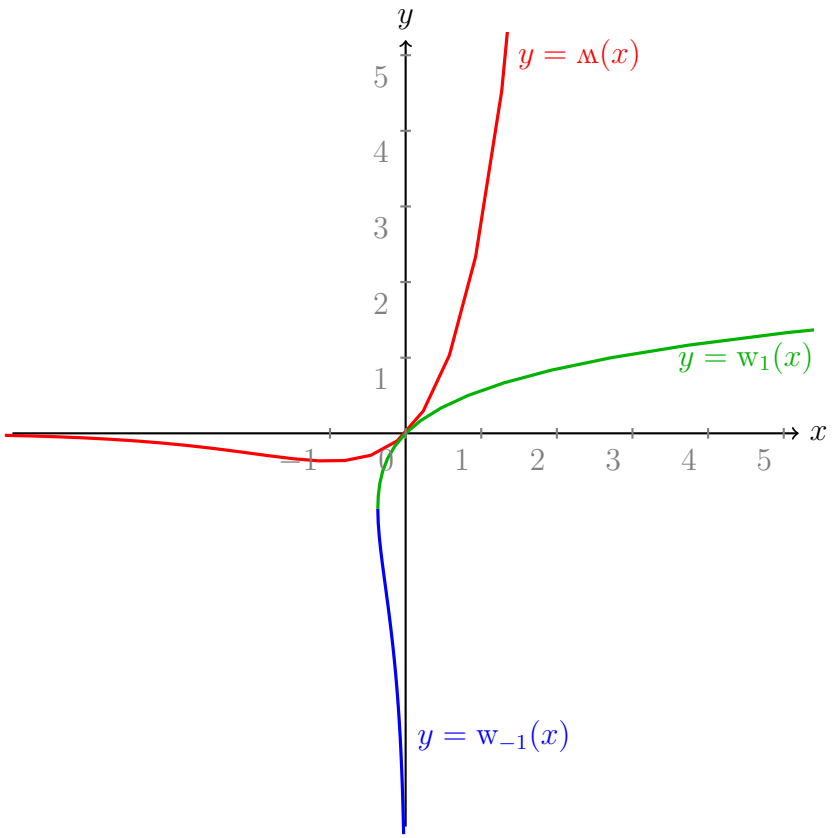
$$\mathrm{w}_1(x) = \ln(x) - \ln(\ln(x)) + O\left(\frac{\ln(\ln(x))}{\ln(x)}\right), \quad x \to \infty.$$

Corollaire B.2. *Les fonctions de Lambert vérifient les inégalités :*

$$\ln(-x) - \ln(-\ln(-x)) - \frac{1}{2} \leqslant \mathrm{w}_{-1}(x) \leqslant \ln(-x) - \ln(-\ln(-x)) \text{ pour } -\frac{1}{e} \leqslant x < 0,$$

$$\ln(x) - \ln(\ln(x)) \leqslant \mathrm{w}_1(x) \leqslant \ln(x) - \ln(\ln(x)) + \frac{1}{2} \text{ pour } x \geqslant e.$$

FIGURE B.1 – La fonction ʍ et ses réciproques.



Démonstration. le corollaire précédent démontre que l'application

$$f : \left\{ \begin{array}{rcl} \left]-\frac{1}{e},0\right[& \to & \mathbb{R} \\ x & \mapsto & \mathrm{w}_{-1}(x) - (\ln(-x) - \ln(-\ln(-x))) \end{array} \right.$$

tend vers 0 quand x tend vers 0, et elle s'annule aussi en $-\frac{1}{e}$. De plus, comme $f'(x) = \frac{1}{x}\left(\frac{1}{1+\frac{1}{\mathrm{w}_{-1}(x)}} - \frac{1}{\ln(-x)} + 1\right)$, une étude rapide montre que f_{-1} change de variation une seule fois (en le réel x tel que $\mathrm{w}_{-1}(x) = \ln(-x) - 1$), en commençant par décroître. Donc f_{-1} est toujours négative, de minimum $f_{-1}(x) > -\frac{1}{2}$ d'après toute méthode d'approximation des extremums, d'où le résultat pour w_{-1}. On procède exactement de la même manière pour démontrer le second encadrement. □

On en déduit le corollaire suivant, que nous utilisons à loisir dans le chapitre 6. Comme on peut s'en douter, en voyant les inégalités vérifiées par les fonctions de

Lambert et la démonstration du corollaire à suivre, les inégalités sont près d'être optimales.

Corollaire B.3. *Soient $\alpha > 0$, $b > 0$ et $s \geqslant 2$ trois réels.*

1. *si $s \geqslant e^{\frac{1}{2\alpha}} \left(\frac{\alpha b}{\ln(\alpha b)}\right)^{\frac{1}{\alpha}}$, alors $s^\alpha \ln(s) \geqslant b$;*
2. *si $s \geqslant e^{\frac{1}{2\alpha}} \left(\frac{b}{\alpha} \ln\left(\frac{b}{\alpha}\right)\right)^{\frac{1}{\alpha}}$, alors $\frac{s^\alpha}{\ln(s)} \geqslant b$.*

Démonstration. L'inégalité $s^\alpha \ln(s) \geqslant b$ peut se réécrire $\mathrm{ʍ}\left(\ln\left(s^\alpha\right)\right) \geqslant \alpha b$, qui est équivalente à $\ln\left(s^\alpha\right) \geqslant \mathrm{w}_1(\alpha b)$, d'où le premier résultat en invoquant le corollaire B.2. Le deuxième s'obtient semblablement. □

Index

Bibliographie

« Excusez-moi d'avoir lu des livres. »
Éric Zemmour

[Ara74] S. J. Arakelov – « An intersection theory for divisors on an arithmetic surface », *Izv. Akad. Nauk SSSR Ser. Mat.* **38** (1974), p. 1179–1192.

[AS64] M. Abramowitz & I. A. Stegun – *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards Applied Mathematics Series, vol. 55, For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964.

[AS92] — (éds.) – *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, Dover Publications, Inc., New York, 1992, Reprint of the 1972 edition.

[BG62] P. T. Bateman & E. Grosswald – « Imaginary quadratic fields with unique factorization », *Illinois J. Math.* **6** (1962), p. 187–192.

[BM12] V. Busch & J. S. Müller – « Local heights on elliptic curves and intersection multiplicities », *Int. J. Number Theory* **8** (2012), no. 6, p. 1477–1484.

[BP05] M. Baker & C. Petsche – « Global discrepancy and small points on elliptic curves », *Int. Math. Res. Not.* (2005), no. 61, p. 3791–3834.

[CGH+96] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey & D. E. Knuth – « On the Lambert W function », *Adv. Comput. Math.* **5** (1996), no. 4, p. 329–359.

[Col98] P. Colmez – « Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe », *Compositio Math.* **111** (1998), no. 3, p. 359–368.

[CS86] G. Cornell & J. H. Silverman – *Arithmetic geometry*, Springer-Verlag, New York, 1986.

[CS83] D. C. Cantor & E. G. Straus – « On a conjecture of D. H. Lehmer », *Acta Arith.* **42** (1982/83), no. 1, p. 97–100.

[Dav67] H. Davenport – *Multiplicative number theory*, Lectures given at the University of Michigan, Winter Term, vol. 1966, Markham Publishing Co., Chicago, Ill., 1967.

[Dav97] S. David – « Points de petite hauteur sur les courbes elliptiques », *J. Number Theory* **64** (1997), no. 1, p. 104–129.

[Del87] H. Delange – « Une remarque sur la dérivée logarithmique de la fonction zêta de Riemann », *Colloq. Math.* **53** (1987), no. 2, p. 333–335.

[Dob79] E. Dobrowolski – « On a question of Lehmer and the number of irreducible factors of a polynomial », *Acta Arith.* **34** (1979), no. 4, p. 391–401.

[Fal84] G. Faltings – « Calculus on arithmetic surfaces », *Ann. of Math. (2)* **119** (1984), no. 2, p. 387–424.

[GM15a] A. Galateau & V. Mahé – « Some consequences of Masser's counting theorem on elliptic curves », 2015.

[GM15b] L. Grenié & G. Molteni – « Explicit versions of the prime ideal theorem for Dedekind zeta functions under GRH », 2015.

[Hab10] P. Habegger – « Weakly bounded height on modular curves », *Acta Math. Vietnam.* **35** (2010), no. 1, p. 43–69.

[Hei67] H. Heilbronn – « Zeta-functions and L-functions », in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Thompson, Washington, D.C., 1967, p. 204–230.

[Hri85] P. Hriljac – « Heights and Arakelov's intersection theory », *Amer. J. Math.* **107** (1985), no. 1, p. 23–38.

[HS88] M. Hindry & J. H. Silverman – « The canonical height and integral points on elliptic curves », *Invent. Math.* **93** (1988), no. 2, p. 419–450.

[HS99] M. Hindry & J. Silverman – « Sur le nombre de points de torsion rationnels sur une courbe elliptique », *C. R. Acad. Sci. Paris Sér. I Math.* **329** (1999), no. 2, p. 97–100.

[HS00] M. Hindry & J. H. Silverman – *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

[Kad12] H. Kadiri – « Explicit zero-free regions for Dedekind zeta functions », *Int. J. Number Theory* **8** (2012), no. 1, p. 125–147.

[KN12] H. Kadiri & N. Ng – « Explicit zero density theorems for Dedekind zeta functions », *J. Number Theory* **132** (2012), no. 4, p. 748–775.

[Lan53] E. Landau – *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*, Chelsea Publishing Co., New York, 1953, 2d ed, With an appendix by Paul T. Bateman.

[Lan78] S. Lang – *Elliptic curves : Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin-New York, 1978.

[Lan88] — , *Introduction to Arakelov theory*, Springer-Verlag, New York, 1988.

[Lau83] M. Laurent – « Minoration de la hauteur de Néron-Tate », in *Seminar on number theory, Paris 1981–82 (Paris, 1981/1982)*, Progr. Math., vol. 38, Birkhäuser Boston, Boston, MA, 1983, p. 137–151.

[Liu02] Q. Liu – *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[LMO79] J. C. Lagarias, H. L. Montgomery & A. M. Odlyzko – « A bound for the least prime ideal in the Chebotarev density theorem », *Invent. Math.* **54** (1979), no. 3, p. 271–296.

[LO77] J. C. Lagarias & A. M. Odlyzko – « Effective versions of the Chebotarev density theorem », in *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press, London, 1977, p. 409–464.

[Mas81] D. Masser – « Small values of the quadratic part of the Néron-Tate height », *Progr. Math.* **12** (1981), p. 213–222.

[Mas89] D. W. Masser – « Counting points of small height on elliptic curves », *Bull. Soc. Math. France* **117** (1989), no. 2, p. 247–265.

[Neu99] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Odl77] A. M. Odlyzko – « On conductors and discriminants », in *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press, London, 1977, p. 377–407.

[Œst79] J. Œsterlé – « Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée », in *Astérisque*, vol. 61, 1979, p. 165–167.

[Pet06] C. Petsche – « Small rational points on elliptic curves over number fields », *New York J. Math.* **12** (2006), p. 257–268 (electronic).

[Ram07] O. Ramaré – « Eigenvalues in the large sieve inequality », *Funct. Approx. Comment. Math.* **37** (2007), no. part 2, p. 399–427.

[Rat04] N. Ratazzi – « Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe », *Int. Math. Res. Not.* (2004), no. 58, p. 3121–3152.

[RS62] J. B. Rosser & L. Schoenfeld – « Approximate formulas for some functions of prime numbers », *Illinois J. Math.* **6** (1962), p. 64–94.

[Sam67] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[Ser77] J.-P. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977, Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Ser81] — , « Quelques applications du théorème de densité de Chebotarev », *Inst. Hautes Études Sci. Publ. Math.* (1981), no. 54, p. 323–401.

[Sil94] J. H. Silverman – *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[Sil04] — , « A lower bound for the canonical height on elliptic curves over abelian extensions », *J. Number Theory* **104** (2004), no. 2, p. 353–372.

[Sil09] — , *The arithmetic of elliptic curves*, second éd., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Smy71] C. J. Smyth – « On the product of the conjugates outside the unit circle of an algebraic integer », *Bull. London Math. Soc.* **3** (1971), p. 169–175.

[ST61] G. Shimura & Y. Taniyama – *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[Sta74] H. M. Stark – « Some effective cases of the Brauer-Siegel theorem », *Invent. Math.* **23** (1974), p. 135–152.

[Szp90] L. Szpiro – « Sur les propriétés numériques du dualisant relatif d'une surface arithmétique », in *The Grothendieck Festschrift, Vol. III*, Progr. Math., vol. 88, Birkhäuser Boston, Boston, MA, 1990, p. 229–246.

[Tôy55] H. Tôyama – « A note on the different of the composed field », *Kōdai Math. Sem. Rep.* **7** (1955), p. 43–44.

[vdW40] B. L. van der Waerden – *Moderne Algebra*, J. Springer, Berlin, 1940.

[Vou96] P. Voutier – « An effective lower bound for the height of algebraic numbers », *Acta Arith.* **74** (1996), no. 1, p. 81–95.

Abstract

In this thesis we consider the problem of lower bounds for the canonical height on elliptic curves, aiming for the conjecture of Lehmer. Our main diophantine result is an explicit version of a theorem of Laurent (who proved this conjecture for elliptic curves with CM up to a ε exponent) using arithmetic intersection, enlightening the dependence with parameters linked to the elliptic curve ; such a result can be motivated by the conjecture of Lang, hoping for a lower bound proportional to, roughly, the Faltings height of the curve.
Nevertheless, our dissertation begins with a part dedicated to a completely explicit version of the density theorem of Chebotarev, along the lines of a previous work due to Lagarias and Odlyzko, which will be crucial to investigate the elliptic Lehmer problem. We also obtain upper bounds for Siegel zeros, and for the smallest prime ideal whose Frobenius is in a fixed conjugacy class.

Keywords Lehmer problem ; Néron-Tate, canonical height ; elliptic curves ; complex multiplication ; Arakelov geometry ; arithmetic intersection ; Chebotarev density theorem ; L-functions, zeta-functions.

Résumé

Cette thèse étudie le problème de minoration de la hauteur canonique sur les courbes elliptiques. Son résultat diophantien principal utilise des méthodes d'intersection arithmétique pour retrouver un résultat de Laurent, qui démontrait la conjecture de Lehmer pour les courbes elliptiques à multiplications complexes à un exposant ε près, tout en explicitant complètement sa dépendance en divers paramètres liés à la courbe elliptique ; une telle démarche peut être motivée par la conjecture de Lang, qui présage une minoration possible de la hauteur canonique proportionnelle, essentiellement, à la hauteur de Faltings de la courbe.
Notre dissertation commence toutefois par une partie dédiée à l'explicitation du théorème de densité de Chebotarev, qui reprend les grandes lignes d'un travail de Lagarias et Odlyzko, et s'avère être cruciale dans notre approche du problème de Lehmer elliptique. On obtient également des majorations des zéros de Siegel et de la norme du plus petit idéal premier entrant en jeu dans le théorème de Chebotarev.

Mots-clés problème de Lehmer ; hauteur canonique, de Néron-Tate ; courbes elliptiques ; multiplication complexe ; géométrie d'Arakelov ; intersection arithmétique ; théorème de densité de Chebotarev ; fonctions L, fonctions dzêta.