UNIVERSITÉ DE LA MEDITERRANEE
U.F.R. M.I.M.
ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE E.D. 184

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LA MÉDITERRANÉE

Spécialité : Mathématiques

par

Philippe LEBACQUE

sous la direction du Pr. Michael A. TSFASMAN

Titre :

SUR QUELQUES PROPRIETES ASYMPTOTIQUES DES CORPS GLOBAUX

soutenue publiquement le 16 mai 2007

Rapporteurs :

M. Joseph OESTERLÉ	Professeur, Université Pierre et Marie Curie
M. René SCHOOF	Professeur, Università di Roma Tor Vergata

JURY

M. Michel BALAZARD	Chargé de Recherches CNRS, I.M.B.	Examinateur
M. Marc HINDRY	Professeur, Université Paris Diderot	Examinateur
M. Gilles LACHAUD	Directeur de Recherches CNRS, I.M.L.	Examinateur
M. Joseph OESTERLÉ	Professeur, Université Pierre et Marie Curie	Rapporteur
M. Michael TSFASMAN	Directeur de Recherches CNRS, I.M.L.	Directeur
M. Serge VLĂDUŢ	Professeur, Université de la Méditerranée	Examinateur

Remerciements

Comment ne pas débuter les traditionnels remerciements par le témoignage de mon infinie gratitude envers celui qui a dirigé mes recherches, Michael A. Tsfasman, dont la gentillesse, la patience, la sollicitude et les connaissances ont été pour moi une aide des plus précieuses, à celui qui m'a fait découvrir les corps globaux infinis et qui m'a offert la possibilité de visiter le laboratoire Poncelet de Moscou pour mon plus grand plaisir intellectuel et culturel, et ainsi de réaliser un de mes rêves d'enfant ?

Comment ne pas remercier Joseph Oesterlé et René Schoof pour avoir accepté la pénible tâche de rapporteur, ni Michel Balazard, Marc Hindry, Gilles Lachaud et Serge Vlăduţ qui siégeront dans le jury, sans qui ce travail n'aurait que peu de valeur ?

Il me serait également impossible d'omettre le personnel scientifique et administratif de l'institut de mathématiques de Luminy, en particulier Gilles Lachaud pour sa disponibilité et l'aide qu'il m'a apportée. Je ne pourrais pas non plus oublier de remercier l'équipe scientifique du laboratoire Poncelet, en particulier Michel Balazard, pour avoir pris le temps de m'apporter remarques et corrections. Il serait enfin injuste de ne pas penser à Christian Maire qui m'a fait parvenir un exemplaire de sa thèse et répondu à mes questions aussi naïves soient-elles.

Je serais ingrat de ne pas me souvenir de ceux qui m'ont transmis leur passion des mathématiques. En premier lieu je n'oublierai pas que c'est d'abord mon père qui m'encouragea dans cette voie dès mon plus jeune âge ; j'aurai aussi une pensée pour Thomas Lafforgue qui sut éveiller une passion ensommeillée, pour Yves Meyer qui m'impressionna tant socialement que scientifiquement, pour Guy Henniart et Jean-Marc Fontaine pour leurs fabuleux cours de théorie des nombres et les difficultés qu'ils me posèrent, enfin pour Jean-François Mestre qui m'a donné goût à la recherche, et qui m'orienta vers Marseille et Michael A. Tsfasman.

Il serait mesquin d'ignorer mes amis mathématiciens, issus de l'ENS Cachan pour la plupart, qui ont également contribué, d'une manière ou d'une autre, à ce que je suis. Ainsi, je tiens à remercier Chab pour nos discussions en tout genre au fil des années, Lapinot qui montra l'exemple à ne pas suivre en toute circonstance, Tontysh pour avoir toujours été en retard et partagé cette passion pour la théorie des nombres, dépassant nos différents footballistiques, Neuneu et Davidor, experts en optimisation de carrière ainsi que Pfff pour nous avoir rappelé que tous les chemins mènent à la finance. Je remercie également Alain, Alexei, Christophe, Frédéric, Nicolas^2 et Yves pour nos discussions, mathématiques ou non, qui ont rendu plus agréables les années de ma thèse.

Je ne peux pas imaginer non plus de passer sous silence mes autres amis dont le soutien constant m'a permis de mener à terme cette longue course de fond qu'est le doctorat. Merci à l'ensemble du Martini Club, à mes amis Guillaume, Jean Noël, Anh, Cécile, Cyrielle et Maëlys ; merci pour tout.

Comment ne pas terminer par remercier du fond du coeur toute ma famille ainsi que Boubi qui partage ma vie depuis déjà presque quatre années, qui a su créer autour de moi une atmosphère de joie et d'amour sans laquelle je n'aurais pas pu trouver la volonté nécessaire pour mener à bien cette aventure ?

« Point n'est besoin d'espérer pour entreprendre, ni de réussir pour persévérer »
Guillaume d'Orange

Table des matières

Introduction

De la Théorie de l'information aux corps globaux infinis

Un des plus fameux débouché moderne de la recherche mathématique réside dans les technologies de l'information. Pour ne citer que quelques exemples, le codage de données en vue de leur transmission, ou encore la cryptographie impliquent des objets mathématiques de plus en plus sophistiqués, et au coeur de ceux-ci se trouvent les courbes et plus généralement les variétés algébriques. Leur utilisation nécessite qu'elles contiennent un grand nombre de points, sans pour autant être monstrueuses ; ainsi, l'un des problèmes principaux rencontrés est la construction de courbes possédant beaucoup de points rationnels, mais dont le genre n'est pas trop gros.

Le nombre de points rationnels d'une courbe définie sur $\mathbb{F}_q$ est lié à son genre par la borne de Hasse-Weil. En effet, pour une courbe C de genre g, il doit vérifier : $N_q(C)-q-1 \leq 2g\sqrt{q}$. Cette borne n'est pas toujours optimale, comme l'a remarqué Serre, qui l'a raffinée légèrement, et il s'agit d'un problème difficile que de déterminer des courbes maximales. Faute de pouvoir connaître le nombre maximum de points que peut avoir une courbe de genre donné, on peut s'interroger sur son comportement dans une famille de courbes lorsque le genre augmente. Drinfeld et Vlăduţ ont alors découvert que la limite du quotient de ces deux quantités est toujours inférieur à $\sqrt{q}-1$. La recherche de familles de courbes atteignant la borne de Drinfeld-Vlăduţ a donné lieu à des exemples divers de constructions, qu'elles soient modulaires, explicites, ou encore utilisant la théorie du corps de classes. Cette étude a également conduit à une généralisation par Tsfasman et Vlăduţ de cette inégalité asymptotique au moyen des formules explicites, dans le cas des corps de nombres et des corps de fonctions, où cette fois toutes les places, pas seulement celles de degré 1, entrent en compte ; de ce fait, ils généralisèrent notamment les résultats d'Ihara sur les tours non ramifiées de corps de nombres, ce dernier ayant utilisé le degré comme référence, au lieu du genre chez Tsfasman et Vlăduţ. Dans leur article qui propose d'essayer de construire une théorie des corps globaux infinis, ils nous donnent quelques indications montrant qu'une telle théorie doit exister, et qu'elle n'est pas seulement le passage à la limite des propriétés des corps globaux. Ainsi, ils ont défini, entre autres, une famille d'invariants relatifs aux corps globaux infinis, établi l'existence d'une fonction zêta limite, d'une densité asymptotique des zéros de la fonctions zêta, et fait le lien entre elles et l'inégalité généralisant la borne de Drinfeld-Vlăduţ.

D'autre part, ils ont généralisé le théorème de Brauer-Siegel (qui prédit le comportement du résidu de la fonction zêta en $s = 1$ dans la tour) dans le cas où le corps global infini ne vérifie pas l'hypothèse n/g tendant vers 0, c'est à dire aux corps de nombres infinis asymptotiquement bons, et ont également affaibli l'hypothèse technique "galoisienne" dans ce cas, résultat qui fut plus tard complété par Zykin dans le cas où la tour est asymptotiquement mauvaise.

Organisation de notre étude et résultats principaux

Ainsi, notre étude des corps globaux infinis tourne autour des résultats de Tsfasman-Vlăduţ. Son fil conducteur est la volonté de décrire précisément l'ensemble des invariants admissibles pour un corps global infini. Malheureusement, cet objectif initial s'est avéré hors d'atteinte pour l'instant, mais nous donnerons des éléments de réponse, ainsi que des pistes qui permettent de comprendre où résident les difficultés.

Dans le premier chapitre, nous rappelons d'abord la définition des invariants des corps globaux infinis, d'après [TV02]. Nous étendons quelque peu cette notion pour des vues pratiques. Dans le cas des corps de nombres, et d'une extension définie sur $\mathbb{Q}$, l'invariant ϕ_p décrira la participation des places de norme p dans la fonction zêta de la tour, et sa contribution sera non nulle si le nombre de places de norme p se comporte comme le genre. Toutefois, il peut s'avérer techniquement utile de considérer, plutôt que ϕ_p, le taux de décomposition d'une place $\mathfrak{p}$. $\phi_{\mathfrak{p},\cdot}$ jouira des mêmes propriétés que ϕ_p (proposition 1.9). Cette généralisation trouve son intérêt dans le fait que les définitions classiques dans le cas des corps de nombres et celui des corps de fonctions sont différentes, dans la mesure où des places finies peuvent avoir même norme dans ces derniers sans être au-dessus de la même place ; utiliser cette définition permet alors d'unifier des résultats. Elle aura également l'intérêt de rendre plus claires les démonstrations de résultats intuitifs, tels la proposition 1.12. Nous définissons également d'autres invariants de corps globaux infinis, dans la proposition 1.10, qui ont pour objet de compter la contribution totale de la place $\mathfrak{p}$, et en donnons quelques propriétés rappelant celles des valeurs absolues ultramétriques.

Après avoir défini la notion de tour asymptotiquement bonne, et défini le défaut des corps globaux infinis d'après [TV02], nous nous attardons d'abord sur des conditions élémentaires qu'ils ont à remplir afin d'être asymptotiquement bons. Utilisant le théorème de Riemann-Hurwitz et nous inspirant de résultats de Garcia et Stichtenoth dans le cas des corps de fonctions, nous donnons des conditions valables pour des cas plus généraux de tours de corps globaux : les tours presque-galoisiennes (proposition 1.22). Les candidats raisonnables pour construire des corps globaux infinis sont alors les extensions modérément ramifiées, non ramifiées hors d'un ensemble fini de places. A la fin du quatrième paragraphe, nous nous attachons à la description des invariants de corps galoisiens, ainsi que leur rapport à la décomposition des places. Enfin, dans le dernier paragraphe, nous réfléchissons au moyen de construire des corps globaux infinis asymptotiquement bons par compositum. Nous rappelons des résultats généraux sur les composita tirés de [Lan02] et [Lan94], pour en déduire quelques résultats importants sur le compositum de corps globaux (corollaire 1.28), ainsi que quelques calculs élémentaires d'invariants (propositions 1.31, 1.33 et corollaire 1.32).

Le second chapitre est consacré à la construction de corps globaux infinis ayant des propriétés voulues. Nous rappelons alors les résultats de la théorie du corps de classes (§2.1), qui, grâce au critère de Golod-Schafarevitch (§2.2) nous permet de construire des tours asymptotiquement bonnes (§2.3), ainsi que le théorème de Grunwald-Wang (§2.4), dont nous proposons une version quelque peu améliorée (corollaire 2.17) à partir des résultats présents dans [NSW00]. Nous donnons alors quelques informations au sujet de l'ensemble des invariants (§3, théorème 2.19), c'est à dire qu'on peut choisir un nombre fini quelconque d'invariants qui seront non nuls, sans pour autant pouvoir s'assurer que les autres seront nuls. Ensuite, dans la quatrième partie, nous raffinerons un peu les résultats de tours de corps de classes, en estimant le défaut de ces tours lorsque le nombre de places dont on contrôle la décomposition augmente (corollaire 2.28). On comprend alors que le nombre de places qui se décomposent totalement ne peut être trop gros, et c'est ce que nous allons étudier dans la cinquième partie, rappelant le théorème de densité de Cebotarev, dont un corollaire (2.30) nous dit que la densité des places qui se décomposent totalement dans une extension infinie est nulle. Nous verrons que dans le cas asymptotiquement bon, la somme des inverses des normes des places finies totalement décomposées est finie (proposition 2.35), et nous donnerons alors des exemples de tours telles que cette somme est infinie et telle que la densité de son lieu de ramification est nulle (théorème 2.36) ; nous démontrerons au passage (proposition 2.39 et corollaire 2.40) qu'une conjecture privée de Michel Balazard est fausse (conjecture 2.38). Dans la partie suivante, nous essaierons de comprendre pourquoi il est très difficile de contrôler l'inertie dans une tour, bien que l'intuition nous laisse penser qu'on devrait pouvoir y parvenir comme pour la décomposition (corollaire 2.42). En effet, dans le cas quadratique, c'est simplement imposer la valeur -1 au caractère en p plutôt que la valeur 1. Nous lierons alors le groupe de décomposition d'une place au-dessus de p aux invariants relatifs à la place p (proposition 2.44), et nous utiliserons des résultats récents de Labute [Lab06] et Schmidt [Sch06] pour construire un corps de nombres infini asymptotiquement bon possédant un nombre prescrit d'invariants nuls (théorème 2.45). Dans la septième partie, nous étudions le défaut des corps globaux infinis plus en détail, montrant sa croissance pour l'inclusion (théorème 2.50). Nous en déduirons alors plusieurs résultats concernant l'optimalité (propositions 2.53 et 2.54), et la non-optimalité (théorème 2.55) des corps globaux infinis qu'on construit à l'aide du critère de Golod-Schafarevitch. Nous montrerons enfin que des corps globaux infinis peuvent avoir un défaut arbitrairement proche de 1 (proposition 2.57).

Enfin le dernier chapitre est un article consacré au théorème de Brauer-Siegel et son lien avec le théorème de Mertens (théorème 3.5). En effet, celui-là décrit le comportement limite du résidu de la fonction zêta en $s = 1$ dans la tour par rapport au genre, tandis que le théorème de Mertens explicite (théorèmes 3.6 et 3.9) que nous démontrons décrit ce qui se passe aux étages finis de la tour. Après avoir énoncé et démontré une généralisation explicite du théorème de Mertens, dans le cas des corps de nombres et celui des variétés algébriques projectives lisses définies sur un corps fini, nous passerons à la limite pour obtenir une version explicite du théorème de Brauer-Siegel sous GRH (corollaire 3.10), et nous retrouverons les résultats de Tsfasman-Vlăduţ-Zykin (corollaire 3.7), ainsi que quelques petits résultats (proposition 3.8) qui décrivent un peu ce qu'il advient dans les mauvais cas. Il est à noter que la généralisation sous une forme non-explicite du théorème de Mertens est due à Rosen [Ros99], mais malheureusement je n'ai eu connaissance de ses travaux qu'après avoir achevé les miens.

Chapitre 1

Invariants des corps globaux infinis

Sommaire

Ce chapitre est consacré aux définitions et aux résultats élémentaires qui permettent de comprendre la problématique et l'intérêt de ce qui va suivre. Après avoir défini le concept de corps global infini, nous en donnerons des propriétés élémentaires.

Définition 1.1 *On appelle un* ***corps global infini*** *une extension algébrique séparable $\mathcal{K}$ de degré infini de $\mathbb{Q}$ (NF) ou de $\mathbb{F}_r(t)$ telle que $\bar{\mathbb{F}}_r \cap \mathcal{K} = \mathbb{F}_r$ (FF).*

Dans toute la suite, les corps de fonctions que nous considérerons seront tous supposés avoir le même corps de constantes, et nous conserverons les notations r pour le cardinal du corps de base, $r = p^d$ où p est un nombre premier. Sauf mention du contraire, **les extensions de corps de fonctions seront toujours supposées sans extension du corps des constantes et séparables**. Nous utiliserons les notations (NF) et (FF) pour signifier qu'une assertion est valable dans le cas d'un corps de nombres ou d'un corps de fonctions respectivement.

Pour comprendre un tel objet, il convient d'en étudier des sous-corps de degré fini, et d'observer leur comportement lorsqu'on fait grossir ces corps jusqu'à notre corps global infini. Pour procéder ainsi, nous avons besoin du lemme suivant :

Lemme 1.2 *Soit $\mathcal{K}$ un corps global infini. Alors il existe une tour (c'est à dire une suite croissante pour l'inclusion) de corps globaux $(K_i)_{i\in\mathbb{N}}$ telle que $\mathcal{K} = \bigcup_{i\in\mathbb{N}} K_i$.*

Preuve du lemme: Comme $\mathcal{K}$ est algébrique, $\mathcal{K}$ est dénombrable, et le résultat s'ensuit. ■

> **Remarque:** Une telle suite n'est pas unique. Afin de se servir de cette expression du corps $\mathcal{K}$, il faudra toujours vérifier que les résultats obtenus ainsi sont indépendants de la représentation ainsi choisie.

Définition 1.3 *On dira que l'extension (éventuellement infinie) $\mathcal{K}/K_0$ est* ***galoisienne*** *(resp.* ***presque-galoisienne****) s'il existe une tour de corps globaux $\bigcup_{i\in\mathbb{N}} K_i = \mathcal{K}$ telle que pour tout i, K_i/K_0 est galoisienne (resp. K_{i+1}/K_i). $\mathcal{K}$ sera dit galoisien (resp. presque-galoisien) si $\mathcal{K}/\mathbb{Q}$ ou $\mathbb{F}_r(t)$ l'est.*

> **Remarque:** Les définitions de presque-galoisien dans le cas d'extensions finies et infinies sont compatibles. En effet, un corps global infini est presque-galoisien si et seulement s'il est réunion croissante de corps globaux presque-galoisiens. Ainsi, pour montrer la réciproque (non triviale a priori), on considère $\mathcal{K} = \cup K_i$, et $K_i = \cup_{j\leq n_i} L_j^i$ avec L_{j+1}^i/L_j^i galoisienne. Alors $\mathcal{K}$ est représenté par
>
> $$\cdots \subset K_{i-1}.L_1^i \subset K_{i-1}.L_2^i \subset \cdots \subset K_{i-1}.L_{n_i}^i = K_i L_1^{i+1} \subset \ldots,$$
>
> où $K_{-1} = \mathbb{Q}$. Chacune de ces extensions est galoisienne sur la précédente, et $\mathcal{K}$ est donc presque-galoisien.

Etant donné un corps global K, on notera son **degré** n_K (ou plus simplement n s'il n'y a pas d'ambiguïté), c'est à dire le degré de K sur $\mathbb{Q}$ ou sur $\mathbb{F}_r(t)$ suivant le cas ; pour une suite de corps globaux $(K_i)_{i\in\mathbb{N}}$, on notera n_i le degré du corps K_i. Dans le cas d'un corps de fonctions K, g_K désignera son **genre** tandis que dans le cas des corps de nombres on posera $g_K = \log\sqrt{D_K}$, où D_K est son discriminant absolu (que l'on nommera également genre). On adoptera également la notation $g_i = g_{K_i}$ lorsque nous aurons affaire à des suites de corps globaux. On pourrait proposer d'autres définitions du genre, afin d'obtenir des formules semblables dans le cas des corps de nombres et des corps de fonctions, en particulier concernant le théorème de Riemann-Hurwitz (voir [Neu99]).

On notera $P(K)$ l'ensemble des places de K, $P_f(K)$ celui des places non archimédiennes, $P_q(K)$ celui des places de norme q (son cardinal sera désigné par $\Phi_q(K)$) pour q une puissance d'un nombre premier, et, dans le cas des corps de nombres, $P_\mathbb{R}(K)$ l'ensemble des places réelles (dont on notera $\Phi_\mathbb{R}(K)$ ou plus simplement r_1 le cardinal), et $P_\mathbb{C}(K)$ celui des places complexes dont le cardinal sera appelé $\Phi_\mathbb{C}(K)$ ou plus simplement r_2. On notera $\mathcal{O}_K$ son anneau des entiers, et on identifiera bien souvent, dans le cas des corps de nombres, les places finies de K et les idéaux maximaux de $\mathcal{O}_K$.

Dans toute notre étude, on ne considérera qu'un type particulier de suites de corps globaux dont le genre tend vers l'infini :

Définition 1.4 *Une* ***famille*** *$(K_i)_{i\in\mathbb{N}}$ de corps globaux est une suite $(K_i)_{i\in\mathbb{N}}$ de corps globaux, extensions finies du même corps de base ($\mathbb{Q}$ ou $\mathbb{F}_r(t)$), telle que K_i n'est pas isomorphe à K_j si $i \neq j$, et telle que, dans le cas des corps de fonctions, le corps des constantes de chaque K_i est le même corps fini $\mathbb{F}_r$ pour tout i.*

Proposition 1.5 *Soit $(K_i)_{i\in\mathbb{N}}$ une famille de corps globaux. Alors la suite des genres $(g_{K_i})_{i\in\mathbb{N}}$ tend vers l'infini.*

Preuve : On se reportera à [TV02]§2. □

Ainsi, pour une tour infinie de corps globaux $(K_i)_{i\in\mathbb{N}}$, avec $K_i \subsetneq K_{i+1}$ pour tout i (et sans extension du corps des constantes dans le cas des corps de fonctions), on a bien $g_{K_i} \to \infty$.

1.1 Définitions et premières propriétés

Lorsqu'on étudie le comportement asymptotique des corps globaux, il faut commencer par se donner une valeur de référence de la tour de corps. Ihara avait proposé dans son article [Iha83] de considérer le degré des corps dans la tour, et a pu ainsi obtenir de bons résultats dans le cas des extensions non ramifiées (où le genre est un multiple du degré). Dans [TV02] Michael Tsfasman et Serge Vlăduţ ont jugé plus judicieux par analogie avec les corps de fonctions de considérer le genre à la place du degré, et ont ainsi obtenu une fonction zêta limite et des résultats très convainquant, comme une généralisation du théorème de Brauer-Siegel, ou bien l'existence d'une densité correspondant à la distribution limite des zéros de la fonction zêta. Nous suiverons donc leur approche pour définir les invariants de corps globaux relatifs aux places finies et archimédiennes de nos corps globaux infinis. Dans un premier temps nous allons rappeler les définitions de base, puis dans un second temps développer quelque peu ces définitions en fonction du corps de base.

1.1.1 Invariants absolus

Nous allons définir dans ce paragraphe les invariants des corps globaux infinis qui nous intéressent, et ensuite donner quelques propriétés élémentaires.

L'Ensemble Φ :

Considérons l'ensemble

$$A = \begin{cases} \left\{\mathbb{R}, \mathbb{C}, p^k, p \text{ premier}, \ k \in \mathbb{N}^*\right\} & (NF) \\ \left\{r^k, k \in \mathbb{N}^*\right\} & (FF). \end{cases}$$

A_f désignera $A - \{\mathbb{R}, \mathbb{C}\}$ dans le cas des corps de nombres, et A dans celui des corps de fonctions.

Définition 1.6 *Soit $\mathcal{K} = (K_i)_{i \in \mathbb{N}}$ une famille de corps globaux.*

*i. On dira que $\mathcal{K}$ est **asymptotiquement exacte** si, pour tout $q \in A$, la suite $\Phi_q(K_i)/g_i$ admet une limite, que l'on notera alors $\phi_q(\mathcal{K})$. Dans ce cas, on considérera $\Phi_{\mathcal{K}} = \{\phi_q, q \in A\}$.*

*ii. On dira que la famille $\mathcal{K}$ est **asymptotiquement bonne** si elle est asymptotiquement exacte et qu'au moins l'un des ϕ_q, $q \in A$, est non nul. Dans le cas contraire on la dira asymptotiquement mauvaise.*

iii. Dans le cas des corps de fonctions, on notera $\lambda(\mathcal{K})$ la limite, si elle existe, du ratio n_i/g_i. Dans celui des corps de nombres, cette limite sera notée $\phi_\infty(\mathcal{K})$.

Par soucis de la forme, on étendra également ces définitions pour un corps global K en considérant la suite constante (K) même si son genre reste constant, mais nous n'abuserons que peu de ces notations afin de ne pas faire disparaître les quantités qui nous intéressent derrière elles.

Remarque: :

i. En utilisant l'extraction diagonale, il est aisé de montrer que toute famille de corps globaux admet une sous-famille asymptotiquement exacte.

ii. Chaque limite, si elle existe, est finie. On donnera par la suite des majorations des ϕ_q.

iii. Il y a ici une différence importante entre la définition dans le cas des corps de nombres et celui des corps de fonctions. Dans celui des corps de nombres, les ϕ_{p^n}, $n > 0$, sont directement liés à la décomposition de la place p dans le corps global infini, tandis que dans celui des corps de fonctions, c'est le comportement des places dans leur ensemble qui est reflété par les invariants ϕ_{r^n}. Cela justifie en partie les définitions qui suivront.

Dans le cas qui nous intéresse, la famille est toujours asymptotiquement exacte, comme l'indique une conséquence de la proposition suivante.

Proposition 1.7 *Soient $K \subset L$ deux corps de nombres (resp. corps de fonctions) tels que $g(K) \geq 1$ (resp. $g(K) \geq 2$). Alors, on a, dans le cas des corps de nombres*

$$\frac{n_L}{g_L} \leq \frac{n_K}{g_K} \qquad (NF),$$

et pour tout nombre premier p et tout $n \geq 1$:

$$\sum_{m=1}^{n} \frac{m\Phi_{p^m}(L)}{g_L} \leq \sum_{m=1}^{n} \frac{m\Phi_{p^m}(K)}{g_K} \qquad (NF).$$

Dans le cas des corps de fonctions, on a, de même :

$$\frac{n_L}{g_L - 1} \leq \frac{n_K}{g_K - 1} \qquad (FF),$$

et pour tout $n \geq 1$:

$$\sum_{m=1}^{n} \frac{m\Phi_{r^m}(L)}{g_L - 1} \leq \sum_{m=1}^{n} \frac{m\Phi_{r^m}(K)}{g_K - 1} \qquad (FF).$$

Preuve : C'est une conséquence de la formule de Riemann-Hurwitz et de la loi de décomposition des places dans les extensions séparables — voir [TV02](lemma 2.3). □

Corollaire 1.8 *Soit $\mathcal{K}$ un corps global infini. Alors $\mathcal{K}$ est asymptotiquement exact et les ϕ_q sont indépendants de la tour considérée.*

Preuve : D'après la proposition précédente, le quotient n/g est décroissant dans une tour pour $g \geq 1$, il admet donc une limite. Les autres inégalités donnent l'existence de ϕ_p, puis ϕ_{p^2} etc. Pour l'indépendance, c'est simplement un argument de pincement ([TV02] Lemma 2.4). □

On considérera alors l'ensemble $\Phi = \{\Phi_{\mathcal{K}}, \mathcal{K} \text{ est un corps global infini}\}$. Plusieurs problèmes s'imposent alors d'eux-mêmes :

Problème:

i. Le support de $\Phi_{\mathcal{K}}$ peut-il être non vide, infini ? Φ est-il contenu dans l'ensemble des suites nulles à l'infini ?

ii. Φ a-t-il des propriétés topologiques remarquables pour une distance classique de $\mathbb{R}^{\mathbb{N}}$?

1.1.2 Invariants relatifs à la place $\mathfrak{p}$

Pour K un corps global, L/K une extension finie, et $\mathfrak{p} \in P_f(K)$, considérons $\Phi_{\mathfrak{p},q}(L)$ le nombre de places de L de norme q au-dessus de $\mathfrak{p}$. De même, si $\mathfrak{p}$ est une place archimédienne, on notera $\Phi_{\mathfrak{p},\mathbb{R}}(L)$ le nombre de places au-dessus de $\mathfrak{p}$ qui sont réelles, $\Phi_{\mathfrak{p},\mathbb{C}}(L)$ celui des places qui sont complexes. On a alors simplement, pour $q \in A$,

$$\Phi_q(L) = \sum_{\mathfrak{p}\in P(K)} \Phi_{\mathfrak{p},q}(L).$$

Considérons la tour (K_i) de corps globaux. On définira alors, lorsqu'elle existe, la limite

$$\phi_{\mathfrak{p},q} = \lim_{i\to\infty} \frac{\Phi_{\mathfrak{p},q}(K_i)}{g_i}.$$

Bien entendu, si pour tout $\mathfrak{p}$ ces limites existent, la tour est asymptotiquement exacte au sens précédent. Dans une famille quelconque de corps contenant K, la réciproque pourrait s'avérer fausse. Toutefois, pour une tour, elle est vraie. En effet la proposition 1.7 reste valable :

Proposition 1.9 *Soit K_0 un corps global. Soient $K \subset L$ deux corps de nombres (resp. corps de fonctions) contenant K_0 tels que $g(K) \geq 1$ (resp. $g(K) \geq 2$). Alors, on a, dans le cas des corps de nombres, pour toute place archimédienne $\mathfrak{p}$,*

$$\frac{\Phi_{\mathfrak{p},\mathbb{R}}(L)}{g_L} + 2\frac{\Phi_{\mathfrak{p},\mathbb{C}}(L)}{g_L} \leq \frac{\Phi_{\mathfrak{p},\mathbb{R}}(K)}{g_K} + 2\frac{\Phi_{\mathfrak{p},\mathbb{C}}(K)}{g_K} \qquad (NF),$$

et pour toute place finie $\mathfrak{p}$ de K_0 et tout $n \geq 1$:

$$\sum_{q\leq \mathrm{N}\mathfrak{p}^n} \frac{\log q\Phi_{\mathfrak{p},q}(L)}{g_L} \leq \sum_{q\leq \mathrm{N}\mathfrak{p}^n} \frac{\log q\Phi_{\mathfrak{p},q}(K)}{g_K} \qquad (NF).$$

Dans le cas des corps de fonctions, on a, de même, pour toute place $\mathfrak{p}$ et tout $n \geq 1$:

$$\sum_{q\leq \mathrm{N}\mathfrak{p}^n} \frac{\log_r(q)\Phi_{\mathfrak{p},q}(L)}{g_L - 1} \leq \sum_{q\leq \mathrm{N}\mathfrak{p}^n} \frac{\log_r(q)\Phi_{\mathfrak{p},q}(K)}{g_K - 1} \qquad (FF).$$

Preuve : Nous adaptons ici la preuve du lemme 2.3 de [TV02]. Dans le cas des corps de nombres, on a

$$g(L) \geq [L:K]g(K),$$

tandis que dans celui des corps de fonctions

$$g(L) - 1 \geq [L:K](g(K) - 1).$$

Soit $\mathfrak{p}$ une place archimédienne du corps de nombres K_0. Au-dessus de $\mathfrak{p}$, il y a dans K $\Phi_{\mathfrak{p},\mathbb{R}}(K)$ places réelles, $\Phi_{\mathfrak{p},\mathbb{C}}(K)$ places complexes de sorte que

$$\Phi_{\mathfrak{p},\mathbb{R}}(K) + 2\Phi_{\mathfrak{p},\mathbb{C}}(K) = [K : K_0],$$

et de même dans L :

$$\Phi_{\mathfrak{p},\mathbb{R}}(L) + 2\Phi_{\mathfrak{p},\mathbb{C}}(L) = [L : K_0] = [L : K][K : K_0],$$

on en déduit alors que

$$\Phi_{\mathfrak{p},\mathbb{R}}(L) + 2\Phi_{\mathfrak{p},\mathbb{C}}(L) = [L : K]\big(\Phi_{\mathfrak{p},\mathbb{R}}(K) + 2\Phi_{\mathfrak{p},\mathbb{C}}(K)\big),$$

et en divisant par $g(L)$, on obtient le résultat souhaité.

En ce qui concerne les places finies, considérons les places au-dessus de $\mathfrak{p}$. Une place finie $\mathfrak{q}|\mathfrak{p}$ de K se décompose dans L en un produit de places $\mathfrak{q}_i$ de L au-dessus de $\mathfrak{p}$, de sorte que

$$\prod \mathrm{N}\mathfrak{q}_i \leq \mathrm{N}\mathfrak{q}^{[L:K]}.$$

En prenant le logarithme, on obtient :

$$\sum_q \log q \Phi_{\mathfrak{q},q}(L) \leq [L : K] \log \mathrm{N}\mathfrak{q}.$$

On a donc

$$\begin{aligned}\sum_{q \leq \mathrm{N}\mathfrak{p}^n} \frac{\log q \Phi_{\mathfrak{p},q}(L)}{g_L} &= \sum_{q \leq \mathrm{N}\mathfrak{p}^n} \sum_{\mathfrak{q} \in P(K),\ \mathfrak{q}|\mathfrak{p}} \frac{\log q \Phi_{\mathfrak{q},q}(L)}{g_L} \\ &\leq \sum_{\mathfrak{q} \in P(K),\ \mathfrak{q}|\mathfrak{p},\ \mathrm{N}\mathfrak{q} \leq \mathrm{N}\mathfrak{p}^n} \frac{\log \mathrm{N}\mathfrak{q}}{g_K},\end{aligned}$$

ce qui termine la preuve pour les corps de nombres, le cas des corps de fonctions se traitant de même en remplaçant g par $g - 1$. □

1.1.3 Propriétés élémentaires

Nous recherchons des corps globaux ayant de bonnes propriétés asymptotiques. Nous allons constater que, partant d'un corps global infini asymptotiquement bon, on ne peut produire que des exemples plus mauvais en lui adjoignant d'autres éléments. En effet, si un corps est inclus dans un autre, alors ce dernier est plus mauvais au sens suivant.

Proposition 1.10 *Soient $\mathcal{K} \subset \mathcal{L}$ deux corps de nombres infinis. Alors*

$$(NF) \quad |\mathcal{K}|_\infty := \phi_\mathbb{R}(\mathcal{K}) + 2\,\phi_\mathbb{C}(\mathcal{K}) \geq \phi_\mathbb{R}(\mathcal{L}) + 2\,\phi_\mathbb{C}(\mathcal{L}).$$

Pour tout nombre premier p et tout entier n, on a également :

$$(NF) \quad \sum_{m=1}^{n} m\phi_{p^m}(\mathcal{K}) \geq \sum_{m=1}^{n} m\phi_{p^m}(\mathcal{L}),$$

en particulier

$$(NF) \quad |\mathcal{K}|_p := \sum_{m=1}^{\infty} m\phi_{p^m}(\mathcal{K}) \geq |\mathcal{L}|_p.$$

Preuve : [TV02](lemma 2.6) $\square$

Corollaire 1.11 *Si $\mathcal{K}$ et $\mathcal{L}$ sont deux corps de nombres infinis, alors, pour tout nombre premier p :*

$$|\mathcal{K}.\mathcal{L}|_p \leq max\{|\mathcal{K}|_p, |\mathcal{L}|_p\},$$

et

$$|\mathcal{K}.\mathcal{L}|_\infty \leq max\{|\mathcal{K}|_\infty, |\mathcal{L}|_\infty\}.$$

Une première indication sur l'amplitude de l'ensemble $\Phi_{\mathcal{K}}$ est donnée par la proposition suivante :

Proposition 1.12 *Soit $\mathcal{K}$ un corps de nombres infini. Pour tout p,*

$$|\mathcal{K}|_p \leq |\mathcal{K}|_\infty \quad (NF).$$

De plus, si p est ramifié dans le corps de nombres infini $\mathcal{K}/\mathbb{Q}$ asymptotiquement bon, l'inégalité est stricte.

Preuve : C'est un corollaire direct du théorème de décomposition des places dans les extensions séparables. En effet, aux étages finis K_i de notre corps de nombres infinis, on a (cf [Ser68] I, prop. 10)

$$\sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} = n,$$

où $e_{\mathfrak{p}}$ est l'indice de ramification de $\mathfrak{p}|p$ et $f_{\mathfrak{p}}$ son indice d'inertie. On a alors

$$\sum_i i\Phi_{p^i} = \sum_{\mathfrak{p}|p} f_{\mathfrak{p}} \leq \sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} = n.$$

Divisant par g, et faisant tendre g vers l'infini, on obtient le premier résultat.

Supposons que p soit ramifié dans $K/\mathbb{Q}$. Soient $\mathfrak{p}_1, ..., \mathfrak{p}_n$ les idéaux premiers au-dessus de p et supposons $e_{\mathfrak{p}_1} \geq 2$. Soit (K_i/K) une tour représentant $\mathcal{K}$. On a alors, pour tout i, j

$$\Phi_{p^i}(K_j) = \sum_{k=1}^{n} \Phi_{\mathfrak{p}_k, p^i}(K_j).$$

Comme chacune des sommes $\sum_i i\Phi_{\mathfrak{p}_k, p^i}(K_j)$ est plus petite que $[K_j : K]$, on obtient

$$\sum_i i\Phi_{p^i}(K_j) \leq n[K_j : K].$$

Comme $[K : \mathbb{Q}] \geq n+1$, on en déduit

$$\sum_i i\Phi_{p^i}(K_j) \leq \frac{n}{n+1}[K_j : \mathbb{Q}].$$

Divisant par le genre et passant à la limite, on obtient le résultat. $\square$

Remarque:

i. Ainsi, si $\lim n_i/g_i$ est nulle, tous les invariants sont nuls et la tour est asymptotiquement mauvaise. C'est le cas par exemple des extensions abéliennes, ou de celles qui contiennent une partie abélienne infinie, entendant par là que la plus grande sous-extension abélienne de $\mathcal{K}/K$, pour un certain corps global K, est infinie (voir [FPS92] dans le cas des corps de fonctions). En fait, si on prend une tour au hasard, elle a toutes les chances d'être mauvaise.

ii. Il y a peu de chances de montrer une réciproque à la deuxième partie de la proposition 1.12, car il est très probable qu'on ait une perte à l'infini dans la somme, et avoir $|\mathcal{K}|_p = 0$ tandis que $|\mathcal{K}|_\infty > 0$. On donnera, à la fin du second chapitre, un exemple de tel corps global infini (voir théorème 2.45). Toutefois, nous verrons plus tard que nous pouvons compléter légèrement la proposition dans le cas galoisien.

1.2 Inégalité fondamentale

Dans ce paragraphe nous allons décrire deux inégalités obtenues avec et sans l'hypothèse de Riemann généralisée (GRH) à partir des formules explicites de Guinand-Weil. Elles donneront une seconde indication quant à l'ensemble Φ.

Les formules explicites

Commençons par exposer les formules explicites dans le cas des corps de fonctions. Nous utiliserons la version suivante, due à Serre :

Théorème 1.13 (Formules explicites) *(FF) Soit K un corps de fonctions. Pour toute suite $v = (v_n)$ telle que $\sum v_n r^{\frac{n}{2}}$ converge, la série $\sum v_n r^{-\frac{n}{2}} \sum_{m/n} m\Phi_{r^m}$ converge et on a :*

$$\sum_{n=1}^{\infty} v_n r^{-\frac{n}{2}} \sum_{m/n} m\Phi_{r^m} = \psi_v(r^{1/2}) + \psi_v(r^{-1/2}) - \sum_{j=1}^{g}\sum_{n=1}^{\infty} v_n r^{-n/2}(\pi_j + \bar{\pi}_j),$$

où π_j sont les inverses des racines du numérateur de la fonction zêta de K et $\psi_v(t) = \sum_{n=1}^{\infty} v_n t^n$.

Dans ce cas, l'égalité est particulièrement simple. Cela provient du fait qu'il n'y a pas de facteurs archimédiens et que nous disposons de GRH. Enonçons à présent les formules explicites dans le cas des corps de nombres.

Théorème 1.14 (Formules explicites) *Soit K un corps de nombres. Soit F une fonction test paire, dérivable et positive définie sur $\mathbb{R}$ telle que $F(0) = 1$ et telle qu'il existe c et ε tels que*

$$F(x), F'(x) \leq ce^{-(1/2+\varepsilon)|x|} \text{ lorsque } x \to \infty.$$

Considérons la transformée de Melin de F :

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x)e^{(s-1/2)x}dx.$$

Alors on a l'égalité suivante :

$$\log D_K = n_1 \frac{\pi}{2} + n(\gamma + \log 8\pi) - n \int_0^{+\infty} \frac{1 - F(x)}{2\, sh\frac{x}{2}} dx - n_1 \int_0^{+\infty} \frac{1 - F(x)}{2\, ch\frac{x}{2}} dx$$

$$-4 \int_0^{+\infty} F(x)\, ch\frac{x}{2} dx + \sum_{\rho}{}' \Phi(\rho) + 2 \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \mathrm{N}\mathfrak{p}^{-m/2} F(m \log \mathrm{N}\mathfrak{p}) \log \mathrm{N}\mathfrak{p},$$

où ρ parcourt l'ensemble des zéros de la fonction zêta dans la bande critique, le $'$ signifiant qu'on groupe ρ et $\bar{\rho}$ dans la sommation, et où $\mathfrak{p}$ parcourt les places finies de K, $\mathrm{N}\mathfrak{p}$ étant sa norme absolue.

En choisissant intelligemment F et après de rudes calculs, on obtient les résultats suivants :

Théorème 1.15 (Inégalité fondamentale sous GRH)) *Pour une famille asymptotiquement exacte de corps de nombres on a :*

$$(NF - GRH) \quad \sum_q \frac{\phi_q \log q}{\sqrt{q} - 1} + (\log \sqrt{8\pi} + \frac{\pi}{4} + \gamma/2)\phi_{\mathbb{R}} + (\log 8\pi + \gamma)\phi_{\mathbb{C}} \leq 1,$$

la somme étant prise sur les puissances de nombres premiers.

Preuve : On prend $F(x) = e^{-yx^2},\ y > 0$, et on suit [TV02](théorème 3.1). □

Dans le cas des corps de fonctions où GRH est vérifiée, un résultat semblable est valable :

Théorème 1.16 (Inégalité fondamentale pour les corps de fonctions) *Pour toute famille asymptotiquement bonne de corps de fonctions sur $\mathbb{F}_r$, on a :*

$$(FF) \quad \sum_{m=1}^{\infty} \frac{m\phi_{r^m}}{r^{\frac{m}{2}} - 1} \leq 1.$$

Preuve : Voir [TV02]. □

Enfin, lorsqu'on n'admet plus GRH, on peut obtenir le résultat un peu plus faible suivant :

Théorème 1.17 *Pour une famille asymptotiquement exacte de corps de nombres, on a*

$$(NF) \quad \sum_q \frac{\phi_q \log q}{q - 1} + (\gamma/2 + \log 2\sqrt{\pi})\phi_{\mathbb{R}} + (\gamma + \log 2\pi)\phi_{\mathbb{C}} \leq 1.$$

Preuve : Pour montrer ce résultat, on peut partir du lemme de Stark comme c'est fait dans [TV02](Prop. 3.2). □

Problème:

i. Est-ce que cette inégalité, combinée avec les autres inégalités précédemment décrites, délimitent réellement l'ensemble Φ ? On peut se demander ainsi s'il n'existe pas d'autres inégalités qui confinent encore davantage les valeurs possibles des invariants de corps globaux infinis.

ii. Plutôt que d'essayer de déterminer l'ensemble Φ, on peut s'interroger sur les valeurs prises par le défaut (la différence entre les deux termes de l'inégalité). Dans le cas des corps de fonctions sur un corps à q^2 éléments, le défaut peut être nul (par exemple pour les tours atteignant la borne de Drinfeld-Vlăduţ), mais dans le cas des corps de nombres, on ne sait pas si un défaut nul est possible.

1.3 Défaut d'une tour et distribution des zéros de la fonction zêta

Définissons le défaut d'un corps global infini comme la différence entre les deux membres de l'inégalité de base 1.17. Un problème plus faible que celui de la description de l'ensemble Φ est celui de l'étude des valeurs pouvant être prises par le défaut. Nous allons dans ce paragraphe étudier quelques propriétés de ce défaut. Comme il y a trois inégalités, nous allons considérer trois défauts $\delta^{(1)}$, $\delta^{(2)}$ et $\delta^{(3)}$ correspondant au défaut pour les corps de nombres sous GRH, sans GRH et pour les corps de fonctions respectivement :

$$\begin{aligned}
(NF-GRH) \quad \delta^{(1)} &= 1 - \sum_q \frac{\phi_q \log q}{\sqrt{q}-1} - (\log\sqrt{8\pi} + \frac{\pi}{4} + \gamma/2)\phi_{\mathbb{R}} - (\log 8\pi + \gamma)\phi_{\mathbb{C}}, \\
(NF) \quad \delta^{(2)} &= 1 - \sum_q \frac{\phi_q \log q}{q-1} - (\gamma/2 + \log 2\sqrt{\pi})\phi_{\mathbb{R}} - (\gamma + \log 2\pi)\phi_{\mathbb{C}}, \\
(FF) \quad \delta^{(3)} &= 1 - \sum_{m=1}^{\infty} \frac{m\phi_{r^m}}{r^{\frac{m}{2}}-1}.
\end{aligned}$$

Les défauts sous GRH sont intimement liés à la distribution limite des zéros des fonctions zêta des étages finis du corps global infini. Suivant [TV02], considérons $\mathcal{S}'$ l'espace des distributions tempérées, notons $\mathcal{M}$ l'espace des mesures, et $\mathcal{M}_{sl} = \mathcal{S}' \cap \mathcal{M}$ celui des mesures à croissance lente.

Soit $\mathcal{K} = (K_i)$ une famille asymptotiquement exacte de corps de nombres (resp. corps de fonctions), définissons les mesures

$$\Delta_{K_i} := \frac{\pi}{g_i} \sum_\rho \delta_{t(\rho)},$$

où ρ parcourt les zéros non triviaux de la fonction zêta de K_i, $t(\rho) = (\rho - \frac{1}{2})/i$, et δ_a désigne la mesure de Dirac en a. Comme on suppose GRH, $t(\rho)$ est réel (resp. défini modulo 2π, on le prendra dans $]-\pi, \pi]$) et on définit ainsi des mesures discrètes sur $\mathbb{R}$. Enonçons alors le théorème 5.1 de [TV02].

Théorème 1.18 *Pour une famille asymptotiquement exacte de corps de nombres* $\mathcal{K} = \{K_i\}$, *(resp. corps de fonctions) la limite*

$$\Delta_{\mathcal{K}} = \lim_{i\to\infty} \Delta_{K_i}$$

existe dans l'espace des mesures à croissance lente sur $\mathbb{R}$ (resp. dans l'espace des mesures sur $\mathbb{R}/2\pi\mathbb{Z}$ muni de la topologie faible). De plus, Δ admet une densité continue M_ϕ, telle que

$$M_\phi(0) = \delta_{\mathcal{K}}^{(1)} \text{ (resp. } M_\phi(0) = \delta_{\mathcal{K}}^{(3)}\text{).}$$

Remarque:

i. Bien qu'on ne l'ait pas définie ici, le défaut est également la valeur en $\frac{1}{2}$ de la dérivée logarithmique de la fonction zêta limite, cf [TV02](5.1,5.2).

ii. Malheureusement, $M_\phi(t)$ n'est pas croissante en $\mathcal{K}$ (pour l'inclusion) pour tout t, contrairement à sa valeur en 0 (voir théorème 2.50).

1.4 Conditions suffisantes à une tour pour être bonne

Dans ce paragraphe, nous allons mettre en évidence des conditions qui permettent à un corps global infini d'être bon. Ces conditions sont connues des experts, mais il semble qu'elles n'aient été écrites que dans le cas des corps de fonctions et dans le cas galoisien. Nous allons traiter dans le même temps corps de fonctions et corps de nombres et ainsi enrichir le parallèle existant entre ces corps globaux.

Commençons par quelques définitions. Dans le cas d'un corps global K, rappelons qu'un diviseur de K est un élément du groupe libre abélien engendré par les places de K. Si $D = \sum_{P \in P(K)} \alpha_P P$ est un diviseur de K, α_P sera appelé l'exposant de P dans D (bien que la notation soit additive). Si $\alpha_P > 0$ on dira que P divise D. Si tous les α_P sont positifs, on dira que D est positif.

Définissons à présent le degré d'un idéal de l'anneau des entiers d'un corps de nombres et d'un diviseur d'un corps de fonctions. Etant donné un idéal $\mathfrak{q} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$ de l'anneau des entiers d'un corps de nombres K décomposé en produit d'idéaux premiers, on pose

$$\deg \mathfrak{q} = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \log \mathrm{N}\mathfrak{p},$$

où $\mathrm{N}\mathfrak{p}$ est la norme (absolue) de l'idéal $\mathfrak{p}$. Pour une place P d'un corps de fonctions K, correspondant à un idéal maximal M_P d'un anneau O_P de valuation, on pose $\deg P = [O_P/M_P : \mathbb{F}_r]$. Une place de degré 1 sera appelée place rationnelle. Etant donné un diviseur $D = \sum_{P \in P(K)} \alpha_P P$ d'un corps de fonctions K, on posera naturellement

$$\deg D = \sum_{P} \alpha_P \deg P.$$

Les définitions sont compatibles puisque, dans le cas des corps de fonctions, on utilise le logarithme en base r.

Rappelons à présent le théorème de Riemann-Hurwitz qui est la clé du critère que nous allons donner. Gardant les définitions du premier paragraphe, nous noterons $\mathfrak{D}_{L/K}$ la différente de L/K. C'est, dans le cas des corps de nombres, l'inverse de l'idéal $\{x \in L | Tr(x\mathcal{O}_L) \subset \mathcal{O}_K\}$ de $\mathcal{O}_L$. Dans celui des corps de fonctions, c'est un diviseur dont la définition est similaire, on se reportera à [NX01](1.3.9). Par soucis de netteté, nous allons poser $g_K^* = g_K$ dans le cas des corps de nombres, et $g_K^* = g_K - 1$ dans le cas des corps de fonctions, afin d'obtenir un théorème homogène. Remarquons enfin que cela ne change pas les propriétés asymptotiques que nous voulons étudier. Enfin, dans tout ce paragraphe, log désignera le logarithme népérien dans le cas des corps de nombres, le logarithme en base r dans le cas des corps de fonctions.

Théorème 1.19 ***(Riemann-Hurwitz)*** *Soit L/K une extension de corps globaux sans extension des constantes dans le cas des corps de fonctions. Alors on a :*

$$g_L^* = [L : K]g_K^* + \frac{1}{2} \deg \mathfrak{D}_{L/K}.$$

Preuve : On se rapporte à [Neu99](III,3.13) dans le cas des corps de nombres et [NX01] (1.3.10) dans le cas des corps de fonctions. □

> **Remarque:** Dans le cas général, la formule de Riemann-Hurwitz devient, pour une extension de corps de fonctions F'/k' de F/k (où k' et k sont les corps des constantes de F' et F respectivement),
>
> $$g_{F'}^* = \frac{[F' : F]}{[k' : k]} g_F^* + \frac{1}{2} \deg \mathfrak{D}_{F'/F}.$$

Définition 1.20 *Soit $\mathcal{K}$ un corps de nombres infini (resp. corps de fonctions infini). On définit le lieu de ramification $Ram(\mathcal{K})$ de $\mathcal{K}$ comme étant l'ensemble des places de $\mathbb{Q}$ (resp. $\mathbb{F}_r(t)$) qui se ramifient dans une extension finie contenue dans $\mathcal{K}$. Pour une sous-extension finie K_0 de $\mathcal{K}$, définissons le lieu de ramification sauvage $Rams(\mathcal{K}/K_0)$ de $\mathcal{K}/K_0$ comme l'ensemble des places de K_0 sauvagement ramifiées dans au moins une extension finie de K_0 contenue dans $\mathcal{K}$. De même on emploiera la dénomination de lieu de décomposition de K/K_0 pour qualifier l'ensemble des places de K_0 totalement décomposées dans l'extension K/K_0, éventuellement infinie, noté souvent $Dec(K/K_0)$. Enfin on notera $Dec(K)$ pour le lieu de décomposition de K sur le corps de base.*

> **Remarque:** Comme le lieu de ramification de $K_0/\mathbb{Q}$ (ou $\mathbb{F}_r(t)$ suivant le cas) est fini pour une extension finie K_0, il reviendra au même de considérer $Ram(\mathcal{K}/K_0)$ (notation naturelle) ou $Ram(\mathcal{K})$. Toutefois on ne pourra pas agir de la sorte en ce qui concerne la ramification sauvage. En effet, celle-ci peut avoir des effets désastreux sur le genre des corps, comme nous allons le voir par la proposition suivante :

Rappelons une proposition que l'on peut trouver dans [Neu99](III,2.6) pour le cas des corps de nombres, et dans [NX01](1.3.12) pour celui des corps de fonctions.

Proposition 1.21 *Soit L/K une extension de corps de nombres (resp. de corps de fonctions). Une place finie de L est ramifié sur K si et seulement si elle divise $\mathfrak{D}_{L/K}$. De plus, si s est l'exposant de $\mathfrak{P}$ dans la décomposition de $\mathfrak{D}_{L/K}$ en produit d'idéaux premiers (resp. sous forme de diviseur, dans le cas des corps de fonctions) et si e désigne l'indice de ramification de $\mathfrak{P}$, on a alors $s \geq e - 1$, avec égalité si et seulement si $\mathfrak{P}$ est modérément ramifiée.*

Muni de cette proposition et du théorème de Riemann-Hurwitz nous pouvons à présent donner une condition suffisante pour qu'un corps global soit asymptotiquement bon.

Proposition 1.22 *Soit $\mathcal{K}$ un corps de nombres (resp. corps de fonctions) infini tel que*

$$\inf_{K' finie} \#Rams(\mathcal{K}/K') = 0.$$

Alors $\mathcal{K}$ est asymptotiquement bon (resp. $\lambda(\mathcal{K}) > 0$) si son lieu de ramification S est fini. De plus, si $\mathcal{K}/K$ (pour une certaine extension K finie) est galoisienne, la réciproque est vraie. Enfin, si $\mathcal{K} = \cup K_i$ est presque-galoisienne (pour la famille (K_i) de corps globaux), $\mathcal{K}$ est asymptotiquement bon (resp. $\lambda(\mathcal{K}) > 0$) si et seulement si

$$\sum_{i=0}^{\infty} \frac{1}{n_{K_i}} \sum_{\mathfrak{p} \in Ram(K_{i+1}/K_i)} \log \mathrm{N}(\mathfrak{p}) < \infty.$$

Preuve : Soit $(K_i)_{i\in\mathbb{N}}$ ($K_0 = K$) une tour représentant $\mathcal{K}$. Supposons que S soit fini. Il s'agit de montrer que le ratio $g^*_{K_i}/n_{K_i}$ est borné. On peut ici remplacer n_{K_i} par $[K_i : K_0]$, les calculs s'en trouvant modifiés par un facteur égal au degré de K_0 sur le corps de base.

Soit K_j un corps global de genre > 1 tel que $\#Rams(\mathcal{K}/K_j) = 0$. Quitte à renommer les corps, on suppose que $j = 0$. On écrira g^*_i, n_i pour $g^*_{K_i}, [K_i : K_0]$ respectivement. S désignera à présent $Ram(\mathcal{K}/K_0)$ et notons $S_i = Ram(K_i/K_0)$. On a alors, d'après le théorème de Riemann Hurwitz et la proposition précédente :

$$g^*_i = n_i g^*_0 + \frac{1}{2} \sum_{\mathfrak{p}\in S_i} \sum_{\mathfrak{P}/\mathfrak{p}} (e_{\mathfrak{P}} - 1) f_{\mathfrak{P}} \log \mathrm{N}\mathfrak{p},$$

où $\mathfrak{P}$ est une place au-dessus de $\mathfrak{p}$, $e_{\mathfrak{P}}$ désigne l'indice de ramification de $\mathfrak{P}/\mathfrak{p}$ communément noté $e_{\mathfrak{P}/\mathfrak{p}}$ et $f_{\mathfrak{P}}$ le degré d'inertie de $\mathfrak{P}/\mathfrak{p}$ habituellement noté $f_{\mathfrak{P}/\mathfrak{p}}$.

Comme les extensions sont toutes supposées séparables,

$$\sum_{\mathfrak{P}/\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = n_i,$$

et on en déduit

$$\begin{aligned} g^*_i &\leq n_i g^*_0 + \frac{1}{2} n_i \sum_{\mathfrak{p}\in S_i} \log \mathrm{N}\mathfrak{p}, \\ &\leq n_i g^*_0 + \frac{1}{2} n_i \sum_{\mathfrak{p}\in S} \log \mathrm{N}\mathfrak{p}, \end{aligned}$$

cette dernière somme étant finie car S est finie, on a démontré le premier point.

Supposons à présent que S est inifini et que la tour (K_i) est galoisienne, c'est à dire que K_i/K_0 est une extension galoisienne. Cette fois, on doit montrer que g^*_i/n_i n'est pas borné.

$$g^*_i = [K_i, K_0] g^*_0 + \frac{1}{2} \sum_{\mathfrak{p}\in S_i} \sum_{\mathfrak{P}/\mathfrak{p}} (e_{\mathfrak{P}} - 1) f_{\mathfrak{P}} \log \mathrm{N}\mathfrak{p}.$$

Comme $e_{\mathfrak{P}} - 1 \geq e_{\mathfrak{P}}/2$ car $e_{\mathfrak{P}} \geq 2$ (l'extension est galoisienne), on en déduit que

$$\begin{aligned} g_i^* &\geq n_i g_0^* + \frac{1}{2} \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p} \sum_{\mathfrak{P}/\mathfrak{p}} \frac{e_{\mathfrak{P}}}{2} f_{\mathfrak{P}} \\ &\geq n_i g_0^* + \frac{1}{4} n_i \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p}. \end{aligned}$$

Cette fois la somme diverge car $\#S_i$ tend vers l'infini, et cela montre la réciproque.

Enfin montrons l'assertion quand $\mathcal{K}$ est presque-galoisienne. Notons cette fois S_i le lieu de ramification de K_{i+1}/K_i. Appliquons de même Riemann-Hürwitz. Comme les extensions K_{i+1}/K_i sont galoisiennes, on a, de même :

$$\begin{aligned} \frac{n_{i+1}}{n_i} g_i^* + \frac{1}{4} \frac{n_{i+1}}{n_i} \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p} \quad &\leq g_{i+1}^* \leq \quad \frac{n_{i+1}}{n_i} g_i^* + \frac{1}{2} \frac{n_{i+1}}{n_i} \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p} \\ \frac{g_i^*}{n_i} + \frac{1}{4\, n_i} \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p} \quad &\leq \tfrac{g_{i+1}^*}{n_{i+1}} \leq \quad \frac{g_i^*}{n_i} + \frac{1}{2\, n_i} \sum_{\mathfrak{p} \in S_i} \log \mathrm{N}\mathfrak{p}. \end{aligned}$$

Par une récurrence immédiate on obtient :

$$\frac{g_0^*}{n_0} + \frac{1}{4} \sum_{j=0}^{i} \sum_{\mathfrak{p} \in S_j} \frac{\log \mathrm{N}\mathfrak{p}}{n_j} \leq \frac{g_{i+1}^*}{n_{i+1}} \leq \frac{g_0^*}{n_0} + \frac{1}{2} \sum_{j=0}^{i} \sum_{\mathfrak{p} \in S_j} \frac{\log \mathrm{N}\mathfrak{p}}{n_j}.$$

Ainsi le comportement de g_i est le même que celui de la double somme et on a montré l'équivalence. $\square$

Exemple : Nous donnerons des exemples de telles tours dans le chapitre suivant. Cependant, donnons ici un contre-exemple montrant la nécessité de l'hypothèse concernant la ramification sauvage. Considérons la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$. Pour la former, considérons, pour tout $n > 1$, la p-part de $\mathbb{Q}(\mu_{p^n})$ — le corps fixé par les éléments de $Gal(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ dont l'ordre est premier à p. Elle n'est ramifiée qu'en p, mais comme elle est abélienne, elle est asymptotiquement mauvaise (cela se voit aussi sur le calcul du discriminant que l'on a explicitement).

Remarque:

i. Il pourrait toutefois arriver qu'un corps global infini ayant un lieu de ramification sauvage non vide pour tout sous-corps fini soit asymptotiquement bon, si la contribution de la ramification sauvage reste faible. Dans le cas des corps de fonctions, un exemple de tour de Fermat donné par Garcia et Stichtenoth fournit un tel exemple [Sti99], mais un tel résultat nous est inconnu dans le cas des corps de nombres.

ii. Il est également possible qu'une extension, même presque-galoisienne, soit bonne malgré un ensemble de ramification infini. Pour cela il faut cependant qu'il soit peu ramifié à chaque étage fini par rapport au degré, ce qui donne des difficultés au niveau de la construction de telles tours.

Considérons à présent un corps global infini $\mathcal{K} = (K_i)$ tel que $\lambda(\mathcal{K}) > 0$ dans le cas d'un corps de fonctions, $\phi_\infty(\mathcal{K}) > 0$ dans celui d'un corps de nombres (ce qui est le cas s'il n'a pas de ramification sauvage, et que son lieu de ramification est fini).

Proposition 1.23 *Soit un corps global infini $\mathcal{K} = (K_i)$ tel que $\lambda(\mathcal{K}) > 0$ dans le cas d'un corps de fonctions, $\phi_\infty(\mathcal{K}) > 0$ dans celui d'un corps de nombres. Supposons qu'il existe une place $\mathfrak{p} \in P(K_0)$ telle que $\mathfrak{p}$ est totalement décomposée dans la tour (K_i). Alors $\phi_{\mathrm{N}\mathfrak{p}} \geq \lim_{i\to\infty} [K_i : K_0]/g(K_i) > 0$.*

Preuve : Notons $n_i = [K_i : K_0]$. Comme $\mathfrak{p}$ est totalement décomposé dans K_i/K_0 , $\Phi_{\mathrm{N}\mathfrak{p}}(K_i) \geq n_i$ on a

$$\frac{\phi_{\mathrm{N}\mathfrak{p}}}{g_i} = \frac{\phi_{\mathrm{N}\mathfrak{p}}}{n_i}\frac{n_i}{g_i} \geq \frac{n_i}{g_i}.$$

D'après les hypothèses, la limite de $\frac{n_i}{g_i}$ est strictement positive, et on en déduit le résultat. □

Donnons à présent une sorte de réciproque dans le cas des extensions galoisiennes de $\mathbb{Q}$ (qui se généralise à ses extensions finies) :

Proposition 1.24 *Soit $\mathcal{K}/\mathbb{Q}$ une extension galoisienne infinie représentée par la tour $(K_i)_{i\in\mathbb{N}}$. Pour tout p premier, il existe au plus un entier m tel que $\phi_{p^m} > 0$. Soit q une puissance d'un nombre premier p telle que $\phi_q > 0$. Alors il existe j telle que toutes les places au-dessus de p dans K_j soient totalement décomposées dans $\mathcal{K}/K_j$.*

Preuve : remarquons d'abord que dans une extension galoisienne finie K_i, toutes les places au-dessus de p ont même degré d'inertie $f_p(K_i)$ et même indice de ramification $e_p(K_i)$. De plus, pour tout m $\Phi_{p^m}(K_i)f_p(K_i)e_p(K_i) \leq n_i$. Ainsi, si $\Phi_{p^m}(K_i)/n_i$ a une limite strictement positive $e_p(K_i)f_p(K_i)$ est borné, et donc les places au-dessus de p sont totalement décomposées à partir d'un certain corps K_j. Toutes les places au-dessus de p sont donc de degré d'inertie $f = f_p(K_j)$ dans les extensions de K_j, seul ϕ_{p^f} peut être différent de 0. □

Nous pouvons également compléter la proposition 1.12

Proposition 1.25 *Considérons le cas d'une extension galoisienne $\mathcal{K} = \cup K_i$ de $\mathbb{Q}$, telle que $|\mathcal{K}|_p > 0$. Alors l'indice e_p de ramification de p dans $\mathcal{K}$ est fini, et on a $e_p|\mathcal{K}|_p = |\mathcal{K}|_\infty$ ($e_p = 1$ si et seulement si p n'est pas ramifiée dans $\mathcal{K}/\mathbb{Q}$).*

Preuve : Supposons que $\phi_q > 0$, pour une certaine puissance $q = p^d$ de p. Il existe j_0 telle que, pour tout $j \geq j_0$, toutes les places au-dessus de p dans K_j sont de norme q. L'égalité $\sum_{\mathfrak{p}|p} e_{\mathfrak{p}}f_{\mathfrak{p}} = n$ devient simplement $\Phi_q(K_i)e_i d = n_i$ (où e_i, f_i sont les indices de ramification de d'inertie de p dans K_i). Alors en divisant par g_i et en passant à la limite, on obtient $e_p d\phi_q = \phi_\infty$, où e_p est la limite entière ou infinie de la suite croissante d'entiers naturels e_i, ce qui termine la preuve. □

1.5 Tours et composita

Nous allons à présent donner quelques résultats élémentaires mais toutefois très importants sur les composita de corps globaux. Leur importance provient du fait qu'ils permettent, à partir d'une construction de corps global infini asymptotiquement bon d'en produire autant d'autres que l'on veut. Malheureusement il paraît difficile, à part dans le cas simple qu'on traitera à la fin du paragraphe, de connaître les invariants du compositum de corps globaux infinis. En effet, on ne connaît généralement pas le comportement de l'inertie des places par compositum, comme nous le verrons au chapitre suivant.

Dans tout ce qui suit, lorsqu'on considérera le compositum de deux corps de fonctions ayant même corps de constantes k, on supposera que son corps de constantes est également k. Cette propriété n'est pas restrictive en vue de nos applications, puisqu'on fera en sorte qu'une place rationnelle se décompose totalement, et dans ce cas, il n'y a pas d'extension des constantes possible (voir [NX01], §1.5 par exemple).

Proposition 1.26 *Soit E/K, F/K deux extensions finies séparables de corps globaux.*

i. Si $K \subset F \subset E$, E/K n'est pas ramifiée (resp. est modérément ramifiée) si et seulement si E/F et F/K ne sont pas ramifiées (resp. sont modérément ramifiées).

ii. Si E/K n'est pas ramifiée (resp. est modérément ramifiée), alors $E.F/F$ n'est pas ramifiée (resp. est modérément ramifiée).

iii. Si E/K et F/K ne sont pas ramifiées (sont modérément ramifiées), alors $E.F/K$ n'est pas ramifiée (resp. est modérément ramifiée).

Preuve : Pour montrer les assertions « non ramifiées » et « modérément ramifiées », on se ramène au cas local, et on applique la proposition analogue pour le cas local qu'on trouve dans [Lan94] (II, prop. 8 et 13). C'est rendu possible car la complétion du compositum est le compositum des complétions ([Lan02]XII.3), et que ces propriétés sont locales. Dans le cas des corps de fonctions, on peut également appliquer le lemme d'Abhyankar, qui nous donne directement le résultat, et en fait quelque chose de beaucoup plus fort. Rappelons alors ce lemme tel qu'on peut le trouver dans [Sti93] (III.8.9) :

Proposition 1.27 (lemme d'Abhyankar) *Soit F'/F une extension finie séparable de corps de fonctions. Supposons que $F' = F_1F_2$, avec $F \subset F_1, F_2 \subset F'$. Soit P' une place de F', P, P_1, P_2 ses restrictions à F, F_1, F_2 respectivement. Supposons qu'au moins l'une des extensions P_1/P ou P_2/P soit modérément ramifiée. Alors*

$$e(P'/P) = ppcm(e(P_1/P), e(P_2/P)).$$

□

On déduit de ce résultat le corollaire suivant :

Corollaire 1.28 *Soit $\mathcal{K}$ un corps global infini, représenté par la tour (K_i). Soit $\mathcal{L} = \cup L_i$, où L_i est la clôture galoisienne de K_i. Supposons $\mathcal{K}$ sans ramification sauvage, et non ramifié hors d'un ensemble fini de places S.*

i. On a alors $\lim\limits_{i\to\infty} \dfrac{n_{L_i}}{g_{L_i}} > 0$.

ii. Considérons $q = p^d$, et une place finie $\mathfrak{p}$ n'appartenant pas à S. Si $\phi_{\mathfrak{p},q}(\mathcal{L}) > 0$ alors

$$\sup_{\mathfrak{P}\in P(K_i), \mathfrak{P}|\mathfrak{p}} \mathrm{N}\mathfrak{P} \leq q.$$

Dans ce cas il existe $\mathfrak{P}|\mathfrak{p}$ dans un certain $P(K_i)$, de norme maximale tel que $\mathfrak{P}$ est totalement décomposé dans $\mathcal{K}/K_i$.

iii. Le compositum de deux corps de nombres modérément ramifiés, non ramifiés hors d'un ensemble fini de places est asymptotiquement bon.

Preuve :

i. C'est une conséquence directe de la proposition précédente : comme pour chaque i, L_i est le compositum de conjugués de K_i, on en déduit que L_i n'est pas ramifié hors de S et est modérément ramifié. D'après la proposition 1.22, cette limite est bien strictement positive.

ii. Supposons alors $\phi_{\mathfrak{p},q}(\mathcal{L}) > 0$. D'après 1.24, il existe i_0 tel que toutes les places au-dessus de $\mathfrak{p}$ dans L_i, $i \geq i_0$ ont pour norme q. Comme $K_i \subset L_i$, toutes les places au-dessus de $\mathfrak{p}$ dans K_i (pour tout i) ont une norme au plus q.

   Soit $\mathfrak{q}$ une place d'un certain K_i réalisant le maximum des normes des places au-dessus de $\mathfrak{p}$ (cela existe bien puisque les normes des places au-dessus de $\mathfrak{p}$ sont bornées par q). Ainsi toutes les places au-dessus de $\mathfrak{q}$ dans K_j, $j > i$, ont la même norme que $\mathfrak{q}$. Etant non ramifiée, $\mathfrak{q}$ est totalement décomposée.

iii. Le compositum jouit des mêmes propriétés qui garantissent le fait qu'il est asymptotiquement bon.

□

Remarque:

i. Ainsi, dans le cas des corps de nombres, la clôture galoisienne d'un corps modérément ramifié, non ramifié hors d'un ensemble fini, est asymptotiquement bonne.

ii. La réciproque à la seconde partie de la proposition peut malheureusement s'avérer être fausse, car le corps $\mathcal{L}$ est très gros par rapport à $\mathcal{K}$ en général, et en prenant les composita des conjugués des K_i, on peut a priori faire exploser les normes des idéaux au-dessus de p dans L_i.

iii. Dans le cas de places ramifiées, on peut obtenir un résultat similaire en considérant les places $\mathfrak{q}$ de norme et d'indice d'inertie maximal. En effet, celui-ci est également borné indépendamment de i d'après la condition $\phi_{\mathfrak{p},q}(\mathcal{L}) > 0$.

iv. Dans le cas des corps de fonctions, on a en fait un résultat plus fort, obtenu en utilisant l'inégalité de Castelnuovo : en effet, supposons que le corps de fonctions L de corps de constantes k soit le compositum de deux corps de fonctions E et F ayant même corps de constantes k. Alors son genre vérifie

$$\frac{g_{E.F}}{n_{E.F}} \leq \frac{g_E}{n_E} + \frac{g_F}{n_F} + 1.$$

   Ainsi, sous la condition que les trois corps suivant aient le même corps de constantes $\mathbb{F}_r$, le compositum $\mathcal{F}$ de deux corps de fonctions infinis $\mathcal{F}_1$, $\mathcal{F}_2$, tels que $\lambda(\mathcal{F}_i) > 0$, $i \in \{1, 2\}$, vérifie $\lambda(\mathcal{F}) > 0$.

Proposition 1.29 *Soient E/K, F/K deux extensions séparables de corps globaux et $\mathfrak{p} \in P(K)$.*

i. Supposons $K \subset F \subset E$. $\mathfrak{p}$ se décompose totalement dans E/K si et seulement si $\mathfrak{p}$ est totalement décomposée dans F/K et toutes les places au-dessus d'elle dans F se décomposent totalement dans E/F.

ii. Si $\mathfrak{p} \in P(K)$ se décompose totalement dans E, alors toute place au-dessus de $\mathfrak{p}$ dans F se décompose totalement dans $E.F/F$.

iii. Si $\mathfrak{p}$ se décompose totalement dans E/K et F/K alors $\mathfrak{p}$ se décompose totalement dans $E.F/K$.

Preuve : Une place p se décompose totalement dans E si et seulement si tout plongement de E dans $\bar{K}_p$ sur K envoie E sur K_p. On en déduit les trois assertions — cf [Lan94] (II, th. 2). □

> **Remarque:** Cette proposition sera très importante pour la suite, car elle nous garantit la décomposition des places dans les tours formées par compositum (voir le chapitre suivant).

Terminons nos généralités par le résultat suivant sur le compositum de deux extensions abéliennes. C'est un résultat important, car il ruine toute chance d'obtenir des tours asymptotiquement bonnes en prenant le compositum d'une infinité d'extensions obtenues par la théorie du corps de classes.

Proposition 1.30 *Soient E et F deux extensions galoisiennes de K linéairement disjointes. Alors EF/K est galoisienne, et $Gal(EF/K) = Gal(E/K) \times Gal(F/K)$. Ainsi, si deux extensions sont abéliennes, leur compositum est également abélien.*

Preuve : On se reportera à [Lan02]($VI, th.$1.14). Le fait que les corps soient linéairement disjoints n'intervient que pour montrer l'égalité des groupes de Galois, et dans tous les cas le morphisme de restriction $\sigma \to (\sigma_{|K}, \sigma_{|E})$ est injectif. □

Nous allons à présent considérer la question suivante :

> **Problème:** Est-il possible, étant donné deux corps globaux infinis $\mathcal{K}$ et $\mathcal{L}$ de connaître les invariants de leur compositum $\mathcal{KL}$?

Cette question apparaît comme très difficile a priori, car on ne sait pas bien comment se comportent les places dans le compositum de deux corps, à l'exception du cas où elles sont totalement décomposées. On peut toutefois apporter quelques éléments de réponse dans certains cas.

Traitons le cas le plus simple de compositum qu'on puisse étudier. Considérons un corps de nombres infini $\mathcal{K}$. Notons $\hat{n}$ son degré surnaturel et $\hat{\delta}$ son discriminant surnaturel (en fait le produit des ℓ^∞ pour ℓ ramifié dans la tour). Prenons un entier ℓ (non nécessairement premier) premier à $\hat{n}$, et L une extension galoisienne de $\mathbb{Q}$ de degré ℓ, dont le discriminant est premier à $\hat{\delta}$.

Afin de calculer les invariants du corps de nombres infini $\mathcal{K}.L$, considérons une tour $(K_i)_{i \in \mathbb{N}}$ représentant $\mathcal{K}$. Calculons, pour $q \in A_f$, $\Phi_q(K_n.L)$. Dans ce cas bien particulier, le résultat intuitif suivant est vrai :

Proposition 1.31 *Soient $\mathcal{K}$ et L vérifiant les propriétés ci-dessus. Supposons que l'on soit dans l'un des deux cas suivant :*

i. ℓ est premier,

ii. $(K_i)_{i\in\mathbb{N}}$ est galoisienne,

alors, on a :

$$\Phi_{p^d}(L.K_n) = \sum_{ij=d} \Phi_{p^i}(L)\Phi_{p^j}(K_n).$$

Preuve : i. Compte tenu des hypothèses, il n'y a dans $L/\mathbb{Q}$ que trois possibilités pour un premier p de $\mathbb{Z}$: il est ou bien totalement ramifié, ou bien il est totalement inerte, ou bien il est totalement décomposé. Dans ce premier cas, comme ℓ n'est pas ramifié dans $K_n/\mathbb{Q}$, l'indice de ramification des places $p_1, ..., p_m$ au-dessus de p vaut 1. Par multiplicativité, chaque p_i a un indice de ramification p dans $L.K_n/K_n$, et ils sont donc totalement ramifiés dans $L.K_n/K_n$. On en déduit $\Phi_q(L.K_n) = \Phi_q(K_n)$ dès que q n'est pas premier avec δ_L.

De même, si p est totalement inerte dans $L/\mathbb{Q}$, et si q est une puissance de p, alors on a $\Phi_{q^\ell}(L.K_n) = \Phi_q(K_n)$ (les autres valant 0 si q n'est pas une puissance $\ell^{\text{ième}}$ d'une puissance de p).

Enfin si p est totalement décomposée dans L, toutes les places au-dessus de p dans K_n sont totalement décomposées dans $L.K_n/K_n$ et on en déduit $\Phi_q(L.K_n) = \ell\Phi_q(K_n)$ dès que p divise q.

ii. Considérons à présent une extension galoisienne $K/\mathbb{Q}$ et prenons un premier p de $\mathbb{Z}$. Notons e_L, f_L, g_L l'indice de ramification de p, son indice d'inertie et le nombre de places au-dessus de p dans L respectivement. On notera e_K, f_K, g_K ceux qui correspondent aux corps K. D'après les hypothèses faites sur les degrés, e_K (resp. f_K, resp. g_K) est premier avec e_L (resp. f_L, resp. g_L) car ils divisent le degré de nos extensions séparables. Comme e_L et e_K divisent $e_{K.L}$ (notations naturelles), $e_L.e_K$ divise $e_{K.L}$, et de même f_Lf_K divise $f_{L.K}$, g_Kg_L divise $g_{L.K}$. Par multiplicativité du degré, et d'après le théorème de décomposition des places dans les extensions séparables, on en déduit que ces quantités sont en fait égales ($e_Ke_L = e_{KL}$ etc). Ainsi, au-dessus de p, il y a $\Phi_{p^{f_K}}(K)\Phi_{p^{f_L}}(L)$ places de norme $p^{f_Kf_L}$, et on en déduit la proposition. □

> **Remarque:** Un tel résultat peut également être obtenu pour un corps global infini $\mathcal{K}/K$ et une extension cyclique L/K de degré premier (corps de nombres et corps de fonctions) tels que les lieux de ramification sont disjoints :
>
> $$\Phi_{\mathfrak{p},p^d}(L.K_n) = \sum_{ij=d} \Phi_{\mathfrak{p},p^i}(L)\Phi_{\mathfrak{p},p^j}(K_n).$$
>
> Néanmoins, ce résultat est faux en général, comme en attestera la proposition 2.41.

Rappelons qu'on a, pour un tel compositum de corps de nombres linéairement disjoints dont les discriminants sont premiers entre eux,

$$g_{L.K_n} = [L : \mathbb{Q}]g(K_n) + [K_n : \mathbb{Q}]g(L).$$

On en déduit alors le résultat suivant :

Corollaire 1.32 *Sous l'une des deux hypothèses de la proposition précédente, on a :*

$$\phi_{p^d}(L.\mathcal{K}) = \sum_{ij=d} \frac{\phi_{p^i}(L)\phi_{p^j}(\mathcal{K})}{\phi_\infty(L) + \phi_\infty(\mathcal{K})},$$

et

$$\phi_\infty(L.\mathcal{K}) = \frac{\phi_\infty(\mathcal{K})\phi_\infty(L)}{\phi_\infty(\mathcal{K}) + \phi_\infty(L)}.$$

Preuve : On divise par le genre de $L.K_n$, et ce n'est qu'un simple calcul. Dans le cas archimédien, cela donne

$$\phi_\infty(L.K_n) = \frac{[L:\mathbb{Q}][K_n:\mathbb{Q}]}{[L:\mathbb{Q}]g(K_n) + [K_n:\mathbb{Q}]g(L)} = \frac{\phi_\infty(K_n)\phi_\infty(L)}{\phi_\infty(K_n) + \phi_\infty(L)}.$$

□

> **Problème:** La relation ci-dessus est la relation que l'intuition nous impose dès le départ. Sous quelles hypothèses est-elle vérifée ?

Enfin, dans le cas où L est un corps de nombres infini, on peut donner de la même façon un résultat analogue sous les mêmes conditions très fortes :

Proposition 1.33 *Soient $\mathcal{K}$ et $\mathcal{L}$ deux corps de nombres infinis asymptotiquement bons, tels que leurs degrés surnaturels et leurs discriminants surnaturels sont premiers entre eux. Supposons qu'ils soient galoisiens. Alors on a*

$$\phi_{p^d}(\mathcal{L}.\mathcal{K}) = \sum_{ij=d} \frac{\phi_{p^i}(\mathcal{L})\phi_{p^j}(\mathcal{K})}{\phi_\infty(\mathcal{L}) + \phi_\infty(\mathcal{K})},$$

$$\phi_\infty(\mathcal{K}\mathcal{L}) = \frac{\phi_\infty(\mathcal{K})\phi_\infty(\mathcal{L})}{\phi_\infty(\mathcal{K}) + \phi_\infty(\mathcal{L})}.$$

> **Remarque:** Si l'un d'eux est mauvais, alors les quantités ci-dessus sont nulles. On peut également donner des résultats analogues dans le cas des corps de fonctions, on remplaçant ϕ_{p^i} par $\phi_{\mathfrak{p},p^i}$.

Chapitre 2

Tours asymptotiquement bonnes de corps globaux

Sommaire

Constuire une tour asymptotiquement bonne s'avère être une tâche très difficile. Dans le cas des corps de fonctions, il existe différentes méthodes. Tout d'abord, on peut construire de façon explicite — c'est à dire au moyen d'équations— de bonnes tours, et même optimales si r est un carré (Garcia et Stichtenoth). Mais on peut également utiliser des courbes modulaires, classiques (Ihara [Iha81]), ou de Shimura (Tsfasman-Vlăduţ-Zink [TVZ82]), ou encore de Drinfeld, et obtenir des courbes optimales dans le cas où r est un carré. A notre disposition, nous avons en outre la possibilité de les construire grâce à la théorie du corps de classes (Serre [Ser85]). On peut aussi utiliser des techniques inspirées des équations différentielles. Mais dans le cas des corps de nombres, la seule construction connue est celle des tours de corps de classes, qui ne sont absolument pas explicites, ce qui limite d'autant nos moyens d'action.

2.1 Constructions explicites

La première chose qui vient à l'esprit lorsque l'on souhaite exhiber un corps global infini asymptotiquement bon est de vouloir le construire explicitement au moyen d'un polynôme ou d'une famille de polynômes. Malheureusement, on se rend très vite compte que le problème est très difficile car on demande à la fois à la tour d'être peu ramifiée, mais en plus que la ramification sauvage ne soit pas trop profonde. Toutefois, Garcia et Stichtenoth [GS95] sont parvenus à exhiber de telles tours de corps de fonctions (qu'on appellera itérée) asymptotiquement bonnes (même optimales dans certains cas). Dans le cas des corps de nombres, Aitken, Hajir et Maire [AHM05] ont proposé une méthode inspirée de la dynamique qui permet d'obtenir des tours itérées non ramifiées hors d'un ensemble fini, mais sans toutefois pouvoir contrôler la ramification sauvage (ils sont également capables de contrôler la ramification sauvage, mais alors la tour se ramifie en une infinité de places). Malheureusement, nous n'avons pas pu construire explicitement des tours de corps de nombres, nous allons donc porter notre attention principalement sur les tours que nous avons à disposition, c'est à dire les tours de corps de classes.

2.2 Théorie du corps de classes et tours non ramifiées

La théorie du corps de classes compte parmi les plus belles réussites du vingtième siècle, répondant à la question suivante. Etant donné un corps de nombres K, peut-on caractériser toutes les extensions abéliennes de K en termes d'éléments de K ? Autrement dit, est-ce qu'un corps de nombres contient toutes les informations concernant ses extensions galoisiennes dont le groupe de Galois est commutatif ? Nous allons d'abord en exposer les points principaux, puis nous expliquerons en quoi elle est importante pour notre problème en décrivant le critère de Golod-Schafarevitch.

2.2.1 Résultats principaux de la théorie du corps de classes

Commençons par quelques notations. Soit K un corps global, on notera A_K le groupe des adèles de K [Neu99](VI,1), $I_K = A_K^*$ son groupe d'idèles et enfin $C_K = I_K K^*/K^*$ le groupe des idèles principaux. A_K et I_K sont munis de la topologie naturelle du produit restreint et pour C_K de la topologie quotient. C_K admet des sous-groupes d'indices finis remarquables pour cette topologie, appelés sous-groupes de congruences mod $\mathfrak{m}$ qui sont définis ainsi : pour tout diviseur positif $\mathfrak{m} = \sum_{\mathfrak{p}\in P(K)} n_\mathfrak{p}\mathfrak{p}$ de K, on pose $U_\mathfrak{p}^{(0)} = U_\mathfrak{p}$, et si $n_\mathfrak{p} > 0$,

$$U_\mathfrak{p}^{(n_\mathfrak{p})} := \begin{cases} 1+\mathfrak{p}^{n_\mathfrak{p}}, \text{ si } \mathfrak{p} \text{ est fini} \\ \mathbb{R}_+^*, \text{ si } \mathfrak{p} \text{ est réelle,} \\ \mathbb{C}^*, \text{ si } \mathfrak{p} \text{ complexe.} \end{cases}$$

On considère alors le sous-groupe des idèles, pour $\mathfrak{m}$ un tel diviseur vérifiant $n_\mathfrak{p} = 0$ si $\mathfrak{p}$ est archimédienne, $I_K^\mathfrak{m} = \prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})}$, et le sous-groupe de congruence mod $\mathfrak{m}$, $C_K^\mathfrak{m} = I_K^\mathfrak{m} K^*/K^*$. Enfin le groupe quotient $Cl_K^\mathfrak{m} = C_K/C_K^\mathfrak{m}$ (la notation n'est pas fortuite) est appelé groupe de classes de rayon mod $\mathfrak{m}$. Dans le cas où $\mathfrak{m}$ est trivial, ce quotient n'est rien d'autre que le groupe des classes d'idéaux. De plus, tous les sous-groupes fermés d'indice fini de C_K sont précisément les sous-groupes qui contiennent un sous-groupe de congruence.

Pour L/K une extension finie, on définit l'application $N_{L/K}$ de I_L dans I_K à partir des normes locales $N_{L_\mathfrak{P}/K_\mathfrak{p}}$ de la façon suivante : pour $\alpha = (\alpha_\mathfrak{P})_\mathfrak{P} \in I_L$, on pose $N_{L/K}(\alpha)_\mathfrak{p} = \prod_{\mathfrak{P}/\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha_\mathfrak{P})$. Cette application passe au quotient et induit une application $N_{L/K}$ de C_L dans C_K.

Enfin notons que dans le cas d'extensions galoisiennes, ces groupes sont munis d'une structure de G-modules donnée par la formule $(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_\mathfrak{P}$.

Nous allons à présent rappeler les résultats principaux de la théorie du corps de classes dans le cas des corps de nombres. Toutefois, ils restent tous valables dans le cas des corps de fonctions, comme en atteste le théorème 2.5.1 de [NX01] par exemple.

Théorème 2.1 (Loi de réciprocité d'Artin) *Soit L/K une extension finie galoisienne de corps de nombres, on a un isomorphisme canonique*

$$r_{L/K} : G(L/K)^{ab} \xrightarrow{\sim} C_K / N_{L/K} C_L.$$

Sa réciproque induit un morphisme surjectif

$$(\cdot, L/K) : C_K \to G(L/K)^{ab},$$

appelé symbole d'Artin global.

Armé de ce théorème, on peut décrire toutes les extensions abéliennes de K à partir de la connaissance de C_K et de ses sous-groupes fermés.

Théorème 2.2 *L'application $L \mapsto \mathcal{N}_L = N_{L/K} C_L$ est une bijection décroissante entre les extensions abéliennes finies L/K et les sous-groupes fermés d'indice fini dans C_K. De plus on a $\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ et $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}$.*

Preuve :[Neu99](VI). □

L'extension abélienne correspondant à $\mathfrak{m} = 1$ est appelée le grand corps de classes de Hilbert, et jouit de la propriété suivante :

Définition-Proposition 2.3 *Soit K un corps de nombres. Le grand corps de classes de Hilbert est l'extension abélienne non ramifiée maximale de K. Son groupe de Galois est canoniquement isomorphe à Cl_K.*

Preuve :[Neu99](VI.7.4) □

Etant donné un corps K, on construit $H(K)$ son grand corps de classes de Hilbert. On peut alors recommencer et construire $H(H(K))$. Cette extension ne sera plus abélienne (sauf dans le cas trivial), mais elle sera toujours non ramifiée. Toutefois, il est aisé de montrer qu'elle est galoisienne. On peut continuer ainsi, en espérant que cela ne s'arrête pas, pour obtenir un corps global infini, qui, étant non ramifié à partir du corps K, jouira de bonnes propriétés asymptotiques. Durant des années, le problème de savoir si une telle construction finissait toujours ou non est resté ouvert, jusqu'à ce que les mathématiciens russes Golod et Schafarevitch donnent la réponse à cette question.

Nous allons à présent donner un autre exemple d'extensions abéliennes qui nous sera utile dans la suite. En effet nous allons considérer des extensions non ramifiées en dehors d'un ensemble donné S et pour cela nous aurons besoin de quelques nouvelles définitions et quelques résultats.

Soit S un ensemble de places de K contenant l'ensemble S_∞ des places infinies. On notera $\mathcal{O}_{K,S}$ l'anneau des S-entiers de K (on impose aux éléments de $a \in K$ la condition $v_\mathfrak{p}(a) \geq 0$ si $\mathfrak{p} \notin S$). Soit $I_{K,S}$ le groupe des S-idèles défini par le produit restreint :

$$I_{K,S} := \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\times$$

et posons $C_{K,S} := I_{K,S}/\mathcal{O}_{K,S}^{\times}$. Considérons le sous-groupe compact

$$U_{K,S} := \prod_{\mathfrak{p}\in S}\{1\} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

de I_K, et enfin le groupe des classes de S-idèles

$$C_S(K) = C_K/U_{K,S}.$$

$C_{K,S}$ est un sous-groupe ouvert de $C_S(K)$ (groupe qui a l'intérêt d'être bon pour la descente galoisienne) et ils sont liés par la suite exacte suivante

$$0 \longrightarrow C_{K,S} \longrightarrow C_S(K) \longrightarrow Cl_S(K) \longrightarrow 0,$$

la première flèche étant induite par l'homomorphisme naturel $I_{K,S} \to C_S(K)$.

Pour comprendre quelles sont les extensions ainsi considérées, nous allons faire appel à des résultats prédisant le comportement des places si on connaît le sous-groupe de C_K correspondant.

Théorème 2.4 *Soit K/k une extension abélienne de corps de nombres. Soit v une place finie de k. Alors l'application d'Artin envoie k_v^* sur G_v (où $G_v = G_{w/v}$ est le groupe de décomposition de $w|v$), a pour noyau $\mathrm{N}_w K_w^*$ et induit donc l'isomorphisme $k_v^*/\mathrm{N}_w K_w^* \to G_v$, où N_w est l'application de norme locale de K_w/k_v.*

Preuve : On se reportera à [Lan94](IX,theorem 3) □

On en déduit alors :

Corollaire 2.5 *Soit H le sous-groupe de I_k^* contenant k^* représentant K. Alors v se décompose totalement dans K/k si et seulement si $k_v^* \subset H$.*

Enfin on a également le résultat suivant qui nous permet de savoir quelles places sont non ramifiées :

Théorème 2.6 *Avec les notations précédentes, v est non ramifiée dans K/k si seulement si $U_v \subset H$. Plus généralement, $(U_v, K/k) = I_v$, où I_v est le groupe d'inertie de $w|v$ pour tout $w|v$.*

Preuve : [Lan94](IX, theorem 4) □

Supposons que S est un ensemble fini. D'après la théorie du corps de classes, $U_{K,S}$ correspond à l'extension maximale abélienne de K non ramifiée hors de l'ensemble S. Son groupe de Galois est donc $C_S(K)$. $I_{K,S}U_{K,S}K^{\times}$ correspond à une autre extension abélienne de K, cette fois l'extension maximale non ramifiée de K où les places de S sont totalement décomposées. D'après la suite exacte précédente, le groupe de Galois de cette extension abélienne est $Cl_S(K)$.

2.2.2 Critère de Golod-Schafarevitch

En 1964 ces deux mathématiciens russes créèrent la surprise en prouvant que la p-extension maximale non ramifiée d'un corps de nombres n'était pas nécessairement finie, répondant ainsi au problème des tours de corps de classes. Nous allons rappeler l'argument de théorie des groupes qui conduit à ce résultat. On peut trouver plusieurs preuves de ce résultat, notamment dans [Ser94] ou [Koc02], mais nous suivrons [NSW00] (III,9).

Rappelons d'abord quelques définitions et résultats concernant les générateurs et relations d'un p-groupe. Soit G un pro-p-groupe, c'est à dire la limite projective de p-groupes. G est muni d'une structure de groupe topologique héritée de la limite projective, pour laquelle il est compact et totalement déconnecté.

Considérons $H^n(G) = H^n(G, \mathbb{Z}/p\mathbb{Z})$ le $n^{\text{ième}}$ groupe de cohomologie de G à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, vu comme un $\mathbb{F}_p$-espace vectoriel.

Un système de générateurs de G est un sous-ensemble $S \subset G$ convergent (vers 1, c'est à dire que tous les sous-groupes ouverts de G contient presque tous ses éléments) qui génère G comme groupe topologique. Un système de générateurs sera dit minimal s'il ne contient pas de sous-ensemble qui soit un système de générateurs de G. Le rang de G est par définition le minimum des cardinaux des systèmes de générateurs et sera noté $d(G)$. On peut montrer [NSW00](3.9.1) que tout système de générateurs minimal a même cardinal et on a même l'égalité

$$d(G) = \dim H^1(G).$$

Ainsi si $H^1(G)$ est fini, G est engendré par un nombre fini d'éléments.

Soit S un système de générateurs de G et soit F le pro-p-groupe libre sur S, c'est à dire que F est l'unique pro-p-groupe muni de l'application $i : S \to F$ vérifiant les conditions suivantes : tout sous-groupe ouvert contient presque tous les éléments de $i(S)$, et si $j : S \to H$ est une autre application jouissant de la première propriété dans un pro-p-groupe H, il existe un unique morphisme $f : F \to H$ tel que $j = f \circ i$. On a alors la suite exacte :

$$1 \longrightarrow R \longrightarrow F \xrightarrow{f} G \longrightarrow 1.$$

Un système de relations (par rapport à S) est alors un système de générateurs $\mathcal{R}$ de R en tant que sous-groupe normal de F. Dans le cas où G est engendré par un nombre fini d'éléments, un système de relations fini $\mathcal{R}$ existe si et seulement si $H^2(G)$ est fini, et dans ce cas on a l'égalité

$$\mathrm{card} S - \mathrm{card} \mathcal{R} = \dim H^1(G) - \dim H^2(G),$$

qui provient directement de la suite exacte à cinq termes. Si S est minimal, $\mathcal{R}$ est également minimal, son cardinal est indépendant de S et on posera alors $r(G) = \mathrm{card}\mathcal{R}$. On a donc

$$r(G) = \dim H^2(G).$$

En particulier, G est un pro-p-groupe libre si la dimension cohomologique de G est plus petite que 1. On peut alors énoncer le théorème de Golod-Schavarevitch (en fait un résultat un peu plus fort du à Gaschütz et Vinberg [Vin65] indépendamment).

Théorème 2.7 *Si G est un p-groupe fini, alors*

$$r(G) > \frac{1}{4} d(G)^2.$$

Autrement dit, si $\dim H^2(G) \leq \frac{1}{4}(\dim H^1(G))^2$, alors G est infini.

2.2.3 Application aux tours non ramifiées de corps de nombres

Nous allons à présent étudier ce qu'on appelle les tours de corps de classes qui fournissent un exemple de tours non ramifiées de corps de nombres, et par conséquent des tours asymptotiquement bonnes. En fait, nous ne considérerons que les p-tours de corps de classes. En effet, le critère de Golod-Schafarevitch ne donne d'information que sur la finitude de p-extensions, et le problème reste ouvert quant à l'existence d'autres tours (mêlant p et q par exemple). Ce n'est malheureusement pas une méthode de construction explicite comme il en existe dans le cas des corps de fonctions (voir [GS96]).

Considérons la tour suivante : partons d'un corps global $K = K_0$, d'un ensemble de places S et supposons le corps K_{i-1} construit. On prend alors pour K_i le corps de classes défini par le p-Sylow du groupe $Cl_{S_{i-1}}(K_{i-1})$ où S_{i-1} est l'ensemble des places au-dessus de S. Alors K_i est une extension galoisienne de K_0. En effet, supposons que K_{i-1}/K_0 soit galoisienne, et montrons que K_i l'est en considérant un morphisme σ de K_i dans une clôture séparable de K_0. Par hypothèse, $\sigma(K_{i-1}) = K_{i-1}$ et ainsi $\sigma(K_i)$ est une extension abélienne de K_{i-1} non ramifiée où les places au-dessus de S sont totalement décomposées, et ainsi $\sigma(K_i) = K_i$ et K_i est bien galoisienne. Bien sûr, un tel raisonnement tient également pour la tour d'extension T-ramifiée, S-décomposée. Notons enfin L l'union de tous ces corps K_i. S est ainsi totalement décomposé dans L.

Bien que la plupart des résultats valables pour les corps de nombres sont adaptables aux corps de fonctions, la présence des places archimédiennes dans le cas de corps de nombres rend les situations un peu différentes. Nous allons donc traiter les deux cas l'un après l'autre.

Dans le cas des corps de nombres, le critère de Golod-Schafarevitch s'exprime ainsi :

Lemme 2.8 *Soit K un corps de nombres. Si*

$$\dim_p Cl_S(K)/p \geq 2 + 2\sqrt{\dim_p \mathcal{O}_{K,S}^*/p + 1},$$

alors L est infinie.

Preuve du lemme: [TV02](lemma 9.1) Ici intervient le critère de Golod-Schafarevitch. Notons également que $\dim_p \mathrm{Cl}_S(K)/p$ n'est rien d'autre que $h^1(G(K_1/K))$ d'après la théorie du corps de classes. ■

De plus, d'après [TV02](lemma 9.2) le p-rang de $\mathcal{O}_{K,S}^*$ est $r_1 + r_2 + \delta_p - 1 + |S|$, où δ_p vaut 1 si K contient les racines $p^{\text{ièmes}}$ de l'unité, 0 sinon.

On en déduit alors [TV02](theorem 9.1) :

Théorème 2.9 *Soit k un corps de nombres. Soit $P = \{p_1, ..., p_n\}$ et $Q = \{q_1, ..., q_r\}$ deux ensembles disjoints de places finies de k et soit t_0 le nombre d'idéaux principaux dans P. Considérons un corps de nombres K/k de degré premier ℓ, ramifié exactement en Q. Soit S l'ensemble des idéaux premiers au-dessus de P, $s = |S|$. Supposons :*

$$r \geq s - t_0 + r_1 + r_2 + \delta_\ell + 2 - \rho + 2\sqrt{\ell(r_1 + r_2 - \rho/2) + \delta_\ell + s},$$

où δ_ℓ vaut 1 si K contient les racines $\ell^{\text{ième}}$ de l'unité, 0 sinon, et ρ est le nombre de places réelles qui se ramifient dans K. Alors K admet une ℓ-tour non ramifiée infinie de corps de classes, où S se décompose totalement.

On en déduit le corollaire suivant qui nous sera utile lorsqu'on voudra construire des corps globaux infinis asymptotiquement bons.

Corollaire 2.10 *i. Supposons que $K/\mathbb{Q}$ soit complexe (resp. réel) et quadratique, et que K soit ramifié en exactement r idéaux premiers. Si $r \geq 6$ (resp. $r \geq 8$), K admet une 2-tour non ramifiée infinie. Si de plus $r \geq 8$ (resp. $r \geq 10$), et p un premier non ramifié dans K, alors K admet une 2-tour non ramifiée où toutes les places au-dessus de p sont totalement décomposées.*

ii. Supposons que $K/\mathbb{Q}$ soit une extension cyclique de degré impair ℓ, ramifiée en exactement r premiers. Si $r \geq 3+\ell+2\sqrt{2+\ell^2}$, alors, pour tout premier p de $\mathbb{Z}$ non ramifié, K admet une tour de corps de classes non ramifiée où tous les premiers au-dessus de p dans $\mathcal{O}_K$ sont totalement décomposés.

Preuve : On applique simplement le théorème précédent. □

A l'aide du théorème précédent, nous pouvons également construire une 2-tour de corps de nombres où n places arbitraires de $\mathbb{Q}$ sont totalement décomposées. Considérons $P = \{p_1, ..., p_n\}$ cet ensemble. Comme ensemble Q nous prendrons r nombres premiers $(q_1, ..., q_r)$ différents des $p_1, ..., p_{n_0}$ afin de vérifier le théorème avec $s = 2n$. La première étape consiste à construire le corps K_0, extension quadratique de $\mathbb{Q}$ où toutes les places de P sont totalement décomposées et ramifiées au moins en Q. Bien qu'une construction explicite soit possible (cf paragraphe 2.4), nous allons ici utiliser le théorème de Grunwald-Wang.

Dans le cas des corps de fonctions, il faut faire attention au fait que l'extension obtenue dans la tour de Golod-Schafarevitch peut contenir des extensions des constantes, ce qui est exclu dans notre étude.

Rappelons le critère de Golod-Schafarevitch comme on peut le trouver dans [Ser85] : Soit C une courbe de genre g, définie sur $\mathbb{F}_r$. Soit K son corps de fonctions, et ℓ un nombre premier. Soit S un ensemble non vide de points fermés de C (i.e. d'idéaux maximaux de $\mathcal{O}_K$). On considère de même la tour de corps de classes K_i. Si ℓ ne divise pas le *pgcd* des degrés des places de S, il n'y a pas d'extension des constantes, et autrement il y en a.

Théorème 2.11 *Soit K un corps de fonctions et S un ensemble de places de K. Supposons que $d := d_\ell Cl_S \geq 2$ et que*

$$|S| \leq \frac{d^2}{4} - d + \varepsilon,$$

où $\varepsilon = 1$ si $\ell \,|\, r-1$, 0 sinon. Alors K admet une ℓ-tour de corps de classes non ramifiée où les places de S sont totalement décomposées.

Pour estimer d, on peut faire appel à un résultat de Xing et Niedereiter, corrigé par Serre, présent dans [NX98] :

Proposition 2.12 *Soit K/k une extension abélienne finie de corps de fonctions, soit S un ensemble fini de places de k et $S(K)$ les places au-dessus de S dans K. Supposons que le pgcd des degrés des places contenues dans S vaut 1. Alors, pour tout premier ℓ,*

$$d_\ell Cl_{S(K)} \geq \sum_P d_\ell I_P - (s-\varepsilon) - d_\ell G,$$

où $s = \#S$, $G = Gal(K/k)$, où la somme est prise sur toutes les places P de k et I_P est le groupe d'inertie de la place P de k dans K/k.

Le corollaire suivant, qui est l'analogue du théorème de Tsfasman-Vlăduţ dans le cas des corps de nombres, s'ensuit directement :

Corollaire 2.13 *Soit K/k une extension abélienne de corps de fonctions, de groupe de galois G, ramifiée en un ensemble Q de cardinal r. Soit S_k un ensemble fini de places de k, et S_K l'ensemble des places au-dessus de S_k dans K. Supposons que le pgcd des degrés des places de S_K vaut 1. Notons $s = \#S_k$ et $S = \#S_K$. Soit ℓ un nombre premier, et supposons que*

$$\sum_{P \in Q} d_\ell I_P \geq s - \varepsilon + 2 + d_\ell G + 2\sqrt{S + 1 - \varepsilon}.$$

Alors K admet une $\ell-$tour de corps de classes non ramifiée où les places de S_K sont totalement décomposées. En particulier, si K/k est cyclique de degré ℓ, la condition se réécrit :

$$r \geq s + 3 - \varepsilon + 2\sqrt{S + 1 - \varepsilon}.$$

Preuve : La condition du théorème 2.11 se reformule ainsi : $d \geq 2 + 2\sqrt{S + 1 - \varepsilon}$. Celle du corollaire ainsi que la minoration pour d de la proposition nous assure que d la vérifie, et on peut donc appliquer le théorème précédent. □

Nous connaissons donc à présent des moyens de construire des corps globaux infinis asymptotiquement bons dans le cas des corps de fonctions et des corps de nombres, à condition de savoir construire la première extension cyclique. On peut ou bien la construire explicitement, ou bien, puisque notre tour ne sera elle-même pas explicite, utiliser le théorème de Grunwald-Wang pour y parvenir, ce que nous allons étudier dans le paragraphe suivant.

2.2.4 Théorème de Grunwald-Wang et applications

Le théorème de Grunwald, établi dans les années 1930, affirme l'existence d'une extension cyclique globale réalisant un nombre fini d'extensions locales données. En 1948, Wang se rendit compte que le théorème de Grunwald était faux en toute généralité en proposant un contre-exemple, et finalement donna la forme exacte du théorème de Grunwald. Par la suite, en considérant ce résultat sous l'approche plus générale des problèmes de plongements dans les corps globaux, Neukirch [Neu73] compléta le théorème de Grunwald-Wang pour les groupes nilpotents finis.

Considérons k un corps global et S un ensemble de places non vide de k contenant les places archimédiennes dans le cas des corps de nombres. On notera $G_S(k)$ (ou plus simplement G_S si aucune confusion n'est possible) le groupe de Galois de l'extension maximale k_S de k non ramifiée hors de S, et

$$\mathbb{N}(S) = \{n \in \mathbb{N} \mid v_\mathfrak{p}(n) = 0 \text{ pour tout } \mathfrak{p} \notin S\}.$$

Soit T un ensemble fini contenu dans S, et A un $G_S(k)$-module fini tel que $\#A \in \mathbb{N}(S)$. Pour tout $\mathfrak{p} \in S$, on choisit un k-plongement de $k_S \to \bar{k}_\mathfrak{p}$ par le choix d'une place $\bar{\mathfrak{p}}$ de k_S au-dessus de $\mathfrak{p}$. Cela induit une application de restriction $G(\bar{k}_\mathfrak{p}/k_\mathfrak{p})$ dans $G_S = G(k_S/k)$ dont l'image est le groupe de décomposition de $\bar{\mathfrak{p}}$ sur k. A son tour elle induit un homomorphisme

$$H^i(G_S, A) \to H^i(G(\bar{k}_{\mathfrak{p}}/k_{\mathfrak{p}}), A)$$

indépendant du choix du plongement. On s'intéresse alors au conoyau de l'application de restriction :

$$H^1(k_S|k, A) \xrightarrow{res} \prod_T H^1(\bar{k}_{\mathfrak{p}}|k_{\mathfrak{p}}, A) \twoheadrightarrow \mathrm{coker}(k_S, T, A).$$

Le problème de l'étude du noyau est le problème de la réalisation du principe de Hasse. Dans notre problème, c'est la surjectivité de cette application qui est importante. Toutefois, ces deux questions sont très liées par des considérations de dualité, c'est pourquoi les résultats dont nous avons besoin se déduisent des résultats correspondant dans le problème du principe de Hasse.

Définissons le cas spécial (k, m, T) comme le cas où le principe de Hasse pour le $G_S(k)$-module $A = \mu_m$ et les places $T \subset S$ n'est pas vérifié (voir [NSW00](9.13) : le groupe de Schafarevitch valant alors $\mathbb{Z}/2\mathbb{Z}$). Ce cas spécial correspond à la situation où toutes les conditions suivantes sont vérifiées :

i. $m = 2^r m', \quad r > 2$
ii. k est un corps de nombres
iii. $k(\mu_{2^r})/k$ n'est pas cyclique
iv. $\{\mathfrak{p} \in S \ \mid \mathfrak{p}/2$ et $\mathfrak{p}$ n'est pas totalement décomposé dans $k(\mu_{2^r})/k\} \subset T$.

Ici nous n'aurons pas besoin d'utiliser des extensions d'exposant divisible par 8 et ainsi nous éviterons ce cas.

Définissons à présent ce que nous appelons la densité de Dirichlet d'un ensemble de places. Pour R un ensemble de places de K, et $s > 1$ on pose

$$\delta_R(s) = \frac{\sum_{\mathfrak{p} \in R} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in P(K)} \mathrm{N}(\mathfrak{p})^{-s}}.$$

On définit sa densité de Dirichlet, si elle existe, comme

$$\delta(R) = \lim_{s \to 1^+} \delta_R(s).$$

Si elle n'existe pas, on pose alors

$$\bar{\delta}(R) = \limsup_{s \to 1^+} \delta_R(s).$$

Rappelons le théorème de Grunwald-Wang classique, puis démontrons une version un tout petit peu plus générale de ce résultat en s'appuyant sur des résultats de [NSW00].

Théorème 2.14 *(Grunwald-Wang)[NSW00](9.2.3) Soit T un ensemble fini de places d'un corps global k et soit A un groupe abélien fini. Soient $K_{\mathfrak{p}}/k_{\mathfrak{p}}$, pour $\mathfrak{p} \in T$ des extensions abéliennes locales telles que $G(K_{\mathfrak{p}}/k_{\mathfrak{p}})$ peut être plongé dans A. Alors il existe une extension abélienne K/k de groupe de Galois A telle que K a les complétions $K_{\mathfrak{p}}$ pour tout $\mathfrak{p} \in T$, à part dans le cas spécial $(k, exp(A), T)$, où $exp(A)$ est l'exposant de A.*

Utilisons ce théorème pour construire un corps global infini asymptotiquement bon où un ensemble fini de places finies donné du corps de base est totalement décomposé.

Corollaire 2.15 *Soit P un ensemble fini de places finies de $\mathbb{Q}$ (resp. de $\mathbb{F}_r(t)$, contenant au moins une place rationnelle). Alors il existe un corps de nombres infini (resp. un corps de fonctions infini) asymptotiquement bon tel que toutes les places de P sont totalement décomposées.*

Preuve : soit Q un ensemble de places finies de $\mathbb{Q}$ (resp. de $\mathbb{F}_r(t)$) tel que $P \cap Q = \emptyset$, et $\#Q$ suffisamment grand pour vérifier les hypothèses de 2.9 (resp. 2.13 dans le cas des corps de fonctions). Appliquant ce théorème à $A = \mathbb{Z}/2\mathbb{Z}$, $T = P \cup Q$, on obtient une extension cyclique de degré 2 de $\mathbb{Q}$ (resp. de $\mathbb{F}_r(t)$) où l'ensemble Q, au moins, est totalement ramifié, et tel que l'ensemble P est totalement décomposé. Notons qu'on obtient les 2-extensions locales séparables totalement ramifiées par des polynômes d'Eisenstein séparables par exemple. On utilise alors le théorème 2.9 (resp. 2.13) afin d'obtenir une 2-tour de corps de classes où toutes les places de P sont totalement décomposées, que l'on notera $\mathcal{K} = \cup_{i \geq 0} K_i$. Dans le cas des corps de fonctions, tous les corps de cette tour ainsi construite ont bien pour corps de constantes $\mathbb{F}_r$ puisque P contient une place rationnelle. Le corps global infini $\mathcal{K}$ est asymptotiquement bon car non ramifié hors d'un ensemble fini de places, et toutes les places de P y sont totalement décomposées. $\square$

Nous allons voir que nous pouvons renforcer légèrement ce théorème, ce dont nous aurons besoin dans la construction d'un exemple de corps global infini dont la ramification a une densité nulle. Donnons alors le théorème dont on va déduire notre version de Grunwald-Wang.

Théorème 2.16 *Soit S un ensemble non vide de places d'un corps global k contenant les places archimédiennes dans le cas des corps de nombres, et T un sous-ensemble fini de S. Soit A un G_S-module fini avec $\#A \in \mathbb{N}(S)$. Alors coker(k_S, T, A) est trivial dans le cas où A est un G_S-module trivial, où le lieu de décomposition de $k(\mu_{p^r})|k$ est contenu dans S à un ensemble de densité de Dirichlet nulle près pour tout $p^r|\#A$ et où on n'est pas de le cas spécial $(k, exp(A), T)$.*

Preuve : On se reportera à [NSW00](9.2.2) pour la preuve de ce résultat. $\square$

Corollaire 2.17 *Soit S un ensemble de places d'un corps global k tel que $\delta(S) = 1$, contenant les places archimédiennes dans le cas des corps de nombres, $T \subset S$ un ensemble fini de places de k et soit A un groupe abélien fini tel que $\#A \in \mathbb{N}(S)$. Soit $K_\mathfrak{p}/k_\mathfrak{p}$, pour $\mathfrak{p} \in T$ des extensions abéliennes locales telles que $G(K_\mathfrak{p}/k_\mathfrak{p})$ peut être plongé dans A. Alors il existe une extension abélienne K/k de groupe de Galois A non ramifiée hors de S telle que K a les complétions $K_\mathfrak{p}$ pour tout $\mathfrak{p} \in T$, à part dans le cas spécial $(k, exp(A), T)$.*

Preuve : Il s'agit de l'adaptation de la preuve du théorème 9.2.2. de [NSW00]. On va appliquer le théorème au G_S-module trivial A. On veut montrer que l'application canonique

$$\mathrm{Epi}(G_S, A) \to \prod_T \mathrm{Hom}(G(\bar{k}_\mathfrak{p}/k_\mathfrak{p}), A)$$

est surjective (où $\mathrm{Epi}(G_S, A)$ désigne l'ensemble des homomorphismes surjectifs de G_S dans A). Soient $\mathfrak{q}_1, ..., \mathfrak{q}_r$ des places finies dans $S - T$ ne divisant pas 2 dans le cas des corps de nombres (de sorte que ces places ne nous fassent pas tomber dans le cas spécial) et soient des homomorphismes

$$\psi_{\mathfrak{q}_i} : G(\bar{k}_{\mathfrak{q}_i}/k_{\mathfrak{q}_i}) \to A$$

tels que les images des $\psi_{\mathfrak{q}_i}$ engendrent A. Pour tout $\mathfrak{p} \in T$, $\psi_{\mathfrak{p}} : G(\bar{k}_{\mathfrak{p}}/k_{\mathfrak{p}}) \to A$ désignera l'application canonique induite par un plongement $G(K_{\mathfrak{p}}/k_{\mathfrak{p}}) \to A$. Notons enfin T' l'ensemble $T \cup \{\mathfrak{q}_1, ..., \mathfrak{q}_r\}$. D'après le théorème, l'application

$$H^1(k_S|k, A) \to \prod_{T'} H^1(\bar{k}_{\mathfrak{p}}|k_{\mathfrak{p}}, A)$$

est surjective sauf dans le cas spécial $(k, exp(A), T') = (k, exp(A), T)$. Mais alors un antécédent $\psi : G_S \to A$ de $(\psi_{\mathfrak{p}}, \mathfrak{p} \in T')$ dans $H^1(G_S, A) = \mathrm{Hom}(G_S, A)$ (car A est un G_S-module trivial) réalise les extensions locales et est surjectif d'après le choix des $\psi_{\mathfrak{q}_i}$. □

Terminons ce paragraphe par une remarque complémentaire.

> **Remarque:** Suivant les applications que l'on a en tête, il existe des versions plus fortes, et surtout explicites de ce résultat. Par exemple, dans le cas des extensions cycliques de degré p^e, on trouvera dans [Gra05] (chapitre 5), des conditions sur l'ensemble S, ne dépendant que de T, e, K et p, pour l'existence d'une p^e-extension de K S-totalement ramifiée, T-décomposée (également non ramifiée hors de S.). Il démontre alors le résultat suivant :
>
> **Proposition 2.18** *Soit K un corps de nombres, p un nombre premier, e un entier naturel non nul, T et S deux ensembles disjoints de places, telles que pour tout $\mathfrak{q} \in S$, $\mathrm{N}\mathfrak{q} = 1 \, mod p^e$. Alors il existe une infinité de places s telles qu'il existe une extension de K, T-décomposée, S ou $S \cup s$-totalement ramifiée, cyclique de degré p^e, sauf dans le cas spécial.*
>
> De plus, en étudiant la preuve de ce résultat, on s'aperçoit qu'on peut également choisir s dans un ensemble de densité égale à 1. Ce résultat trouve également son intérêt dans le fait qu'on peut demander la ramification d'une seule place, dont on peut essayer d'estimer la norme, et ainsi tenter de construire, au moyen de nos résultats, une tour presque-galoisienne asymptotiquement bonne où une infinité de places se ramifient. Malheureusement, les estimations naïves que nous connaissons ne semblent pas suffisantes.

2.3 Application à l'ensemble Φ

Nous pouvons à présent démontrer un théorème qui nous donne quelques indications concernant l'ensemble Φ. On complète ainsi le résultat déduit du théorème de Tsfasman-Vlăduţ qui affirme qu'il existe un corps global infini dont n invariants sont non-nuls. En fait, on peut même choisir ceux qui sont positifs parmi tous les invariants possibles :

Théorème 2.19 *Soit n éléments $t_1, ..., t_n \in A_f$. Alors Il existe un corps global infini ((NF) et (FF)) tel que $\phi_{t_1}, ..., \phi_{t_n}$ sont tous > 0, et tel que, dans le cas des corps de nombres les autres ϕ_q, tels que q n'est pas premier à $\prod t_i$ soient nuls.*

Dans le cas des corps de fonctions, on applique le corollaire 2.15 avec un ensemble de places P contenant des places de degré $\log_r t_i$ pour tout $i = 1, ..., n$, ce qui donne directement le résultat. On peut aussi l'obtenir en partant d'une seule place et en raisonnant comme dans le cas des corps de nombres, en faisant toutefois attention à éviter les extensions du corps des constantes.

Dans le cas des corps de nombres, on considère l'ensemble $P = \{p^{(1)}, \ldots, p^{(k)}\}$ des nombres premiers $p^{(1)}, \ldots, p^{(k)}$ qui divisent un des t_i. Nous allons construire une autre extension qui devra avoir la propriété d'avoir des places de norme t_i pour chaque t_i et aucune autre de norme divisible par les éléments de P (propriété $\star$). Pour y parvenir, nous allons avoir besoin du théorème de Grunwald-Wang. Ensuite nous prendrons le compositum avec la tour construite dans le corollaire 2.15 pour arriver à nos fins.

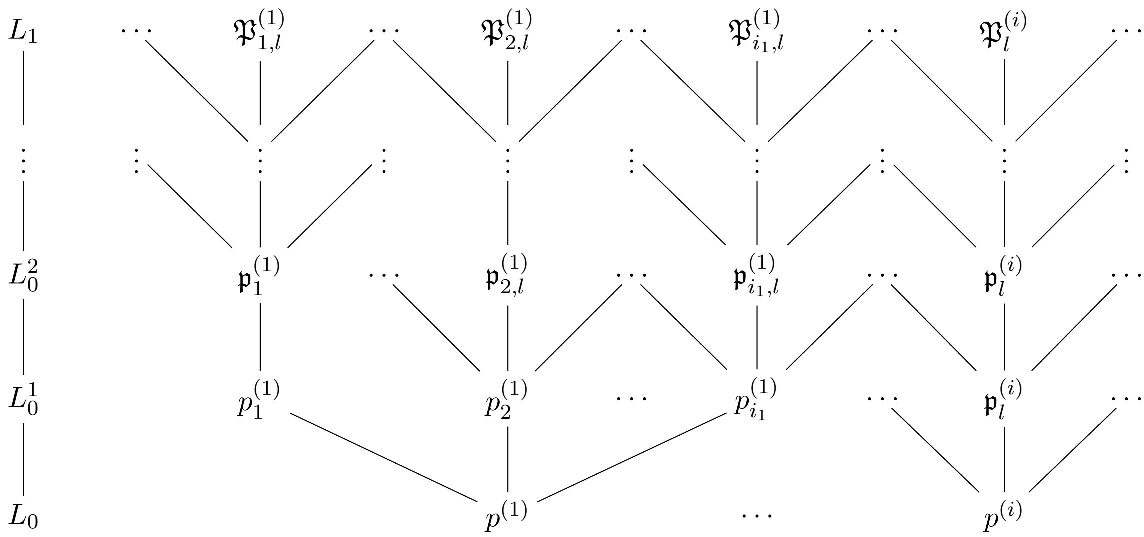
Lemme 2.20 *Il existe une extension L de $\mathbb{Q}$ possédant la propriété $\star$.*

Preuve du lemme: Nous allons construire une tour finie $L_0 = \mathbb{Q}, L_1, ..., L_k = L$ à l'aide du théorème de Grunwald-Wang. Commençons par ordonner l'ensemble T. On écrit

$$T = \left\{t_1^{(1)}, ..., t_{i_1}^{(1)}; t_1^{(2)}, ..., t_{i_2}^{(2)}; t_1^{(k)}, ..., t_{i_k}^{(k)}\right\}$$

en fonction de l'entier premier qui les divise. Notons $d_j^{(r)} = \log_{p^{(r)}} t_j^{(r)}$.

Représentons les extensions de corps intervenant et les places de ceux-ci. L'indice l sera un indice générique, et plusieurs traits partant d'une place signifient qu'elle est totalement décomposée, tandis qu'un seul signifie qu'elle est inerte.



Rappelons d'abord la propriété suivante des corps locaux qui garantit qu'on peut utiliser le théorème de Grunwald-Wang de la façon suivante (voir [Ser68],§III.5, théorème 2 pour un théorème plus fort).

Lemme 2.21 *Soit K un corps local de corps résiduel fini k, et k'/k une extension cyclique de k. Alors il existe une extension cyclique non ramifiée K'/K de corps résiduel k'.*

Ainsi, étant donné un corps global K, une place finie $\mathfrak{p}$, la complétion $K_\mathfrak{p}$ de K en $\mathfrak{p}$, un entier $n > 0$, il existe une extension cyclique non ramifiée K' de $K_\mathfrak{p}$, de degré n, c'est à dire où $\mathfrak{p}$ est totalement inerte.

Construisons par récurrence une tour $L_0 \subset \cdots \subset L_k$ à l'aide du théorème de Grunwald-Wang ayant les propriétés suivantes :

i. dans L_{r+1}/L_r, toutes les places au-dessus de $p^{(j)}$ sont totalement décomposées pour $j \neq r+1$,

ii. il existe $L_r \subset L_r^1 \subset L_{r+1}$ de degré i_{r+1} telle que toutes les places au-dessus de $p^{(r+1)}$ sont totalement décomposées,

iii. dans L_{r+1}/L_r^1 il y a $[L_{r+1} : L_0]/(i_{r+1} d_j^{(r+1)})$ places de norme $t_j^{(r+1)}$ pour tout j (et ainsi aucun autre Φ_q non nul).

L_0 est déjà construite. Supposons L_r/L_0 formée. Notons $m_r = [L_r : L_0]$. Soit L_r^1 une extension de L_r de degré i_{r+1} où toutes les places au-dessus des $p^{(i)}$ sont totalement décomposées. Dans L_r^1 on a alors $i_{r+1} m_r$ places $p_{1,1}^{(r+1)}, \dots, p_{1,m_r}^{(r+1)}, \dots, p_{i_{r+1},1}^{(r+1)}, \dots, p_{i_{r+1},m_r}^{(r+1)}$ au-dessus de $p^{(r+1)}$, groupées en i_{r+1} paquets de m_r places. On considère alors des extensions cycliques successives de degré premier (pour éviter de prendre des extensions de degré 4) de sorte d'obtenir une extension L_{r+1}/L_r^1 telle que :

i. toutes les places au-dessus des $p^{(i)}$ soient totalement décomposées pour $i \neq r+1$,

ii. au-dessus de $p_{j,l}^{(r+1)}$, pour tout j et tout l, il y a $[L_{r+1}/L_r^1]/d_j^{(1)}$ places de norme $t_j^{(r+1)}$.

Pour traiter le $j^{\text{ème}}$ paquet, on demande l'existence d'extensions cycliques de degré premier divisant $t_j^{(r+1)}$, où les places au-dessus des $p_{j,l}^{(r+1)}$ sont totalement inertes pour tout l, et où toutes les autres places pointées sont totalement décomposées, jusqu'à obtenir des places de norme $t_j^{(r+1)}$.

Par récurrence, on obtient alors $L_k = L$, et ce corps vérifie bien la propriété $(\star)$. ■

Il suffit alors de former le compositum de ce corps avec une tour (K_i) asymptotiquement bonne dans laquelle les places de P sont totalement décomposées, construite dans le corollaire 2.15. D'après les résultats du premier chapitre, ce corps global convient. En effet, toutes les places au-dessus de P sont totalement décomposées dans la tour (LK_i). □

> **Remarque:** On peut donner une propriété analogue dans le cas des corps de fonctions à la propriété additionnelle (et gratuite) qu'on a dans le cas des corps de nombres. Si au lieu de calculer Φ_q on calcule $\Phi_{R,q}$ le nombre de places de norme q au-dessus d'une place donnée R, on peut alors montrer un théorème analogue : il existe une place rationnelle R telle que $\phi_{R,q} > 0$ pour $q \in T$ et $\phi_{R,q} = 0$ pour $q \notin T$.

2.4 Limites de la théorie du corps de classes

La théorie du corps de classes nous prédit l'existence d'une tour non ramifiée, ainsi que la décomposition dans la tour d'un nombre fini de places arbitraires, que l'on paie par la ramification au premier étage de la tour. Mais comme nous allons le voir, cette technique s'avère inefficace dès que l'on veut utiliser cela pour un nombre de plus en plus grand de places qui se décomposent dans la tour, car on ne peut borner son défaut que par quelque chose de proche de 1.

Pour tout $n \in \mathbb{N}$, appliquant la construction des tours de corps de classes, on sait qu'il existe un corps global infini ayant n invariants ϕ_n non nuls et dont l'erreur est au plus δ_n. L'objectif est d'estimer asymptotiquement δ_n.

On définit le défaut d'une tour dans deux cas, avec GRH (1) et sans GRH (2) par

$$(1) \quad \delta_n = 1 - \sum_q \phi_q \frac{\log q}{\sqrt{q} - 1} - (\gamma + \log 8\pi)\phi_{\mathbb{C}} - (\gamma/2 + \pi/4 + \log \sqrt{8\pi})\phi_{\mathbb{R}},$$

$$(2) \quad \delta_n = 1 - \sum_q \phi_q \frac{\log q}{q - 1} - (\gamma + \log 2\pi)\phi_{\mathbb{C}} - (\gamma/2 + \log 2\sqrt{\pi})\phi_{\mathbb{R}}.$$

Remarque:

i. Le problème est d'optimiser les invariants ϕ_q que nous recherchons. Pour cela il s'agit donc de trouver une tour dont le genre n'est pas trop gros par rapport au degré et dont n places au moins se décomposent totalement de préférence.

ii. Les constructions que nous connaissons de corps globaux infinis sont telles que lorsque n augmente, le genre du corps augmente aussi.

iii. Contrairement au cas borné, les facteurs archimédiens n'auront pas de contribution puisque le genre du premier corps de la tour tend vers l'infini.

Rappelons le théorème qui permet de construire une tour de corps de classes ayant n invariants non nuls, et dont on pourra estimer le défaut.

Théorème 2.22 *Soit $P = \{p_1, ..., p_n\}$ et $Q = \{q_1, ..., q_r\}$ deux ensembles disjoints de nombres premiers. Considérons un corps de nombres $K/\mathbb{Q}$ de degré premier ℓ, ramifié exactement en Q. Soit S l'ensemble des idéaux premiers au-dessus de P, $s = \#S$. Supposons :*

$$r \geq s - n + r_1 + r_2 + \delta_\ell + 2 - \rho + 2\sqrt{\ell(r_1 + r_2 - \rho/2) + \delta_\ell + s},$$

où δ_ℓ vaut 1 si K contient les racines $\ell^{\text{ième}}$ de l'unité, 0 sinon, et ρ est le nombre de places réelles qui se ramifient dans K. Alors K admet une ℓ-tour non ramifiée infinie de corps de classes, où S se décompose totalement.

Prenons pour ensemble P les n nombres premiers qui suivent 2 : $P = \{3, 5, 7, ..., p_n\}$ Nous allons considérer pour K une extension quadratique, $\mathbb{Q}(\sqrt{q_1 ... q_{r_n} r})$, où r_n est le plus petit entier vérifiant assurément la condition du théorème avec $s = 2n$:

$$r_n = 1 + E(n + 5 + 2\sqrt{2n + 4 + 1}).$$

On a alors $r_n = n + 2\sqrt{2n} + reste_n$ où $reste_n$ est une fonction bornée avec n.

> **Remarque:** En prenant un corps quadratique imaginaire, on peut légèrement abaisser le nombre r_n, mais asymptotiquement, c'est la même chose.

On va choisir r avec attention. On veut s'assurer que les p_i soient décomposées (sinon elles peuvent être inertes et on perd un facteur $\sqrt{n}$). On prend pour q_i, pour $i \leq r_n$, les r_n premiers qui suivent p_n, mais on va prendre r de telle sorte que les p_i se décomposent de la façon suivante.

Proposition 2.23 *Il existe $r \in \{0, ..., 2\prod p_i \prod q_j - 1\}$ premier à $2, p_i, q_j$ pour tout i, j tel que les places p_i se décomposent dans $K/\mathbb{Q}$.*

Preuve : On rappelle que p_i se décompose dans l'extension $K/\mathbb{Q}$ si $\prod q_j$ est un carré modulo p_i, c'est à dire si, pour tout $i \leq n$

$$\left(\frac{\prod q_j}{p_i}\right) = \prod_j \left(\frac{q_j}{p_i}\right) = 1.$$

Lorsque les p_i et les q_j, $j < r_n$ ont été choisis, r doit vérifier

$$\forall i \in \{1, ..., n\} \qquad \left(\frac{r}{p_i}\right) = \prod_j \left(\frac{q_j}{p_i}\right).$$

On commence par choisir une solution non nulle *mod* p_i pour tout i. On la relève en un entier impair de $\{0, ..., 2\prod p_i \prod q_j - 1\}$ congru à 1 *mod* q_j pour tout j. Si cet entier est différent de 1 il se décompose en produit de facteurs premiers, qui sont distincts des p_i, q_i et de 2. On le choisit sans facteur carré, ce qui est possible car si r a un facteur carré p alors r/p^2 convient aussi. Notons que r peut éventuellement être égal à 1, et que ses facteurs premiers se ramifient dans $K/\mathbb{Q}$ mais cela n'influe pas sur la validité du théorème. □

On note maintenant K_n le corps ainsi construit pour tout n.

Proposition 2.24 *Le genre g_{K_n} de K_n vérifie*

$$g_{K_n} \leq g_n, \text{ où } \; g_n = \frac{3}{2} n \log n + o(n \log n)$$

$$g_{K_n} \geq g'_n, \text{ où } \; g'_n = \frac{1}{2} n \log n + o(n \log n)$$

Preuve :

$$g_{K_n} = \frac{1}{2} \sum_j \log q_j + \frac{1}{2} \log r + \frac{1}{2} \varepsilon \log 2,$$

où $\varepsilon = 2$ si 2 se ramifie, 0 sinon. On a $\log r \leq \sum_i \log p_i + \sum_j \log q_j + \log 2$. D'où

$$\log r \leq \sum_{p \leq q_{r_n}} \log p.$$

Ainsi

$$g_{K_n} \leq \sum_{p \leq q_{r_n}} \log p - \frac{1}{2} \sum_{p \leq p_n} \log p + \log 2 = g_n.$$

D'après les résultats de progression arithmétique [HW79], la fonction $\vartheta(x) = \sum_{p\leq x} \log p$ vaut $x + o(x)$, et le $n^{\text{ième}}$ nombre premier p_n vérifie $p_n = n \log n + o(n \log n)$. Ainsi

$$\sum_{p\leq p_n} \log p = n \log n + o(n \log n).$$

Comme $r_n = n + 2\sqrt{2n} + \mathcal{O}(1)$, on a $q_{r_n} = (2n + 2\sqrt{2n}) \log n + o(n \log n)$, q_{r_n} étant le $(n + r_n)^{\text{ième}}$ nombre premier. D'où :

$$\sum_{p\leq q_{r_n}} \log p = (2n + 2\sqrt{2n}) \log n + o(n \log n),$$

et on a :

$$g_n = \frac{3}{2} n \log n + o(n \log n).$$

La seconde inégalité qui nous servira dans le corollaire est similaire, on l'obtient en minorant r par 1. $\square$

On applique le théorème à $K_n/\mathbb{Q}$. Alors il existe une 2-tour non ramifiée $(K_n^i)_{i\geq 0}$, avec $K_n^0 = K_n$, où les places p_n sont totalement décomposées.

Proposition 2.25 $g_{K_n^i} = 2^i g_{K_n}$

Preuve : Comme la tour est non ramifiée, on a l'égalité pour tout i, $g_{K_n^{i+1}} = g_{K_n^i}[K_n^{i+1} : K_n^i]$. Ainsi par récurrence immédiate on a le résultat. $\square$

Corollaire 2.26 $2\phi_{\mathbb{C}} + \phi_{\mathbb{R}} = O((n \log n)^{-1})$

Preuve : Comme pour tout i, on a $[K_n^i : K_n] = r_1 + 2r_2$,

$$\frac{2^i}{g_{K_n^i}} = \frac{r_1}{g_{K_n^i}} + 2\frac{r_2}{g_{K_n^i}}$$

et, en passant à la limite,

$$\frac{1}{g_{K_n}} = \phi_{\mathbb{R}} + 2\phi_{\mathbb{C}}.$$

D'où $\phi_{\mathbb{R}} + 2\phi_{\mathbb{C}} \leq g_n'^{-1}$ et on a le résultat d'après la proposition 2.24. $\square$

Evaluons maintenant la somme intervenant dans (1) et (2). Comme les places p_i sont totalement décomposées, à chaque étage j il y a 2^{j+1} places de normes p_i, et on a, à la limite $\phi_{p_i} = 2\frac{1}{g_{K_n}}$. Ainsi il nous faut étudier les sommes suivantes :

Proposition 2.27 *Notons* $S_n = \sum_{i=1}^n \frac{\log p_i}{\sqrt{p_i}-1}$, $S'_n = \sum_{i=1}^n \frac{\log p_i}{p_i-1}$. *Alors*

$$S_n \sim 2\sqrt{n \log n}$$

$$S'_n \sim \log (n \log n).$$

Preuve : On introduit la fonction $\Lambda : \mathbb{N} \to \mathbb{R}$ définie par

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p \text{ est premier,} \\ 0 & \text{sinon.} \end{cases}$$

Alors comme $\vartheta(x) = \sum_{n \leq x} \Lambda(n)$, on a :

$$\sum_{n \leq x} \frac{\Lambda(n)}{\sqrt{n}} = \frac{\vartheta x}{\sqrt{x}} + \int_2^x \frac{\vartheta(t)dt}{2t\sqrt{t}}.$$

Comme $\vartheta(x) = x + o(x)$, le premier terme de la somme vaut $\sqrt{x} + o(\sqrt{x})$ avec $x \to \infty$. Quant au second, c'est une intégrale divergente. Comme $\frac{\vartheta(x)}{2x\sqrt{x}} \sim \frac{1}{2\sqrt{x}}$, on a :

$$\int_2^x \frac{\vartheta(t)dt}{2t\sqrt{t}} \sim \int_2^x \frac{dt}{2\sqrt{t}} \sim \sqrt{x}$$

Comme $p_n \sim n \log n$ et la somme S_n est divergente, on a

$$S_n \sim \sum_{i \leq n} \frac{\Lambda(i)}{\sqrt{i}} \sim 2\sqrt{n \log n}.$$

Le calcul de l'équivalent de S'_n est plus aisé : il est en effet bien connu [HW79] (et cela se calcule de même que l'autre somme) que

$$\sum_{p \leq x} \frac{\log p}{p - 1} \sim \log x.$$

$\square$

Corollaire 2.28 *$\delta_n \leq 1 - \varepsilon$, où*

$$\textit{cas (1)} \quad \varepsilon \sim \frac{8}{3\sqrt{n \log n}} \quad \textit{et,}$$

$$\textit{cas (2)} \quad \varepsilon \sim \frac{4}{3n}.$$

Preuve : Nous traiterons le cas (1), le second cas se traitant de même. Comme $\sum_q \phi_q \frac{\log q}{\sqrt{q}-1} \geq 2\frac{1}{g_{K_n}} S_n$, on a

$$\delta_n \leq 1 - 2\frac{1}{g_{K_n}} S_n - (\gamma + \log 8\pi)\phi_{\mathbb{C}} - (\gamma/2 + \pi/4 + \log\sqrt{8\pi})\phi_{\mathbb{R}}.$$

Le résultat provient alors de l'équivalent du genre et de S_n, ainsi que du fait que les facteurs archimédiens soient négligeables. $\square$

Ainsi, le théorie du corps de classes se montre très efficace pour produire des exemples dans lesquels un nombre fini de places se décomposent totalement, mais donne a priori un défaut très mauvais lorsqu'on essaie d'imposer cette propriété à un nombre arbitrairement grand de places. La question se pose alors de savoir s'il existe des corps asymptotiquement bons tels qu'une infinité de places se décomposent dans ce corps. Une question plus faible est de savoir s'il est possible qu'une infinité de places se décomposent dans un corps global infini, qu'il soit bon ou mauvais, et si oui, a-t-on des informations sur la taille de son lieu de décomposition et de ramification ? C'est ce que nous allons aborder dans le paragraphe suivant.

2.5 Sur la Décomposition des places dans une tour

Comme nous l'avons vu au premier chapitre, la décomposition d'une place $\mathfrak{p}$ dans une tour asymptotiquement bonne fournit un invariant $\phi_{\mathrm{N}\mathfrak{p}}$ non nul. Il est donc censé de s'interroger sur la quantité de places qui peuvent se décomposer dans une tour infinie, qu'elle soit bonne ou mauvaise. Une première réponse est donnée par le théorème de densité de Cebotarev. Mais ce résultat n'est pas satisfaisant car il donne un renseignement sur la densité au sens de Dirichlet (où seules les places de norme égale à un nombre premier sont considérées). Le théorème de Tsfasman-Vlăduţ (inégalité fondamentale) nous donnera un résultat plus fin dans le cas des tours asymptotiquement bonnes. Enfin nous donnerons un exemple de construction d'un corps global infini qui nous permet de mieux cerner ces deux résultats.

> **Problème:** Etant donné un corps global infini, et T un ensemble de places qui s'y décomposent totalement, T peut-il être gros ? Comment est alors la ramification ?

Une première réponse est donnée par le résultat suivant :

Proposition 2.29 *Soit K un corps de nombres ou un corps de fonctions sur $\mathbb{F}_r$ et T un ensemble fini de places finies de K qui se décomposent totalement dans une extension séparable L/K de degré n telle que, si K est un corps de fonctions, $\bar{\mathbb{F}}_r \cap L = \mathbb{F}_r$. Alors $\bar{\delta}(T) \leq \frac{1}{n}$.*

Corollaire 2.30 *Soit (K_i) un corps global infini et T un ensemble de places finies de K_0 totalement décomposées dans (K_i). Alors $\delta(T)$ existe et vaut 0.*

On rappelle le théorème de densité de Cebotarev : Pour L/K une extension galoisienne comme dans la proposition, $G = Gal(L/K)$ et $\sigma \in G$. On pose

$$P_{L/K}(\sigma) = \left\{ \mathfrak{p} \in P(K) \mid \quad \exists \mathfrak{P} | \mathfrak{p} \in P(L) \quad \sigma = \left(\frac{L/K}{\mathfrak{P}} \right) \right\},$$

et $< \sigma >= \left\{ \tau^{-1} \sigma \tau \mid \ \tau \in G \right\}$.

Théorème 2.31 *(Cebotarev) Soit L/K une extension galoisienne comme dans la proposition, de groupe de Galois G. Alors $P_{L/K}$ admet une densité au sens de Dirichlet et*

$$\delta(P_{L/K}(\sigma)) = \frac{\# < \sigma >}{\# G}.$$

Preuve : : [Neu99, 7.13.4] $\square$

Rappelons le lemme suivant :

Lemme 2.32 *Soit L/K une extension de corps globaux comme dans la proposition, et N la clôture galoisienne de L/K. $\mathfrak{p}$ se décompose totalement dans L/K si et seulement si il se décompose totalement dans N/K.*

Preuve du lemme: la seule chose à démontrer est l'implication. En effet si $\mathfrak{p}$ se décompose dans N/K alors elle est évidemment décomposée dans L/K en tant que sous-corps. Considérons donc $\mathfrak{p}$ une place finie de K totalement décomposée dans L/K, et considérons $\mathfrak{P}/\mathfrak{p}$ une place au-dessus de $\mathfrak{p}$ dans N. Soit $G_{\mathfrak{P}}$ son groupe de décomposition. Considérons le double quotient $H\backslash G/G_{\mathfrak{P}}$, c'est à dire l'ensemble quotient de G par la relation d'équivalence $\sigma \sim \rho$ s'il existe $\tau \in H$ et $\gamma \in G_{\mathfrak{P}}$ tel que $\sigma = \tau\rho\gamma$. Notons $P_{\mathfrak{p}}$ l'ensemble des places de L au-dessus de $\mathfrak{p}$. Alors

$$\begin{array}{ccc} H\backslash G/G_{\mathfrak{P}} & \to & P_{\mathfrak{p}} \\ H\sigma G_{\mathfrak{P}} & \mapsto & \sigma(\mathfrak{P}) \cap L \end{array}$$

définit une application bijective.

Le premier point à démontrer est que cette application est bien définie. Si $\sigma \in G, \tau \in H$ et $\gamma \in G_{\mathfrak{P}}$ alors $\tau\sigma\gamma(\mathfrak{P}) = \tau\sigma(\mathfrak{P})$. Mais $\sigma(\mathfrak{P})$ et $\tau\sigma(\mathfrak{P})$ sont deux places de N au-dessus de $\sigma(\mathfrak{P}) \cap L$ et ainsi l'application est bien définie. La surjectivité provient de celle de l'application $G \to P_{\mathfrak{p}}$. En effet soit $\mathfrak{q} \in P_{\mathfrak{p}}$ et $\mathfrak{Q}/\mathfrak{q}$. Il existe $\sigma \in G$ tel que $\sigma(\mathfrak{P}) = \mathfrak{Q}$ car l'action du groupe de Galois est transitive. Ainsi on a la surjectivité.

Pour l'injectivité, on suppose que σ et ρ ont même image, et on montre qu'ils appartiennent à la même classe. Comme $\sigma(\mathfrak{P}) \cap L = \rho(\mathfrak{P}) \cap L$, il existe $\tau \in H$ tel que $\tau\sigma(\mathfrak{P}) = \rho(\mathfrak{P})$ $(\star)$ car H agit transitivement sur les idéaux au-dessus de $\sigma(\mathfrak{P}) \cap L$. Alors on pose $\gamma = \tau^{-1}\sigma^{-1}\rho$. Comme $\tau^{-1}\sigma^{-1}\rho(\mathfrak{P}) = \mathfrak{P}$ d'après $(\star)$, on a bien $\gamma(\mathfrak{P}) = \mathfrak{P}$, c'est à dire $\gamma \in G_{\mathfrak{P}}$.

Ainsi on définit une application bijective, et en particulier, les deux ensembles finis ont même cardinal. Si $\mathfrak{p}$ se décompose totalement dans L, $\#(P_{\mathfrak{p}}) = n$. Mais alors $H\sigma G_{\mathfrak{P}}$ a pour cardinal $\#G/n = \#H = \#H\sigma$. Comme $H\sigma \subset H\sigma G_{\mathfrak{P}}$ ces deux ensembles sont égaux. On a donc, pour tout $\sigma \in G$, $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}}\sigma^{-1} \subset H$.

Considérons alors G' le sous-groupe de G engendré par les $G_{\sigma\mathfrak{P}}$. Il est distingué dans G, et est en fait un sous-groupe de H. Ainsi le sous-corps de N fixé par ce sous-groupe contient L et est galoisien sur K. Supposons que L/K n'était pas galoisienne (sinon le résultat est trivial). Comme N est le plus petit sur-corps de L tel que N/K est une extension galoisienne on a $N^{G'} = N$ et $G' = \{1\}$. Ainsi $G_{\mathfrak{P}} = \{1\}$ et on a prouvé le lemme. $\blacksquare$

Pour une extension L/K de corps de nombres, on définit $P_{L/K}$ comme l'ensemble des places non ramifiées de K admettant une place de degré 1 sur K au-dessus d'elle.

Lemme 2.33 *Avec les hypothèses du lemme précédent, notant $G = Gal(N/K)$ et $H = Gal(N/L)$, on a :*

$$P_{L/K} = \bigsqcup_{<\sigma> \cap H \neq \emptyset} P_{N/K}(\sigma).$$

Preuve du lemme: [Neu99, 7.13.5] $\blacksquare$

Lemme 2.34 *Sous les mêmes hypothèses, on a* $\delta(P_{L/K}) \geq \frac{1}{n}$ *avec égalité si et seulement si* L/K *est galoisienne.*

Preuve du lemme:[Neu99, 7.13.6] ■

Preuve de la proposition : on considère N/K la clôture galoisienne de L/K. Comme T est inclus dans l'ensemble des places de L qui sont totalement décomposées, on a $T \subset P_{N/K}$ d'après le lemme (2.3). Alors, d'après le lemme précédent,

$$\bar{\delta}(T) \leq \delta(P_{N/K}) = \frac{1}{[N : K]} \leq \frac{1}{n}.$$

Pour ce qui est de son corollaire, on fait tendre $n \to +\infty$. □

Proposition 2.35 *Soit* $\mathcal{K} = \bigcup K_n$ *une tour de corps globaux (infinie) vérifiant la propriété :*

$$\exists \varepsilon > 0 \quad \forall n \quad \frac{[K_n : K_0]}{g(K_n)} > \varepsilon$$

(c'est le cas des tours asymptotiquement bonnes). Soit T *un ensemble de places totalement décomposées dans* $\mathcal{K}$*. Alors*

$$\sum_{\mathfrak{p} \in T} \frac{\log \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p}) - 1} \leq \frac{[K_0 : \mathbb{Q}]}{\varepsilon}(1 - \frac{1}{2}(\log 2\pi + \gamma)\varepsilon) \quad (NF),$$

$$\sum_{\mathfrak{p} \in T} \frac{\log_r \mathrm{N}(\mathfrak{p})}{\sqrt{\mathrm{N}(\mathfrak{p})} - 1} \leq \frac{n_{K_0}}{\varepsilon} \quad (FF),$$

où γ *est la constante d'Euler. En particulier, on obtient un bien meilleur résultat que précédemment.*

Preuve : Faisons la preuve dans le cas des corps de nombres, celui des corps de fonctions se traitant de même à partir de l'inégalité appropriée. D'après le théorème 1.17, on a

$$\sum_q \frac{\phi_q \log q}{q - 1} + (\gamma/2 + \log 2\sqrt{\pi})\phi_{\mathbb{R}} + (\gamma + \log 2\pi)\phi_{\mathbb{C}} \leq 1.$$

Comme $\phi_{\mathbb{R}} + 2\phi_{\mathbb{C}} = \lim [K_n : K_0]/g(K_n) \geq \varepsilon$, on a l'inégalité

$$\sum_q \frac{\phi_q \log q}{q - 1} \leq 1 - \frac{1}{2}(\log 2\pi + \gamma)\varepsilon.$$

Soit $T = Dec(\mathcal{K})$ l'ensemble des places de K_0 totalement décomposées dans la tour. Pour q tel qu'il existe dans T une place de norme q (l'ensemble de ces places étant noté T_q, $\#T_q = N_q(T)$), on a $\Phi_q(K_n)/g(K_n) \geq [K_n : K_0]/g(K_n) \geq \varepsilon$, d'où $\phi_q \geq \varepsilon$. On a alors

$$\sum_{\mathfrak{p} \in T} \frac{\log \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p}) - 1} \leq \sum_q N_q(T) \frac{\log q}{q - 1} \leq \sum_{q \in T_q} [K_0 : \mathbb{Q}] \frac{\log q}{q - 1} \leq \frac{[K_0 : \mathbb{Q}]}{\varepsilon} \sum_{q \in T_q} \phi_q \frac{\log q}{q - 1},$$

$$\text{d'où} \quad \sum_{\mathfrak{p} \in T} \frac{\log \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p}) - 1} \leq \frac{[K_0 : \mathbb{Q}]}{\varepsilon} \sum_q \phi_q \frac{\log q}{q - 1} \leq \frac{n_{K_0}}{\varepsilon}(1 - \frac{1}{2}(\log 2\pi + \gamma)\varepsilon).$$

□

Remarque:

i. Sous GRH et d'après un calcul similaire, le théorème 1.15 nous donne même l'inégalité

$$\sum_{\mathfrak{p}\in T} \frac{\log \mathrm{N}(\mathfrak{p})}{\sqrt{\mathrm{N}(\mathfrak{p})}-1} \leq \frac{[K_0:\mathbb{Q}]}{\varepsilon}(1-\frac{1}{2}(\log 8\pi+\gamma)\varepsilon).$$

ii. Dans le cas des corps de nombres l'hypothèse revient à dire que la tour est asymptotiquement bonne, car $\lim[K_n:K_0]/g(K_n)=\phi_{\mathbb{R}}+2\phi_{\mathbb{C}}$. Ainsi si le terme de droite est non nul, la limite est positive et la tour vérifie la propriété de la proposition, et réciproquement, si la tour vérifie la propriété, alors la somme de droite est non nulle.

Nous allons à présent montrer que ces résultats ne peuvent être que difficilement améliorés sous la forme d'un exemple.

Théorème 2.36 *Pour tout corps global K_0, il existe un corps global infini $\mathcal{K}/K_0$ tel qu'une infinité de places T se décompose dans $\mathcal{K}$, tel que $\sum_{\mathfrak{p}\in T}\mathrm{N}\mathfrak{p}^{-1}$ est infinie, n'ayant pas de ramification sauvage sur K_0, et tel que la densité de Dirichlet de Ram($\mathcal{K}$) est nulle.*

Preuve : On va une nouvelle fois utiliser le théorème de Grunwald-Wang qui se montre très efficace lorsqu'on ne veut pas s'assurer d'un nombre fini de places ramifiées. Pour un ensemble E de places d'un corps global K, nous noterons $s(E):=\sum_{\mathfrak{p}\in E}\mathrm{N}\mathfrak{p}^{-1}$, éventuellement infinie.

Soit K_0 un corps global quelconque. Traitons, par commodité, le cas des corps de nombres. Notons S_0 (resp. D_0) le lieu de ramification de $K_0/\mathbb{Q}$ (resp. l'ensemble des places totalement décomposées dans $K_0/\mathbb{Q}$). On généralisera cette notation aux autres indices que 0 par $S_n=Ram(K_n/K_{n-1})$ et $D_n=Dec(K_n/\mathbb{Q})$. Soit T_0 un ensemble fini de places de $\mathbb{Q}$ totalement décomposées dans $K_0/\mathbb{Q}$ tel que $s(T_0)\geq 1$. Un tel ensemble existe puisqu'en vertu du théorème de Cebotarev, $\delta(D_0)>0$.

Pour K_1 prenons une extension de K_0 cyclique de degré ℓ (avec $\ell\in T_0$, et ℓ différent de la caractéristique de K_0 dans le cas des corps de fonctions), non ramifiée au-dessus des places finies de $K_0/\mathbb{Q}$ dont la norme n'est pas un premier, telle que l'ensemble au-dessus de T_0 est totalement décomposé. Ceci est possible d'après le théorème de Grunwald-Wang car la densité de Dirichlet des places qui n'ont pas pour norme un nombre premier est nulle. Pour former T_1, adjoignons à T_0 un ensemble de places de $\mathbb{Q}$ totalement décomposées dans $K_1/\mathbb{Q}$ et tel que $s(T_1)\geq 2$. C'est possible pour la même raison que cela l'était pour T_0. De même on forme par récurrence K_n et on vérifie que cette tour $\mathcal{K}=\cup K_i$ a les propriétés voulues. En effet, on a alors $s(T_n)\geq n$. Si on appelle T l'ensemble des places totalement décomposées dans $\mathcal{K}/\mathbb{Q}$ et $S=\cup S_n$ le lieu de ramification de $\mathcal{K}/\mathbb{Q}$, alors on a $s(T)\geq s(T_n)$ pour tout n et donc $s(T)=\infty$. De plus, comme S_n est inclus dans D_{n-1} pour tout n et donc $\cup_{m>n}S_m\subset D_n$, on peut montrer que $\delta(S)=0$. En effet, supposons $\bar{\delta}(S)>1/l^{n_0}$ pour un certain entier $n_0>0$. Alors $\bar{\delta}(S-\cup_{i\leq n_0}S_i)>1/\ell^{n_0}$, mais ceci est impossible car $S-\cup_{i\leq n_0}S_i\subset D_{n_0}$ et $\delta(D_{n_0})\leq\ell^{-n_0}$, d'après la proposition 2.29. □

Remarque:

i. On peut également rencontrer des corps de nombres infinis asymptotiquement mauvais où aucun premier n'est totalement décomposé. C'est le cas de l'extension abélienne maximale de $\mathbb{Q}$ par exemple.

ii. Utilisant la proposition 2.18, on peut en fait imposer, dans le cas des corps de nombres, pour tout $\varepsilon > 0$, que $s(Ram\,\mathcal{K}) \le \varepsilon$.

Terminons par donner une réponse négative à une conjecture privée de Michel Balazard dans le cadre du séminaire du Laboratoire Poncelet (Moscou). Dans le cas de $\mathbb{Q}$ et des extensions cyclotomiques, on a le résultat extraordinaire suivant qui se cache au plus profond de l'article de Norton [Nor76].

Proposition 2.37 *Soient q un nombre premier et a non divisible par q. Soit*

$$I_x = \{p \text{ premier} \mid p = a \mod q, p \le x\}.$$

Alors il existe une constante effective M indépendante de q, a telle que

$$\left| \sum_{p \in I_x} \frac{1}{p} - \frac{1}{q-1} \log\log x \right| \le M.$$

Preuve : Ce résultat se montre en utilisant les théorèmes de Brün-Titchmarch et de Siegel-Walfisz. □

Il est difficile d'obtenir de bonnes généralisations de ces théorèmes aux corps globaux en général, en particulier dans le cas où les anneaux d'entiers ne sont pas principaux. On pourra toutefois se reporter à [Gol70] pour leur généralisation aux corps de nombres. Michel Balazard avait alors émis la conjecture :

Conjecture 2.38 *Soit K un corps global. Soit L/K une extension abélienne de degré n. Alors il existe une constante M ne dépendant que de K telle que :*

$$\left| \sum_{\mathfrak{p} \in Dec(L/K),\ \mathrm{N}\mathfrak{p} \le x} \frac{1}{\mathrm{N}\mathfrak{p}} - \frac{1}{n} \log\log x \right| \le M.$$

Malheureusement, cette conjecture n'est pas valable, du moins pas sous cette forme, comme nous allons le montrer en exhibant un exemple de corps global infini abélien (de groupe de Galois en fait pro-cyclique) :

Proposition 2.39 *Il existe un corps global infini galoisien de groupe de Galois pro-cyclique tel que $\sum_{\mathfrak{p} \in Dec(\mathcal{K})} \frac{1}{\mathrm{N}\mathfrak{p}} = \infty$.*

Preuve : Le théorème de Grunwald-Wang va une nouvelle fois nous permettre de construire cet exemple. Prenons un nombre premier $p_0 = 3$ et considérons une extension cyclique K_0 du corps de base (K extension finie séparable de $\mathbb{Q}$ ou $\mathbb{F}_r(t)$) de degré p_0. Prenons alors pour ensemble fini T_0 des idéaux premier $\mathfrak{p}_1^0, ..., \mathfrak{p}_n^0$ du corps de base totalement décomposés dans K_0 tels que $\sum_{\mathfrak{p} \in T_0} \frac{1}{\mathrm{N}\mathfrak{p}} \ge 1$.

Considérons comme corps K_1 une extension cyclique de $\mathbb{Q}$ de degré premier $p_1 > p_0$ ne divisant pas le degré de K, telle que T_0 est totalement décomposée. Alors $K_1.K_0/K$ est une extension cyclique de degré $p_1.p_0$, où T_0 est totalement décomposée. Prenons alors pour T_1 un ensemble de places du corps de base totalement décomposées dans $K_1.K_0$, contenant T_0 et vérifiant $\sum_{\mathfrak{p}\in T_1} \frac{1}{\mathrm{N}\mathfrak{p}} \geq 1$.

Supposons construite de la sorte une extension cyclique $K_n.K_{n-1}...K_0$ de K de degré $p_n...p_0$ munie d'un ensemble T_n de places totalement décomposées vérifiant $\sum_{\mathfrak{p}\in T_n} \frac{1}{\mathrm{N}\mathfrak{p}} \geq n$. Construisons K_{n+1}, T_{n+1} à partir de $K_n.K_{n-1}...K_0, T_n$ de même qu'on a construit K_1, T_1 à partir de K_0, T_0. On obtient alors une tour $K_0...K_n....$ par récurrence, qui vérifie les hypothèses de la proposition. □

Corollaire 2.40 *La conjecture 2.38 est fausse, y compris pour les extensions cycliques.*

Preuve : Supposons qu'elle soit vraie pour un certain K. Construisons la tour comme dans la proposition précédente et notons T son lieu de décomposition. On a alors, en passant à la limite avec n : pour tout x

$$\sum_{\mathfrak{p}\in T,\ \mathrm{N}\mathfrak{p}\leq x} \frac{1}{\mathrm{N}\mathfrak{p}} \leq M.$$

Passons alors à la limite pour x pour obtenir une contradiction. □

2.6 Sur l'Annulation des invariants

Jusqu'à présent nous étions intéressés par l'existence des corps globaux infinis asymptotiquement bons dans lesquels des places se décomposaient totalement, afin d'obtenir un $\phi_p > 0$. Une question très proche consiste à déterminer le support de l'ensemble Φ, c'est à dire savoir quand $\phi_q = 0$. On peut également restreindre la question, et se demander quelles places sont totalement inertes dans un corps global (infini). En effet, on s'attend à ce qu'un résultat du genre de celui de G-S permette d'exhiber une tour de corps globaux asymptotiquement bonne telle qu'une place est totalement inerte, étant donné que dans le cas quadratique, c'est seulement fixer la valeur du caractère à -1 et non 1. Mais contrairement au cas des places totalement décomposées, les places totalement inertes n'ont pas un bon comportement par compositum ou par clôture galoisienne. Toutefois, on peut passer par le cas local pour comprendre l'inertie des places de nos corps globaux.

Commençons par rappeler un exercice présent dans [SD01], qui montre déjà l'obstruction rencontrée lorsqu'on prend le compositum dans le problème des places totalement inertes.

Proposition 2.41 *Soient K et L deux extensions finies du corps global k. Soit $\mathfrak{p}$ une place de k totalement inerte dans $K.L$. Alors*

$$[K.L : k] = ppcm([K : k], [L : k]).$$

Preuve : Comme $\mathfrak{p}$ est totalement inerte dans $K.L/k$, il l'est dans K/k et L/k d'après la loi de décomposition des places dans les extensions séparables. On notera donc toujours $\mathfrak{p}$ les places au-dessus de $\mathfrak{p}$ dans les autres corps. Observons ce qui se passe dans les extensions locales. De ce fait, les extensions de $\mathcal{O}_{k_\mathfrak{p}}/\mathfrak{p}$ $\mathcal{O}_{(K.L)_\mathfrak{p}}/\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p} L_\mathfrak{p}}/\mathfrak{p}$, $\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}$ et $O_{L_\mathfrak{p}}/\mathfrak{p}$ sont de degré respectif $[K.L : k]$, $[K : k]$, et $[L : k]$. La bijection entre les extensions non ramifiées de $k_\mathfrak{p}$ et celles de $\mathcal{O}_{k_\mathfrak{p}}/\mathfrak{p}$ fait correspondre $(K.L)_\mathfrak{p}$ et $\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}.\mathcal{O}_{L_\mathfrak{p}}/\mathfrak{p}$. Mais le degré de ce dernier est ppcm$([K : k], [L : k])$ en tant que compositum de corps finis, et on en déduit donc l'égalité sur le degré souhaitée. □

Corollaire 2.42 *Le compositum de deux extensions distinctes de degré n n'a pas de places totalement inertes. En particulier, si l'extension K n'est pas galoisienne, sa clôture galoisienne K^{gal} (dans une clôture séparable $\bar{K}$) n'admet pas de place totalement inerte.*

Preuve : Le premier point est une conséquence directe de la proposition, et pour le second point on l'applique avec K et ses conjugués. □

Ainsi, contre toute attente, le problème du corps de classes pour les places totalement inertes s'avère être différent de celui des places totalement décomposées. Toutefois, dans notre étude des corps asymptotiquement bons, il nous suffit de savoir pour l'instant si $\phi_q = 0$ ou non, et dans ce cas on peut obtenir des éléments de réponse dans le cas galoisien au moyen des groupes de décomposition. Pour chaque place $\mathfrak{p}$ du corps de base k, considérons une place de la clôture séparable $\bar{k}$ la prolongeant, c'est à dire un plongement de $\bar{k}$ dans $\bar{k_{\mathfrak{p}}}$. Ainsi chaque extension de k possédera une place pointée $\mathfrak{P}$ prolongeant $\mathfrak{p}$. Etant donné une extension galoisienne K/k, on notera $G_{\mathfrak{P}}(K/k)$ ou plus simplement $G_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$ dans $\mathrm{Gal}(K/k)$.

Lemme 2.43 *Soit k un corps global. Soit K/k une extension galoisienne éventuellement infinie, $\mathfrak{p}$ une place finie de k et $\mathfrak{P}$ une place de K la prolongeant. Alors $G_{\mathfrak{P}}$ a pour cardinal $e_{\mathfrak{P}}f_{\mathfrak{P}}$ et l'extension maximale de k contenue dans K telle que $\mathfrak{p}$ est totalement décomposée est le sous-corps stable par le sous-groupe distingué $< G_{\mathfrak{P}} >$ engendré par $G_{\mathfrak{P}}$.*

Preuve : Il s'agit du passage au cas profini du cas fini que l'on supposera connu (on se rapportera à [Lan94] pour une preuve). Prenons (K_i) une suite croissante d'extensions galoisiennes sur k représentant K. Considérons $\mathfrak{p}_i$ la restriction de la place $\mathfrak{P}$ à K_i. La sous-extension maximale de K contenant k où $\mathfrak{p}$ est totalement décomposée est la réunion des $K_i^{<G_{\mathfrak{p}_i}>}$, où $G_{\mathfrak{p}_i}$ est le groupe de décomposition de $\mathfrak{p}_i$ dans K_i/k et ainsi c'est bien le corps stable par $< G_{\mathfrak{P}} >= \varprojlim < G_{\mathfrak{p}_i} >$. En effet, il est bien connu que, pour tout entier n, tout système projectif (G_i) de groupes, et tout système inductif d'anneaux (A_i), $H^n(\varprojlim G_i, \varinjlim A_i) = \varinjlim H^n(G_i, A_i)$, et en particulier c'est vrai pour $n = 0$. L'égalité des cardinaux provient du fait qu'au cas fini, la restriction est un isomorphisme entre les groupes de décomposition à chaque étage de la tour, à partir d'un certain rang. □

Proposition 2.44 *Soit $\mathcal{K}/K$ un corps global galoisien infini asymptotiquement bon, et $\mathfrak{P}$ une place de $\mathcal{K}$ au-dessus de la place finie $\mathfrak{p}$ dans K. Alors $G_{\mathfrak{P}}$ est infini si et seulement si $\phi_{\mathfrak{p},q}(\mathcal{K}) = 0$ pour tout $q \in A$.*

Preuve : En effet, le cardinal du groupe $G_{\mathfrak{P}}$ est $e_{\mathfrak{p}}f_{\mathfrak{p}}$, éventuellement infini. Supposons qu'il soit fini. Toutes les places au-dessus de $\mathfrak{p}$ ont même indice d'inertie et de ramification, et si on représente $\mathcal{K}$ par une tour (K_i) de corps galoisiens sur K, toutes les places au-dessus de $\mathfrak{p}$ dans un certain K_{i_0} sont totalement décomposées dans la tour et l'un des invariants est non nul. Réciproquement, le nombre de places au-dessus de $\mathfrak{p}$ dans K_i est $\frac{n_{K_i}}{f_{\mathfrak{p}}^{(i)} e_{\mathfrak{p}}^{(i)}}$, où $f_{\mathfrak{p}}^{(i)}$ et $e_{\mathfrak{p}}^{(i)}$ sont les indices d'inertie et de ramification dans K_i, et pour que l'un des invariants soit non-nul, il faut que $\frac{1}{f_{\mathfrak{p}}^{(i)} e_{\mathfrak{p}}^{(i)}}$ ne tende pas vers 0, et ainsi que le groupe de décomposition soit fini. □

Remarque:

i. Dans une extension galoisienne asymptotiquement bonne, seul un nombre fini de places se ramifient, et ainsi on peut lire directement le degré d'inertie de presque toutes les places au moyen des groupes de décomposition, et également dans les invariants comme étant l'exposant m tel que ϕ_{p^m} est positif, et, si aucun d'eux ne l'est, alors il est infini.

ii. Malheureusement, même dans le cas où $G_{\mathfrak{P}}$ est fini, il peut arriver que $< G_{\mathfrak{P}} >$ soit ouvert. C'est le cas des extensions ayant un faible défaut, comme nous allons le voir par la suite.

Nous avons montré qu'il existe des corps globaux infinis dont un ensemble fini prescrit d'invariants sont non nuls. Nous allons à présent démontrer un résultat que notre intuition présumait plus faible, mais qui s'avérait finalement être très difficile. Montrons alors qu'il existe un corps de nombres asymptotiquement bon tel qu'un ensemble prescrit d'invariants est nul :

Théorème 2.45 *Soit p un nombre premier impair et S_0 un ensemble de premiers congrus à 1 modulo p, tels que $\mathbb{Q}_{S_0}(p)$ — la p-extension maximale de $\mathbb{Q}$ non ramifiée hors de S_0— soit de dimension cohomologique 2. Soit P un ensemble fini de nombres premiers. Alors il existe un ensemble fini de premiers S contenant S_0 et ne contenant pas p, tel que, pour tout $\ell \in S \cup P$, pour tout $m > 0$, $\phi_{\ell^m}(\mathbb{Q}_S(p)) = 0$.*

Remarque: Notons que seuls les premiers congrus à $0, 1$ modulo p peuvent se ramifier dans une p-extension, ainsi la condition sur S_0 n'est pas très forte.

Donnons alors immédiatement le corollaire qui nous intéresse :

Corollaire 2.46 *Soit P un ensemble fini de nombres premiers. Alors il existe un corps de nombres infini $\mathcal{K}$ asymptotiquement bon tel que, pour tout $\ell \in P$, pour tout $m > 0$, $\phi_{\ell^m}(\mathcal{K}) = 0$.*

Preuve : D'après [Lab06], $cd\,Gal(\mathbb{Q}_{\{7,19,61,163\}}(3)/\mathbb{Q}) = 2$, et on peut alors appliquer le théorème à l'ensemble P. De plus, le corps de nombres infini ainsi obtenu est asymptotiquement bon car modérément ramifié et non ramifié hors d'un ensemble fini. □

Montrons alors le théorème 2.45. Pour ce faire, rappelons (de façon incomplète) deux théorèmes dus à Schmidt ([Sch06] théorèmes 2.2 et 2.3). On notera $G_S(p)$ le groupe de Galois de la p-extension maximale de $\mathbb{Q}$ non ramifiée hors de S.

Théorème 2.47 (Schmidt) *Soit p un nombre premier impair et S un ensemble fini de nombres premiers congrus à 1 modulo p.*

i. Supposons que $G_S(p) \neq 1$ et que $cdG_S(p) \leq 2$. Alors $cd\,G_S(p) = 2$, $scd\,G_S(p) = 3$, et pour tout $\ell \in S$, $\mathbb{Q}_S(p)$ réalise la p-extension maximale de $\mathbb{Q}_\ell$.

ii. Supposons $cd\,G_S(p) = 2$. Soit $\ell \notin S$ un autre nombre premier congru à 1 modulo p, qui n'est pas totalement décomposé dans $\mathbb{Q}_S(p)/\mathbb{Q}$. Alors $cdG_{S\cup\{\ell\}}(p) = 2$.

Considérons donc un nombre premier p impair, S_0 un ensemble de premiers congrus à 1 modulo p, tels que $cd\, G_{S_0} = 2$ et un ensemble P de nombres premiers. Commençons par prouver deux lemmes :

Lemme 2.48 *Si* $cd\, G_S(p) = 2$, *alors pour tout* $m > 1$, *pour tout* ℓ *premier qui n'appartient pas à* S, $\phi_{\ell^m}(\mathbb{Q}_S(p)) = 0$.

Preuve du lemme: Si $\mathrm{cd} G_S(p) = 2$, alors pour tout sous-groupe fermé H de $G_S(p)$, $H^n(H) = 0$ pour tout $n > 2$ [Ser94](I prop 21′). Supposons que $\phi_{\ell^m} > 0$ pour $\ell \notin S$ et $m > 1$. Alors le Frobenius de $\mathbb{F}_{\ell^m}$ qui est d'ordre fini se relève dans le groupe de décomposition de ℓ dans $G_S(p)$ en un élément d'ordre fini. Le sous-groupe cyclique fini qu'il engendre ne vérifie pas la propriété précédente, et c'est donc absurde. ■

Lemme 2.49 *Si* $cd\, G_S(p) = 2$, *alors pour tout* m, *pour tout* ℓ *premier appartenant à* S, $\phi_{\ell^m}(\mathbb{Q}_S(p)) = 0$.

Preuve du lemme: On applique le premier point du théorème 2.47, qui nous dit que l'indice d'inertie de ℓ dans $\mathbb{Q}_S(p)$ est infini (en effet, il existe des extensions non ramifiées de $\mathbb{Q}_\ell$ de degré infini). ■

Prouvons à présent le théorème.

Preuve : Considérons $\mathbb{Q}_{S_0}(p)$ et son lieu T de places totalement décomposées. On va compléter de même l'ensemble S_0 par un nombre fini de places afin d'annuler chaque ϕ_p les uns après les autres. On va montrer qu'on peut construire un ensemble S de premiers ayant les propriétés suivantes :

i. tous les $q \in S$ sont congrus à 1 modulo p,
ii. $\mathbb{Q}_S(p)$ est asymptotiquement bon et $cd\, G_S(p) = 2$,
iii. p_i, $i \leq r$, n'est pas totalement décomposé dans $\mathbb{Q}_S(p)$.

La clé de cette preuve est l'existence d'une p-extension modérément ramifiée, non ramifiée en T, telle que les p_n soient inertes. Une telle extension est rendue possible par la version précisée du théorème de Grunwald-Wang.

En effet, d'après le corollaire 2.17, il existe une extension cyclique K de degré p, non ramifiée hors de $(P(\mathbb{Q}) - T) \cup \{p\}$, telle que p et les p_i soient inertes. Posons $S = S_0 \cup \mathrm{Ram}(K)$. Ainsi aucun des p_i n'est totalement décomposé dans $\mathbb{Q}_S(p)$.

Comme seuls les nombres premiers congrus à 1 mod p peuvent se ramifier dans une p-extension (dès lors qu'ils sont premiers à p), S vérifie la première condition. $k_S(p)$ est bien asymptotiquement bon, puisque modérément ramifié, non ramifié hors d'un ensemble fini.

Afin de montrer ii, il faut montrer qu'on peut appliquer le théorème 2.47 (ii) à toutes les places de $\mathrm{Ram}(K) = \{s_1, ..., s_m\}$. Il faut alors vérifier que s_i n'est pas totalement décomposée dans $\mathbb{Q}_{S_0 \cup s_0 \cdots \cup s_{i-1}}(p)$. Comme ce corps contient $\mathbb{Q}_{S_0}$, et comme s_i n'est pas décomposé dedans puisque T est non ramifié, il n'est pas non plus décomposé dans $\mathbb{Q}_{S_0 \cup s_0 \cdots \cup s_{i-1}}(p)$. Ainsi on peut appliquer le théorème 2.47 (ii) à tout $\mathrm{Ram}(K)$ pour obtenir ii.

D'après le premier lemme, on en déduit que les $\phi_{p_i^m}(\mathbb{Q}_S)$ sont tous nuls et on a prouvé le théorème. □

Remarque: En fait, on montre le résultat plus fort suivant : en dehors d'un ensemble de densité nulle ($Dec(\mathbb{Q}_{S_0}(p))$), tous les invariants sont nuls. De plus on peut imposer que dans cet ensemble, un nombre fini quelconque d'invariants sont nuls. Il apparaît toutefois difficile d'imposer qu'ils soient tous nuls.

Problème: Est-il possible d'obtenir des résultats analogues pour le groupe de Galois de l'extension maximale de $\mathbb{Q}$, T-décomposée, S-ramifiée ? Ainsi on pourrait obtenir des corps de nombres infinis ayant un ensemble fini prescrit d'invariants non-nuls, et un ensemble fini prescrit d'invariants nuls.

2.7 Défaut des corps globaux infinis

Revenons dans ce paragraphe à la notion de défaut de corps globaux infinis. La question de l'existence de corps globaux dont le défaut est nul est d'une grande importance dans l'étude des corps globaux infinis. Dans le cas des corps de fonctions, de nombreuses constructions permettent d'obtenir des corps asymptotiquement optimaux définis sur $\mathbb{F}_{q^2}$. C'est le cas des corps globaux infinis atteignant la borne de Drinfeld-Vlăduţ . Dans le cas des corps de nombres, ou des corps de fonctions définis sur $\mathbb{F}_q$, la question est ouverte. Rappelons qu'on définit ainsi le défaut d'un corps global infini :

$$\begin{aligned}
(NF-GRH) \quad \delta^{(1)} &= 1 - \sum_q \frac{\phi_q \log q}{\sqrt{q}-1} - (\log\sqrt{8\pi} + \frac{\pi}{4} + \gamma/2)\phi_{\mathbb{R}} - (\log 8\pi + \gamma)\phi_{\mathbb{C}}, \\
(NF) \quad \delta^{(2)} &= 1 - \sum_q \frac{\phi_q \log q}{q-1} - (\gamma/2 + \log 2\sqrt{\pi})\phi_{\mathbb{R}} - (\gamma + \log 2\pi)\phi_{\mathbb{C}}, \\
(FF) \quad \delta^{(3)} &= 1 - \sum_{m=1}^{\infty} \frac{m\phi_{r^m}}{r^{\frac{m}{2}}-1}.
\end{aligned}$$

Théorème 2.50 *Pour tout i, l'application $\mathcal{K} \mapsto \delta^{(i)}(\mathcal{K})$ est croissante pour l'inclusion des corps globaux infinis.*

Preuve : Nous allons en fait montrer un résultat plus fort. Nous allons d'abord traiter le cas des places non-archimédiennes, et constater que $\mathcal{K} \mapsto \sum_q \frac{\phi_q(\mathcal{K})\log q}{\sqrt{q}-1}$ est décroissante. Les sommes intervenant dans les deux autres défauts seront également décroissantes pour les mêmes raisons.

Lemme 2.51 *Pour tout p premier, tout $m \in \mathbb{N}$, et tout $\mathcal{K} \subset \mathcal{L}$,*

$$(NF) \qquad \sum_{k=1}^{m} \frac{k\phi_{p^k}(\mathcal{L})\log p}{\sqrt{p^k}-1} \leq \sum_{k=1}^{m} \frac{k\phi_{p^k}(\mathcal{K})\log p}{\sqrt{p^k}-1},$$

$$(FF) \qquad \sum_{k=1}^{m} \frac{k\phi_{r^k}(\mathcal{L})}{\sqrt{r^k}-1} \leq \sum_{k=1}^{m} \frac{k\phi_{r^k}(\mathcal{K})}{\sqrt{r^k}-1}.$$

> **Remarque:** Ce lemme est en fait valable en remplaçant $\log p/(p^{k/2}-1)$ par toute fonction décroissante avec k.

Preuve du lemme: Traitons le cas des corps de nombres, celui des corps de fonctions se traitant de même en remplaçant p par r, et en considérant le logarithme en base r. Soient $\mathcal{K} \subset \mathcal{L}$ deux corps de nombres infinis et p un nombre premier. Rappelons que pour tout m, on a, d'après la proposition 1.7 :

$$A_m(\mathcal{K}) := \sum_{k=1}^{m} k\phi_{p^k}(\mathcal{K}) \geq A_m(\mathcal{L}).$$

Effectuons une transformation d'Abel sur $\sum_{k=1}^{m} \frac{k\phi_{p^k}(\mathcal{K})\log p}{\sqrt{p^k}-1}$:

$$\sum_{k=1}^{m} \frac{k\phi_{p^k}(\mathcal{K})\log p}{\sqrt{p^k}-1} = A_m(\mathcal{K})\frac{\log p}{\sqrt{p^m}-1} + \sum_{k=1}^{m-1} A_k(\mathcal{K})\left(\frac{\log p}{\sqrt{p^k}-1} - \frac{\log p}{\sqrt{p^{k+1}}-1}\right).$$

On en déduit le résultat. ■

Par passage à la limite des inégalités larges, on obtient :

$$\sum_{k=1}^{\infty} \frac{k\phi_{p^k}(\mathcal{L})\log p}{\sqrt{p^k}-1} \leq \sum_{k=1}^{\infty} \frac{k\phi_{p^k}(\mathcal{K})\log p}{\sqrt{p^k}-1}.$$

Lemme 2.52 *Pour deux corps de nombres infinis $\mathcal{K} \subset \mathcal{L}$ et deux réels positifs α_1, α_2 tels que $2\alpha_1 \geq \alpha_2$, on a :*

$$\alpha_1\phi_{\mathbb{R}}(\mathcal{L}) + \alpha_2\phi_{\mathbb{C}}(\mathcal{L}) \leq \alpha_1\phi_{\mathbb{R}}(\mathcal{K}) + \alpha_2\phi_{\mathbb{C}}(\mathcal{K}).$$

Preuve du lemme: Voyons ce qui se passe aux étages finis. Prenons deux tours de corps de nombres $\mathcal{K} = \cup K_i$, $\mathcal{L} = \cup L_i$, avec $K_i \subset L_i$, et écrivons les relations qui existent entre les places archimédiennes de K_i et L_i. Abandonnons les indices pour noter K et L ces corps de façon générique. Notons $\Phi_{\mathbb{R}}(K)$ l'ensemble des places réelles de K, de cardinal $r_1(K)$, et $R_2(K)$ celui des places complexes, de cardinal $r_2(K)$, et de même pour L. Les places complexes sont toujours totalement décomposées dans L_i/K_i, donnent donc naissance à $[L:K]$ places complexes de L et chaque place réelle v de K donne lieu à des places réelles et complexes de L au nombre de $r_{1,v}(L/K)$ et $r_{2,v}(L/K)$ respectivement telles que $r_{1,v}(L/K) + 2\,r_{2,v}(L/K) = [L:K]$. Ainsi on a

$$r_1(L) = \sum_{v\in R_1(K)} r_{1,v}(L/K),$$

et

$$r_2(L) = [L:K]r_2(K) + \sum_{v\in R_1(K)} r_{2,v}(L/K).$$

Soient α_1 et α_2 tels que $2\alpha_1 \geq \alpha_2$. Ainsi

$$\begin{aligned}
\alpha_1 r_1(L) + \alpha_2 r_2(L) &= \alpha_1 \sum_{v\in R_1(K)} r_{1,v}(L/K) + \alpha_2[L:K]r_2(K) + \alpha_2 \sum_{v\in R_1(K)} r_{2,v}(L/K), \\
&\leq \alpha_1 \sum_{v\in R_1(K)} (r_{1,v}(L/K) + 2\,r_{2,v}(L/K)) + \alpha_2[L:K]r_2(K) \\
&\leq [L:K]\big(\alpha_1(K)r_1(K) + \alpha_2(K)r_2(K)\big).
\end{aligned}$$

Comme $g_L \geq [L:K]g_K$, on a enfin, pour $g_K > 0$, :

$$\alpha_1 \frac{r_1(L)}{g_L} + \alpha_2 \frac{r_2(L)}{g_L} \leq \alpha_1 \frac{r_1(K)}{g_K} + \alpha_2 \frac{r_2(K)}{g_K},$$

et finalement, en passant à la limite on démontre le lemme. ■

Ces deux lemmes (le premier dans le cas des corps de fonctions) nous donnent directement, en prenant les α_1 et α_2 correspondant aux termes archimédiens du défaut, la décroissance de l'application $\mathcal{K} \mapsto 1 - \delta^{(i)}$, pour tout i, ce qui termine la preuve. □

> **Remarque:** Ainsi, pour rechercher des corps globaux **optimaux** (c'est à dire de défaut égal à zéro), il faut s'intéresser aux candidats naturels, les corps globaux juste-infinis, c'est à dire ceux qui n'ont pas de sous-corps propres infinis. Toutefois d'autres corps peuvent a priori être optimaux, mais alors ils ont des propriétés un peu similaires aux corps globaux juste-infinis, comme le montre la proposition suivante.

Nous allons à présent considérer des tours optimales, et tâcher de déduire des conditions nécessaires que doit vérifier un corps global infini pour être optimal.

Proposition 2.53 *Soit $\mathcal{K}$ un corps de nombres infini optimal (pour $\delta^{(i)}$, $i = 1$ ou 2). Si $\ell \notin Supp\Phi_{\mathcal{K}}$ alors il n'y a aucune extension infinie de $\mathbb{Q}$ contenue dans $\mathcal{K}$ telle que $\phi_{\ell^r} > 0$. En particulier, l'extension maximale de $\mathbb{Q}$ contenue dans $\mathcal{K}$ où ℓ est totalement décomposée est finie.*

Preuve : Traitons le cas $i = 1$. Notons $\mathcal{L}$ cette extension dont on suppose l'existence. La preuve du théorème précédent nous assure que, pour chaque p premier

$$\delta_p(\mathcal{L}) := \sum_{k=1}^{\infty} \frac{k\phi_{p^k}(\mathcal{L}) \log p}{\sqrt{p^k} - 1} \geq \sum_{k=1}^{\infty} \frac{k\phi_{p^k}(\mathcal{K}) \log p}{\sqrt{p^k} - 1} = \delta_p(\mathcal{K}).$$

D'après le lemme 2.52, on en déduit que

$$1 - \big(\sum_{p \neq \ell} \delta_p(\mathcal{L}) + \delta_\ell(\mathcal{L}) + \alpha_1 \phi_{\mathbb{R}}(\mathcal{L}) + \alpha_2 \phi_{\mathbb{C}}(\mathcal{L})\big) \leq 1 - (1 + \delta_\ell(\mathcal{L})),$$

où α_1 et α_2 sont les coefficients archimédiens qui interviennent dans le défaut $\delta^{(1)}$. Ainsi $\delta^{(1)}(\mathcal{L}) \leq -r\phi_{\ell^r} \log \ell / (\ell^{r/2} - 1) < 0$, ce qui est absurde. □

Proposition 2.54 *Soit $\mathcal{K}$ un corps de nombres infini galoisien asymptotiquement optimal. Soit d tel que $\phi_{p^d} > 0$. Alors $\mathcal{K}$ ne contient pas de sous-extension infinie avec $\phi_{p^m} > 0$, $m \neq d$.*

Preuve : Soit $\mathcal{L} \subset \mathcal{K}$ tel que l'un des ϕ_{p^m} est non nul, $m < d$ (l'autre cas ne peut pas se produire, du fait que $\mathcal{K}$ est galoisien). Traitons le cas du défaut sous GRH. $\mathcal{L}$ est contenu dans $\mathcal{K}$, et son défaut est strictement plus petit que celui de $\mathcal{K}$. En effet concernant les autres places et les places archimédiennes, le résultat découle des deux lemmes. Concernant la place p, comme $\mathcal{L} \subset \mathcal{K}$ on a

$$\sum_{k \le d} k\phi_{p^k}(\mathcal{L}) \ge d\phi_{p^d}(\mathcal{K}),$$

et ainsi

$$\sum_{k \le d} \frac{k\phi_{p^k}(\mathcal{L})}{\sqrt{p^k}-1} > \sum_{k \le d} \frac{k\phi_{p^k}(\mathcal{L})}{\sqrt{p^d}-1} \ge \frac{d\phi_{p^d}(\mathcal{K})}{\sqrt{p^d}-1}.$$

On en déduit que $\mathcal{L}$ a un défaut strictement plus petit que celui de $\mathcal{K}$, ce qui n'est pas possible. □

> **Remarque:** Ces deux propositions sont également valables pour les corps de fonctions, si on considère, au lieu de ϕ_q, les $\phi_{P,q}$, en définissant le support de Φ comme étant les couples (q, P). L'idée est que si un corps est asymptotiquement optimal et galoisien, une place ne contribuant pas au terme de gauche de l'inégalité fondamentale ne peut pas avoir une contribution dans un sous-corps.

Nous allons à présent démontrer que les extensions maximales de $\mathbb{Q}$ non ramifiées en dehors d'un ensemble fini de places S suffisamment grand ne peuvent jamais être asymptotiquement optimales.

Théorème 2.55 *Soit $K/\mathbb{Q}$ une extension cyclique de degré ℓ de $\mathbb{Q}$, ramifiée exactement en S un ensemble de places finies de $\mathbb{Q}$, tel que $\#S \ge 3+\ell+2\sqrt{2+\ell^2}$, et K_S la ℓ-extension maximale non ramifiée de K. Alors K_S n'est pas asymptotiquement optimal. De plus son défaut vérifie $\delta^{(2)}(K_S) \ge \alpha$, où α est définie ci-après.*

> **Remarque:** Sous ces hypothèses, toute extension contenant K_S ne peut pas être asymptotiquement optimale, en particulier c'est le cas de $\mathbb{Q}_S$.

Remarquons d'abord que la condition sur S nous assure que le corps K_S est bien infini d'après le théorème 2.9. Considérons un ensemble de places finies de K vérifiant les propriétés suivantes : P disjoint de $S(K)$, P stable par l'action du groupe de Galois de K, et constitué des places finies de plus faible norme de K vérifiant la propriété

$$\sum_{\mathfrak{p} \in P} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}-1} > g(K) - \frac{\ell\alpha_2}{2},$$

où $\alpha_2 = \gamma + \log 2\pi$. Cette série prise sur toutes les places finies de K diverge ; ainsi un tel ensemble de places P existe. On le construit en prenant consécutivement toutes les places finies de K (et celles déduites par l'action du groupe de Galois), jusqu'à ce qu'on dépasse le terme de droite. On note $\mathfrak{p}_0$ l'idéal de norme maximale dans P, et p_0 la place de $\mathbb{Q}$ en dessous de lui. On pose

$$\alpha = \frac{\ell \log p_0}{g(K)} \left(\frac{1}{\mathrm{N}\mathfrak{p}_0 - 1} - \frac{1}{\mathrm{N}\mathfrak{p}_0^{\ell} - 1} \right).$$

Preuve : Supposons alors que $\delta^{(2)}(K_S) < \alpha$. Commençons par montrer qu'il existe alors une place finie dont la contribution est nulle.

Lemme 2.56 *Il existe une place $\mathfrak{p}_1 \in P$, $\mathrm{N}\mathfrak{p}_1 \le \mathrm{N}\mathfrak{p}_0$ telle que, pour tout $m > 0$ $\phi_{p_1^m} = 0$, où $p_1 = \mathfrak{p}_1 \cap \mathbb{Q}$.*

Preuve du lemme: Supposons que pour toutes ces places (dont l'ensemble est noté P), il existe $m > 0$ tel que $\phi_{\mathfrak{p},\mathrm{N}\mathfrak{p}^m} > 0$. Comme K_S est galoisienne, c'est le cas pour toutes les places au-dessus de $\mathfrak{p} \cap \mathbb{Q} = p$.

S est par hypothèse suffisamment grand pour que l'extension maximale K_S^p de K, contenue dans K_S, où toutes les places au-dessus de p dans K sont totalement décomposées, est infinie et ceci pour toute place finie $p \notin S$. Montrons alors que pour chacune de ces places, $m = 1$. Si on veut seulement montrer que le corps n'est pas optimal, alors il suffit d'appliquer la proposition précédente, qui nous assure que $m = 1$. Ici, on montre un résultat un peu plus fort, supposons donc que $m > 1$ pour une certaine place p. Toutes les places au-dessus de p ont même norme, elles sont non ramifiées dans les tours, et ainsi sa différence de contribution au défaut dans K_S^p par rapport à celle qu'elle a dans K_S est donnée par

$$\frac{\ell \log p}{g(K)(\mathrm{N}\mathfrak{p} - 1)} - \frac{\ell \log p}{g(K)(\mathrm{N}\mathfrak{p}^m - 1)}.$$

Celle-ci ne peut pas excéder α, d'après l'inégalité fondamentale. De plus, cette quantité est décroissante en p, et croissante en m, ainsi il suffit de vérifier que, pour le plus grand des p de notre ensemble, et pour le plus petit m (soit $m = \ell$), la condition est satisfaite. D'après la définition de α, ce n'est pas vérifié, et on a donc une contradiction. Par conséquent, $m = 1$ pour toutes les places $\mathfrak{p}$ de P.

On a alors, pour chaque $\mathfrak{p} \in P$,

$$\phi_{\mathrm{N}\mathfrak{p}} = \frac{\Phi_{\mathrm{N}\mathfrak{p}}(K)}{g(K)}.$$

En effet, toutes les places au-dessus de $\mathfrak{p} \cap \mathbb{Q}$ dans K sont totalement décomposées et l'inégalité s'ensuit.

On a alors

$$\sum_q \phi_q \frac{\log q}{q-1} + \delta_\infty \geq \frac{1}{g(K)} \sum_{\mathfrak{p} \in P} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p} - 1} + \frac{\ell \alpha_2}{2\, g(K)} > 1,$$

où $\delta_\infty = \alpha_1 \phi_{\mathbb{R}}(\mathcal{L}) + \alpha_2 \phi_{\mathbb{C}}(\mathcal{L})$ est la contribution au défaut des facteurs archimédiens. En effet $\delta_\infty \geq \frac{1}{2}\alpha_2 \phi_\infty$ et $\phi_\infty = \ell\, g(K)^{-1}$. Ainsi cela contredit l'inégalité de base. ■

Considérons à présent l'extension maximale de K telle que $\mathfrak{p}_1$ est totalement décomposée. La contribution de $p_1 = \mathfrak{p}_1 \cap \mathbb{Q}$ au défaut dans cette extension est de $\frac{\ell \log p_1}{g(K)(\mathrm{N}\mathfrak{p}_1 - 1)} > \alpha$, tandis que celle dans K_S est nulle, et on en déduit donc une contradiction. □

Ainsi, on a prouvé que les tours de corps de classes construites à l'aide du théorème 2.9 ne sont jamais optimales dès que $\#S$ est suffisamment grand. Cela ne veut pas dire pour autant qu'aucune tour de corps de classes n'est optimale, en particulier, on ne peut rien dire a priori quant à celles qui seraient infinies sans passer le critère de G-S. Contrairement au cas des corps de fonctions, où l'on connaît des tours asymptotiquement optimales, l'espoir d'obtenir des tours optimales de corps de nombres s'éloigne.

Le problème de l'ensemble des valeurs prises par le défaut des corps globaux est une question difficile, et qui sera au centre de nos recherches à l'avenir. Pour le moment, nous ne savons pas s'il est dense dans $]\inf \delta, 1]$, mais nous pouvons démontrer qu'il existe des corps globaux dont le défaut est arbitrairement proche de 1, et même le résultat un peu plus fort suivant :

Proposition 2.57 *Soit $\mathcal{K}$ un corps de nombres infini galoisien, modérément ramifié, non ramifié hors d'un ensemble fini. Alors il existe une suite croissante de corps globaux infinis asymptotiquement bons contenant $\mathcal{K}$ dont le défaut tend vers* 1.

Preuve : Raisonnons avec le défaut sans GRH. Soit $P = \{p_1, \ldots, p_n, \ldots\}$, $p_1 < ... < p_n < \ldots$, le support de $\Phi_{\mathcal{K}}$. Considérons $P_n = \{p_1, ..., p_n\}$, et les corps globaux infinis $\mathcal{L}_n$ construits en 2.45 dont les invariants relatifs à P_n sont nuls. Soit $\varepsilon > 0$. Comme la série $\sum \phi_q(\mathcal{K}) \log q/(q-1)$ est convergente, il existe n_0 tel que, pour tout $n \geq n_0$,

$$\sum_{p > p_{n_0}, m > 0} \phi_{p^m}(\mathcal{K}) \frac{\log p^m}{(p^m - 1)} < \varepsilon.$$

Considérons alors $\mathcal{L}_{n_0}.\mathcal{K}$. Comme on annule ainsi les n_0 premiers invariants non nuls,

$$\sum \phi_q(\mathcal{K}.\mathcal{L}_{n_0}) \frac{\log q}{q-1} < \varepsilon.$$

On considère ensuite le compositum de ce corps avec la tour considérée en §2.4, avec n suffisamment grand, de sorte que la contribution archimédienne au défaut soit plus petite qu'ε. $\square$

Chapitre 3

Generalised Mertens and Brauer–Siegel theorems

Sommaire

The classical Brauer–Siegel theorem is a well-known theorem which describes the behaviour of the quantity hR (the product of the class number and the regulator) in a family of number fields with growing genus under the conditions that the genus grows much faster than the degree and some additional properties like normality or the Generalised Riemann Hypothesis (GRH) to deal with the Siegel zeroes. These two hypotheses are of different nature : omitting the first one changes the final result, while the second one is a technical hypothesis. Tsfasman and Vlăduţ ([TV02]) were able to remove the first hypothesis, which led to the so called generalised Brauer–Siegel theorem, and Zykin [Zyk05] was able to replace "normality" by "almost normality" in the second one using results of Stark and Louboutin. He also managed to generalise the Brauer–Siegel theorem to the case of smooth absolutely irreducible projective varieties over finite fields.

As for the Mertens theorem, proven by Mertens in the case of $\mathbb{Q}$, and much later generalised by Rosen ([Ros99]) both in cases of number and function fields, it can be regarded as the Brauer–Siegel theorem in the finite steps of the family. An explicit Mertens theorem leads therefore to an explicit formulation of the generalised Brauer–Siegel theorem. We first recall the formulations of the (generalised) Brauer–Siegel theorem and Mertens theorem, then we prove their explicit versions for number fields and smooth projective absolutely irreducible varieties over finite fields, and finally we deduce the explicit generalised Brauer Siegel theorem.

3.1 Around the Brauer–Siegel theorem

Let us now recall the notations and the definitions involved in the generalized Brauer–Siegel theorem, and state it for global fields and smooth absolutely irreducible projective algebraic varieties (*s.a.i.p.a.v.*) over the finite field $\mathbb{F}_r$. Throughout this paper we will write (NF) and (V) to say that something is true in the case of number fields and *s.a.i.p.a.v.* respectively.

3.1.1 Number field case

Given a number field K, let ζ_K be the usual zeta-function of the field K and $\varkappa_K$ be its residue at $s = 1$. Denote by $\Phi_q(K)$ the number of places of K whose norm is equal to q. Let $(K_i)_{i\in\mathbb{N}}$ be a family of finite extensions of $\mathbb{Q}$. Denote by $g_i := \log\sqrt{|\mathrm{Discr}(K_i)|}$ the genus of K_i and n_i its degree. Recall that $(K_i)_{i\in\mathbb{N}}$ is said to be asymptotically exact if $\phi_q := \lim \Phi_q(K_i)/g_i$ exist for all prime powers q and if $\phi_\mathbb{R} := \lim r_1(K_i)/g_i$ and $\phi_\mathbb{C} := \lim r_2(K_i)/g_i$ exist, where $r_1(K_i)$ and $r_2(K_i)$ stand for the number of real and complex places of K_i respectively. We put $\phi_\infty = \phi_\mathbb{R} + 2\phi_\mathbb{C}$. Being asymptotically exact is not a restrictive property. In fact, every tower of global fields is asymptotically exact, and each family of number fields contains an asymptotically exact subfamily. In the classical Brauer–Siegel theorem, all these ϕ_q are equal to zero because of the assumption $n_i/g_i \to 0$:

Theorem 3.1 (Classical Brauer–Siegel) *Assume that the family of number fields (K_i) is normal over $\mathbb{Q}$ or that* GRH *holds, and assume that $\lim_i n_i/g_i = 0$. Then $\log h_iR_i \sim g_i$.*

In order to prove this theorem, we need to use the class number formula :

$$\varkappa_K = \frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}}hR.$$

The result can be reformulated in this way :

$$\lim_i \frac{\log \varkappa_{K_i}}{g_i} = 0.$$

Suppressing this hypothesis leads to the Tsfasman-Vlăduţ Brauer–Siegel theorem (T-V B-S). This time, the ϕ_q are not always equal to zero :

Theorem 3.2 (T-V BS (2002)) *Let $\mathcal{K} = (K_i)_{i\in\mathbb{N}}$ be an asymptotically exact family of number fields. Assume either that* GRH *holds, or that (K_i) is a family of almost-normal number fields (We will say that a number field L is almost normal if there exists a tower $L_0 \subset \cdots \subset L_n = L$ of fields such that L_{i+1} is normal over L_i for all i). Then the limit $\kappa = \lim_i \frac{\log \varkappa_{K_i}}{g_i}$ exists and we have the following equality :*

$$\kappa = \sum_q \phi_q \log\left(\frac{q}{q-1}\right) < +\infty,$$

where the sum is taken over all the powers of prime numbers.

In their paper [TV02], Tsfasman and Vlăduţ proved this theorem without the assumption of GRH for asymptotically good families of almost normal number fields (this means $\lim n_i/g_i > 0$), and Zykin [Zyk05] proved this is also true for asymptotically bad families. In order to get this result, we have to deal with two inequalities, but one of them is always satisfied :

Theorem 3.3 (BS Inequality) *Let $\mathcal{K} = (K_i)_{i\in\mathbb{N}}$ be an asymptotically exact family of number fields. Then*

$$\limsup_i \frac{\log \varkappa_{K_i}}{g_i} \leq \sum_q \phi_q \log\left(\frac{q}{q-1}\right) < +\infty.$$

The difficulties come from the second inequality

$$\sum_q \phi_q \log\left(\frac{q}{q-1}\right) \leq \liminf_i \frac{\log \varkappa_{K_i}}{g_i},$$

which requires technical assumptions.

3.1.2 Case of algebraic varieties over a finite field

Consider an algebraic variety X of dimension d, defined over a finite field $\mathbb{F}_r$. Suppose that X is smooth, projective and absolutely irreducible and let $|X|$ denote the set of its closed points. For $\mathfrak{p} \in |X|$ and $k(\mathfrak{p})$ its residue field, let $\deg(\mathfrak{p})$ be the degree of the field extension $[k(\mathfrak{p}) : \mathbb{F}_r]$. Define now for $m \geq 1$ the Φ-numbers as before :

$$\Phi_{r^m} := \#\left\{\mathfrak{p} \in |X| \mid \deg(\mathfrak{p}) = m\right\}.$$

Put $\bar{X} = X \otimes \mathbb{F}$ where $\mathbb{F} = \bar{\mathbb{F}_r}$ is the algebraic closure of $\mathbb{F}_r$. Let ℓ be a prime different from p. Let $b_i = \dim H^i(\bar{X}, \mathbb{Q}_\ell)$ for $0 \leq i \leq 2d$ be the Betti numbers for the ℓ-adic etale cohomology of X. X is smooth, so they do not depend on ℓ and verify the equality $b_i = b_{2d-i}$ because of the Poncaré duality. Let $b_X = \max_{i=0,..,2d} b_i$. In the case of dimension 1, $b_0 = b_2 = 1$ and $b_1 = g$, so we have $b_X = \max(g, 1)$. In this theory the quantity b_X will play the role of the genus of number fields (and function fields). Since the asymptotic theory of varieties of dimension higher than 1 is not yet well understood, we do not know exactly which quantity is the exact analogue of the genus. We chose this number b_X because it was easier to compute the sums, but it might happen that the sum of b_i or a certain sum of b_i's with coefficients depending on r could make a better choice. However, unless we want to make r or d grow, all these choices are equivalent.

By the famous Deligne–Grothendieck theorem, the zeta function of X verifies

$$Z(X,t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}},$$

where

$$P_i(t) = \prod_{j=1}^{b_i}(1 - \omega_{i,j} r^{i/2} t),$$

$\omega_{i,j}$ being algebraic numbers of module 1 and $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - r^d t$. We will consider $\zeta_X(s) = Z(X, r^{-s})$, and $\varkappa_X = \mathrm{Res}_{s=d}\zeta_X$.

Let us fix the dimension d, and let X go through a family of *s.a.i.p.a.v.* of dimension d. We say that the family $(X_i)_{i\in\mathbb{N}}$ is asymptotically exact if $b_{X_i} \to \infty$, and if, for all $m \geq 1$, the limit $\phi_{r^m} = \lim_i \Phi_{r^m}/b_{X_i}$ exist.

We can now formulate a generalisation of the Brauer–Siegel theorem for varieties of dimension d. It was proved by Tsfasman and Vlăduţ in the function field case [TV02], and by Zykin (unpublished) in the case of $d > 1$, using a different definition of b_X.

Theorem 3.4 *Let $(X_i)_{i\in\mathbb{N}}$ be an asymptotically exact family of s.a.i.p.a.v. of dimension d defined over $\mathbb{F}_r$. Then $\kappa = \lim_i \log(\varkappa_{X_i})/b_{X_i}$ exists and we have the following equality :*

$$\kappa = \sum_{m=1}^{\infty} \phi_{r^m} \log\left(\frac{r^{dm}}{r^{dm}-1}\right)$$

Unfortunetaly, we do not know any reasonable interpretation of the residue of the zeta function at $s = d$, such as we have for $s = 1$ through the class number formula in the number field and function field cases .

3.2 Mertens theorem and its relation to the generalised BS theorem

If one wants to get an explicit version of the generalized Brauer–Siegel equality, one need to know what happens explicitly between $\varkappa_{K_i}$ and $\sum_{q\le x} \phi_q \log \frac{q}{q-1}$ at the finite steps of the family. This is given by the Mertens theorem.

Theorem 3.5 (Mertens) *For any number field K and any s.a.i.p.a.v. X, one has :*

$$(V) \qquad \prod_{\substack{P\in|X|\\ \deg(P)\le N}} \left(1-\frac{1}{\mathcal{N}P^d}\right) = \frac{e^{-\gamma_X}}{N} + \mathcal{O}_X\left(\frac{1}{N^2}\right),$$

$$(NF) \qquad \prod_{\substack{P\in P_f(K)\\ \mathcal{N}P\le x}} \left(1-\frac{1}{\mathcal{N}P}\right) = \frac{e^{-\gamma_K}}{\log x} + \mathcal{O}_K\left(\frac{1}{\log^2 x}\right),$$

$$(NF-GRH) \qquad \prod_{\substack{P\in P_f(K)\\ \mathcal{N}P\le x}} \left(1-\frac{1}{\mathcal{N}P}\right) = \frac{e^{-\gamma_K}}{\log x} + \mathcal{O}_K\left(\frac{1}{\sqrt{x}}\right),$$

where

$$(V) \qquad \gamma_X = \gamma + \log(\varkappa_X \log r),$$

$$(NF) \qquad \gamma_K = \gamma + \log \varkappa_K,$$

$P_f(K)$ being the set of finite places of K, and $\mathcal{N}P$ denoting the absolute norm of the place P.

The function field case and the number field case are due to Rosen, who proved them following the classical proof of the Mertens classical theorem [HW79]. But he paid no attention to the behaviour of the constants in field extensions. Unfortunately we did not know about his work before having ended ours. Mireille Car also proposed in [Car] a different proof in the case of function fields. In the number field case, we also follow the classical Mertens proof with small variations in order to get an explicit version of this theorem, which takes into account the genus and the degree of K. In the case of varieties over finite fields, we present a natural proof using explicit formulae. We prove in fact the following sharper results :

Without assuming GRH, we have to deal with exceptional zeroes. A real zero ρ of ζ_K is said to be exceptional if $1-(8\,g)^{-1}\leq \rho < 1$. A number field has at most one exceptional zero. A real zero ρ is a Siegel zero if $1-(32\,g)^{-1}\leq\rho<1$.

Theorem 3.6 *Let K be a number field.*

$$(NF) \qquad \sum_{q\leq x}\Phi_q\log\left(\frac{q}{q-1}\right)=\log\log x+\gamma+\log\varkappa_K+\tau_1(x)+\frac{1}{1-\rho}\tau_2(x),$$

and there exist effective constants C, C_1, C_2 such that, for all $x\geq Cn\,g^2$,

$$|\tau_1(x)|\leq C_1\frac{1}{\log x},$$

$$|\tau_2(x)|\leq C_2\frac{1}{\log x},\ \textit{if } K \textit{ has an exceptional zero } \rho,$$

and $\tau_2(x)=0$ otherwise.

The condition on x does not allow us to have explicit results as in the case where GRH holds, but these results, combined with theorem 3.3, lead us to the unified proof of the Brauer–Siegel theorem, and to other nice results around the Brauer–Siegel theorem and the family of ϕ_q.

Corollaire 3.7 *Let (K_i) be an asymptotically exact family of almost normal number fields. Then the limit $\lim_{i\to\infty}\frac{\log\varkappa_{K_i}}{g_{K_i}}=\kappa$ exists and verifies the following equality :*

$$\sum_q\phi_q\log\frac{q}{q-1}=\kappa,$$

the sum being taken over all prime powers q.

We cannot suppress the hypothesis of normality, because of exceptional zeroes that can appear in the family. But we can say something more in the general case :

Proposition 3.8 *Let (K_i) be an asymptotically exact family of number fields.*

i. Assume that $\lim_i\frac{n_i\log n_i}{g_i}=0$. Then κ exists and equals 0.

ii. Assume that the family (K_i) is asymptotically good (i.e. $\phi_\infty>0$), and that there are infinitely many Siegel zeroes in the family. Then

$$\sum_q\phi_q\log\frac{q}{q-1}\leq\phi_\infty\log\frac{e}{\phi_\infty}.$$

If we assume GRH, there is no condition on x, and we have the following result, which leads to an explicit version of the generalised Brauer–Siegel theorem.

Theorem 3.9 (GRH Mertens theorem) *Assume that* GRH *holds for number fields. Then*

$$(V) \qquad \sum_{m=1}^{N} \Phi_{r^m} \log\left(\frac{r^{dm}}{r^{dm}-1}\right) = \log N + \gamma + \log\left(\varkappa_X \log r\right) + \mathcal{O}\left(\frac{1}{N}\right) + b_X\,\mathcal{O}\left(\frac{r^{\frac{-N}{2}}}{N}\right)$$

$$(NF-GRH) \quad \sum_{q\leq x} \Phi_q \log\left(\frac{q}{q-1}\right) = \log\log x + \gamma + \log \varkappa_K + n_K\,\mathcal{O}\left(\frac{\log x}{\sqrt{x}}\right) + g_K\,\mathcal{O}\left(\frac{1}{\sqrt{x}}\right)$$

where the constants involved in the $\mathcal{O}$ are effective and do not depend either on X, or on K.

Corollaire 3.10 *Let (K_i) be an asymptotically exact family of number fields, and (X_i) of s.a.p.a.i.v. of dimension d. Assuming* GRH *in the number field case, we get :*

$$(V) \qquad \sum_{q\leq r^N} \phi_q \log\frac{q}{q-1} = \kappa + \mathcal{O}\left(\frac{r^{\frac{-N}{2}}}{N}\right),$$

$$(NF-GRH) \qquad \sum_{q\leq x} \phi_q \log\frac{q}{q-1} = \kappa + \mathcal{O}\left(\frac{\log x}{\sqrt{x}}\right).$$

3.3 Proof of the Mertens theorem

3.3.1 Proof in the number field case

In order to prove the Mertens theorem for number fields, we follow the nice proof of the classical Mertens theorem of [HW79] as Rosen does in his article, but we use another counting function for prime ideals. In addition, we need a precise version of the Mertens theorem, so we will have to do the work once again, sketching Rosen's proofs.

Let K be a number field, let $n = [K : \mathbb{Q}]$ be its degree and $g = \frac{1}{2}\log|\mathrm{Discr}(K)|$. Put $\pi(x) := \#\{P \in P(K)\,|\,\mathcal{N}P \leq x\}$. One can estimate $\pi(x)$ by the following bound due to Lagarias and Odlyzko, and improved by Serre [Ser81] :

Consider the Li-function defined by

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Theorem 3.11 (Prime ideals theorem)

$$(NF) \qquad \pi(x) = \mathrm{Li}(x) + \Delta(x),$$

where, for all x such that

$$(C1) \qquad \log x \geq c_3\, n\, g^2$$

$$|\Delta(x)| \leq \mathrm{Li}(x^\rho) + c_1 x \exp\left(-c_2\, n^{-\frac{1}{2}} \log^{\frac{1}{2}}(x)\right),$$

the term in $\mathrm{Li}(x^\rho)$ is only there if ζ_K has an exceptional zero ρ. Under GRH, one has the stronger result available for all $x \geq 2$:

$$(NF-GRH) \qquad |\Delta(x)| \leq c x^{\frac{1}{2}}\left(2g + n\log x\right).$$

First, we will give an asymptotic expression for $\sum \frac{1}{\mathcal{N}P}$:

Proposition 3.12

$$\sum_{\mathcal{N}P\leq x} \frac{1}{\mathcal{N}P} = \log\log x + B + o(1).$$

Proof : We have the formula :

$$C(x) = \sum_{\mathcal{N}P\leq x} \frac{1}{\mathcal{N}P} = C(2) + \int_2^x \frac{d\pi(t)}{t} = C(2) + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{d\Delta(t)}{t},$$

thus

$$\sum_{\mathcal{N}P\leq x} \frac{1}{\mathcal{N}P} = \int_2^x \frac{dt}{t\log t} + \frac{\Delta(x)}{x} + \int_2^x \frac{\Delta(t)dt}{t^2}.$$

Let us first not take into account the dependancies on n and g. As

$$\mathrm{Li}(t^\rho) \sim \frac{t^\rho}{\log t^\rho}, \quad \rho < 1,$$

$$\int_2^x \mathrm{Li}(t^\rho)t^{-2}dt \quad \text{is convergent.}$$

In order to prove the convergence of the second term, we need the following lemma :

Lemma 3.13 *For all x such that*

$$(C2) \qquad \log x \geq 32^2 c_2^{-2} n \log^2 \frac{n^{\frac{1}{2}}}{c_2},$$

we have

$$\exp\left(-c_2 n^{-\frac{1}{2}} \log^{\frac{1}{2}} x\right) \leq \log^{-2} x.$$

Proof of the lemma: Put $y = \log^{\frac{1}{2}} x$ et $c = n^{\frac{1}{2}}/c_2$. Consider $f(y) = y^4 \exp -\frac{y}{c}$. We have to prove that $f(y)$ is less than 1 if y is big enough. We prove that f is decreasing for $y \geq 4c$. Assume first that $c \leq e$. Then $y = 16c$ verifies the inequality $f(y) \leq 1$. Indeed

$$f(16c) = 2^{16}c^4e^{-16} = \frac{2^{16}}{e^{12}}\frac{c^4}{e^4} \leq 1.$$

If $c > e$, then $y = 32c\log c$ fits. Indeed,

$$f(y) = 32^4c^4\log^4(c)\, e^{-32\log c} = \frac{2^{20}}{c^{24}}\frac{\log^4 c}{c^4} \leq 1,$$

this estimate finishing the proof. ■

Therefore we have $\exp\left(-c_2\, n^{-\frac{1}{2}} \log^{\frac{1}{2}}(t)\right) = \mathcal{O}((\log t)^{-2})$, and

$$\int_2^x \frac{t\exp\left(-c_2\, n^{-\frac{1}{2}} \log^{\frac{1}{2}}(t)\right)dt}{t^2} \quad \text{is convergent.}$$

We obtain the convergence of the second integral with $x \to \infty$, because, for t big enough :

$$|\Delta(t)| \leq \mathrm{Li}(t^\rho) + c_1 t \exp\left(-c_2 n^{-\frac{1}{2}} \log^{\frac{1}{2}}(t)\right).$$

Finally we get

$$\sum_{\mathcal{N}P \leq x} \frac{1}{\mathcal{N}P} = \log\log x + B + o(1).$$

□

We make now the residue appear continuing the asymptotical expansion of $\sum \frac{1}{\mathcal{N}P}$ by the calculation of the constant term B.

Proposition 3.14

$$B = \sum_P \left\{\log\left(1 - \frac{1}{\mathcal{N}P}\right) + \frac{1}{\mathcal{N}P}\right\} + \gamma + \log \mathrm{Res}_{s=1}\zeta_K(s).$$

Proof : For a complete proof, we refer to the article of Rosen [Ros99], but let us still give the sketch of the proof. Write $C(x) = \log\log x + B + \varepsilon(x)$. For $\delta > 0$ define

$$g(\delta) = \sum_P \frac{1}{\mathcal{N}P^{1+\delta}},$$

and

$$f(\delta) = g(\delta) - \log\zeta(1+\delta).$$

After some computation using the Abel transform, we find $g(\delta) = B - \gamma - \log\delta + \mathcal{O}(\delta)$. Comparing with $\log\zeta_K(1+\delta) = -\log\delta + \log \mathrm{Res}_{s=1}\zeta_K(s) + \mathcal{O}(\delta)$, we get $f(\delta) = B - \gamma - \log \mathrm{Res}_{s=1}\zeta_K(s) + \mathcal{O}(\delta)$. Taking the limit when $\delta \to 0$, we obtain :

$$B = \sum_P \left\{\log\left(1 - \frac{1}{\mathcal{N}P}\right) + \frac{1}{\mathcal{N}P}\right\} + \gamma + \log \mathrm{Res}_{s=1}\zeta_K(s).$$

□

We finally conclude that

$$\sum_{\mathcal{N}P \leq x} \log\frac{\mathcal{N}P}{\mathcal{N}P - 1} = \log\log x + \gamma + \log \mathrm{Res}_{s=1}\zeta_K(s) + o(1).$$

Let us now estimate the error term

$$\varepsilon(x) = \Delta(x)x^{-1} - \int_x^\infty \Delta(t)t^{-2}dt,$$

as the function of n and g.

Proposition 3.15 *There are computable constants such that :*

$$(GRH) \qquad \text{For any } x \geq 2 \text{ we have } |\varepsilon(x)| \leq cx^{-\frac{1}{2}}\left(6g + 3n\log x + 2\,n\right),$$

$$(NF) \qquad \text{For } x >> 1, \text{ we have } |\varepsilon(x)| \leq c_4 \frac{1}{\rho\log x}\left(1 + (1-\rho)^{-1}\right) + 2c_1\log^{-1} x,$$

$x >> 1$ meaning that x must verify conditions $(C1)$and $(C2)$, the term in ρ being present only if ζ_K has an exceptional zero.

Proof : Assuming GRH, we obtain directly :

$$|\varepsilon(x)| \leq cx^{-\frac{1}{2}}\,(2g + n\log x) + \int_x^\infty c\,t^{-\frac{3}{2}}\,(2g + n\log t)\,dt$$

$$|\varepsilon(x)| \leq cx^{-\frac{1}{2}}\,(2g + n\log x) + 2cx^{-\frac{1}{2}}(n\log x + 2\,n + 2g),$$

and finally :

$$(GRH) \qquad\qquad |\varepsilon(x)| \leq cx^{-\frac{1}{2}}\,(6g + 3n\log x + 4\,n)\,.$$

If we do not believe in GRH, we have to use the prime ideal theorem again : for x verifying $(C1)$,

$$|\Delta(x)| \leq \mathrm{Li}(x^\rho) + c_1 x\exp\left(-c_2\,n^{-\frac{1}{2}}\log^{\frac{1}{2}}(x)\right),$$

Consider first the term $\Delta_1 := \mathrm{Li}(x^\rho)$. Put

$$\varepsilon_1(x) = \Delta_1(x)x^{-1} - \int_x^\infty \Delta_1(t)t^{-2}dt.$$

Let c_4 be a constant such that $\mathrm{Li}(x) \leq c_4 x\log^{-1} x$ (for example $(1-\log 2)^{-1}$). One has

$$|\varepsilon_1(x)|/c_4 \leq \frac{1}{\rho\log x} + \int_x^\infty \frac{dt}{\rho\log t\; t^{2-\rho}}.$$

We can then easily bound the first error term by the following :

$$|\varepsilon_1(x)|/c_4 \leq \frac{1}{\rho\log x}\left(1 + (1-\rho)^{-1}\right).$$

We now have to deal with the second error term

$$\Delta_2(x) = c_1 x\exp\left(-c_2\,n^{-\frac{1}{2}}\log^{\frac{1}{2}}(x)\right).$$

Using Lemma 3.13, for x verifying the condition $(C2)$, we have :

$$\exp\left(-c_2\,n^{-\frac{1}{2}}\log^{\frac{1}{2}} x\right) \leq \log^{-2} x.$$

Put

$$\varepsilon_2(x) = \Delta_2(x)x^{-1} - \int_x^\infty \Delta_2(t)t^{-2}dt,$$

Thus, for x verifying the hypotheses $(C1)$ and $(C2)$ (note that condition $(C2)$ is very weak as compared to condition $(C1)$) and $x \geq e$, we obtain :

$$\varepsilon_2(x) \leq c_1(\log^{-2} x + \log^{-1} x) \leq 2c_1\log^{-1} x.$$

□

End of the proof of the Mertens theorem :

Let us start with the equality

$$\sum_{\mathcal{N}P \le x} \frac{1}{\mathcal{N}P} = \log\log x + B_K + \varepsilon_K(x).$$

One has

$$\sum_{\mathcal{N}P \le x} \log\left(\frac{\mathcal{N}P}{\mathcal{N}P - 1}\right) = \log\log x + \sum_{\mathcal{N}P > x} \left\{\log\left(1 - \frac{1}{\mathcal{N}P}\right) + \frac{1}{\mathcal{N}P}\right\} + \gamma$$
$$+ \log \mathrm{Res}_{s=1}\zeta_K(s) + \varepsilon_K(x).$$

We can bound the remainder term in the following way :

$$\left|\sum_{\mathcal{N}P > x} \left\{\log\left(1 - \frac{1}{\mathcal{N}P}\right) + \frac{1}{\mathcal{N}P}\right\}\right| \le \sum_{\mathcal{N}P > x} \frac{1}{\mathcal{N}P^2}.$$

This sum can be calculated easily under GRH using the prime ideal theorem :

$$D(x) = \sum_{\mathcal{N}P > x} \frac{1}{\mathcal{N}P^2} = \int_x^\infty \frac{dt}{t^2 \log t} + \int_x^\infty t^{-2} d\Delta(t) \le \frac{1}{x \log x} + \frac{|\Delta(x)|}{x^2} + 2\int_x^\infty |\Delta(t)| t^{-3} dt,$$

therefore

$$(GRH) \qquad \text{for any } x \ge 2 \text{ we have } D(x) \le \frac{1}{x \log x} + \frac{10\, g + 3n \log x}{3\, x\sqrt{x}} + \frac{2n}{x}.$$

Without GRH, we can use the bound for $\pi(x)$ (see [Ser81]) valid for

$$(C3) \qquad \log x \ge c_5\, g \log 2g \log\log 12g :$$
$$\pi(x) \le c_6 x \log^{-1}(x).$$

We have

$$D(x) = \sum_{\mathcal{N}P > x} \frac{1}{\mathcal{N}P^2} = \int_x^\infty \frac{d\pi(t)}{t^2}$$

and, for x sufficiently large,

$$D(x) = -\frac{\pi(x)}{x^2} + 2\int_x^\infty \pi(t) t^{-3} dt \le 2\, c_6 \int_x^\infty t^{-2} \log^{-1}(t) dt \le \frac{2\, c_6}{x \log x}.$$

Putting all this together, we obtain the following. For x verifying $(C1)$, $(C2)$ and $(C3)$

$$\sum_{\mathcal{N}P \le x} \log\left(\frac{\mathcal{N}P}{\mathcal{N}P - 1}\right) = \log\log x + \gamma + \log \mathrm{Res}_{s=1}\zeta_K(s) + \mathcal{O}\left(\frac{1}{\log x}\right) + \frac{1}{1-\rho}\mathcal{O}\left(\frac{1}{\log x}\right),$$

where the term in ρ is there only if K has an exceptional zero. The classical Mertens theorem follows by an easy application of the Taylor expansion.

Under GRH, we obtain a stronger result true for $x \ge 2$:

$$\sum_{\mathcal{N}P \le x} \log\left(\frac{\mathcal{N}P}{\mathcal{N}P - 1}\right) = \log\log x + \gamma + \log \mathrm{Res}_{s=1}\zeta_K(s) + n\, \mathcal{O}\left(\frac{\log x}{\sqrt{x}}\right) + g\, \mathcal{O}\left(\frac{1}{\sqrt{x}}\right),$$

which leads to the Mertens theorem under GRH.

3.3.2 Proof in the case of algebraic varieties

We first establish the Mertens theorem in the case of smooth absolutely irreducible projective algebraic varieties. The generalised Brauer–Siegel follows immediately from it.

For any sequence (v_n) such that the radius of convergence ρ of the series $\sum v_n t^n$ is strictly positive, put

$$\psi_{m,v}(t) = \sum_{n=1}^{+\infty} v_{mn} t^{mn},$$

and $\psi_v(t) = \psi_{1,v}(t)$. For $t < r^{-d}\rho$, we have the explicit formulae :

Theorem 3.16 (Explicit Formula)

$$\sum_{f=1}^{+\infty} f\Phi_{r^f}\psi_{f,v} = \psi_v(t) + \psi_v(r^d t) + \sum_{i=1}^{2d-1}(-1)^i \sum_{j=1}^{b_i} \psi_v(r^{\frac{i}{2}}\omega_{i,j} t)$$

Proof :[LT97] □

Choose $N \in \mathbb{N}$ et take $v_n(N) = \frac{1}{n}$ if $n \leq N$ and 0 otherwise. Applying this explicit formula with $t = r^{-d}$, we get :

$$S_0(N) = S_1(N) + S_2(N) + S_3(N),$$

where

$$\begin{aligned}
S_0(N) &= \sum_{n=1}^{N} n^{-1} r^{-dn} \sum_{m/n} m\Phi_{r^{dm}},\\
S_1(N) &= \sum_{n=1}^{N} \frac{1}{n},\\
S_2(N) &= \sum_{n=1}^{N} \frac{1}{nr^{dn}},\\
S_3(N) &= \sum_{i=1}^{2d-1}(-1)^i \sum_{j=1}^{b_i}\sum_{n=1}^{N} \frac{1}{n}(r^{\frac{i}{2}-d}\omega_{i,j})^n.
\end{aligned}$$

Lemma 3.17

$$0 \leq \sum_{f=1}^{N} \Phi_{r^f} \log \frac{r^{df}}{r^{df}-1} - S_0(N) \leq \frac{8}{N\, r^{dN/2}} + \frac{6\, b}{N\, r^{(d+\frac{1}{2})\frac{N}{2}}}.$$

Proof of the lemma: Let us first transform the expression of S_0 :

$$\begin{aligned}
S_0(N) &= \sum_{f=1}^{N} \sum_{m=1}^{E(N/f)} f\Phi_{r^f} r^{-dfm}(fm)^{-1}\\
&= \sum_{f=1}^{N} \Phi_{r^f} \sum_{m=1}^{E(N/f)} \frac{1}{r^{dfm} m}.
\end{aligned}$$

Then evaluate S_0 :

$$0 \le \sum_{f=1}^{N} \Phi_{r^f} \log \frac{r^{df}}{r^{df}-1} - S_0(N) = \sum_{f=1}^{N} \Phi_{r^f} \left(\log \frac{r^{df}}{r^{df}-1} - \sum_{m=1}^{E(N/f)} \frac{1}{r^{dfm} m} \right)$$
$$= \sum_{f=1}^{N} \Phi_{r^f} \sum_{m=E(N/f)+1}^{\infty} \frac{1}{r^{dfm} m}.$$

As $1/m \le 1/(E(N/f)+1)$, we get :

$$0 \le \sum_{f=1}^{N} \Phi_{r^f} \log \frac{r^{df}}{r^{df}-1} - S_0(N) \le \sum_{f=1}^{N} \Phi_{r^f} \frac{1}{(E(N/f)+1)(r^{df})^{E(N/f)}(r^{df}-1)}.$$

In order to deal with Φ_{r^f} we use

$$\Phi_{r^f} \le \frac{r^{df} + 1 + \sum_{i=1}^{2d-1} r^{if/2} b_i}{f}.$$

Let $b = b_X = \max_i(b_i)$. We obtain :

$$\begin{aligned}
\Phi_{r^f} &\le \frac{1}{f} \left(r^{df} + 1 + b \sum_{i=1}^{2d-1} r^{if/2} \right) \\
&\le \frac{1}{f} \left(r^{df} + 1 + b\, r^{\frac{f}{2}} \frac{r^{\frac{2d-1}{2} f} - 1}{r^{\frac{f}{2}} - 1} \right) \\
&\le \frac{1}{f} \left(r^{df} + 1 + 2\, b\, r^{df - \frac{f}{2}} \right).
\end{aligned}$$

Thus

$$0 \le \sum_{f=1}^{N} \Phi_{r^f} \log \frac{r^{df}}{r^{df}-1} - S_0(N) \le \frac{1}{N} \sum_{f=1}^{N} \frac{\left(r^{df} + 1 + 2b\, r^{df-\frac{f}{2}} \right) \left(r^{df} - 1 \right)^{-1}}{r^{df E(N/f)}}.$$

We split our sum in two in the following way : for $f > E(N/2)$ where $E(N/f) = 1$, and for $f \le E(N/2)$ where we use $f E(N/f) \le N - f$.

$$\begin{aligned}
0 \le \sum_{f=1}^{N} \Phi_{r^f} \log(\frac{r^{df}}{r^{df}-1}) - S_0(N) &\le \frac{1}{N} \sum_{f=1}^{E(N/2)} \frac{2 + 4\, b\, r^{-\frac{f}{2}}}{r^{d(N-f)}} + \frac{1}{N} \sum_{f>E(N/2)}^{N} \frac{2 + 4\, b\, r^{-\frac{f}{2}}}{r^{df}} \\
&\le \frac{8 + 12\, b\, r^{-\frac{N}{4}}}{N\, r^{dN/2}}.
\end{aligned}$$

We finally obtain the following inequality :

$$0 \le \sum_{f=1}^{N} \Phi_{r^f} \log \frac{r^{df}}{r^{df}-1} - S_0(N) \le \frac{8}{N\, r^{dN/2}} + \frac{6\, b}{N\, r^{(d+\frac{1}{2})\frac{N}{2}}}.$$

■

In order to estimate S_1 we use the following well-known inequality ([HW79]) :

Lemma 3.18

$$\frac{1}{N(N+1)} \leq S_1(N) - \log N - \gamma \leq \frac{1}{N}.$$

Lemma 3.19

$$0 \leq \log \frac{r^d}{r^d-1} - S_2(N) = \sum_{n=N+1}^{\infty} \frac{1}{nr^{dn}} \leq \frac{1}{r^{dN}(N+1)(r^d-1)}.$$

Proof of the lemma: S_2 is the partial summation of the entire function $\log \frac{r^d}{r^d-1}$. The inequality comes from the estimation of the remainder term. ■

Let us recall first that :

$$\log \mathrm{Res}_{s=d}(\log r\, \zeta(s)) - \log \frac{r^d}{r^d-1} = \sum_{i=1}^{2d-1} (-1)^{i+1} \sum_{j=1}^{b_i} \log \left(1 - r^{\frac{i}{2}-d}\omega_{i,j}\right).$$

Compute now S_3 :

Lemma 3.20

$$|S_3(N) - \sum_{i=1}^{2d-1} (-1)^{i+1} \sum_{j=1}^{b_i} \log \left(1 - r^{\frac{i}{2}-d}\omega_{i,j}\right)| \leq \frac{b}{(r^{\frac{1}{2}}-1)(N+1)(r^{\frac{N}{2}}-1)}.$$

Proof of the lemma:

$$|S_3(N) - \sum_{i=1}^{2d-1} (-1)^{i+1} \sum_{j=1}^{b_i} \log \left(1 - r^{\frac{i}{2}-d}\omega_{i,j}\right)| = |\sum_{i=1}^{2d-1} (-1)^{i} \sum_{j=1}^{b_i} \sum_{n=N+1}^{\infty} \frac{1}{n}(r^{\frac{i}{2}-d}\omega_{i,j})^n|,$$

and therefore

$$\begin{aligned}
|S_3(N) - \sum_{i=1}^{2d-1} (-1)^{i+1} \sum_{j=1}^{b_i} \log \left(1 - r^{\frac{i}{2}-d}\omega_{i,j}\right)| &\leq \sum_{i=1}^{2d-1} \sum_{j=1}^{b_i} \frac{1}{N+1} \sum_{n=N+1}^{\infty} (r^{\frac{i}{2}-d})^n, \\
&\leq \frac{1}{N+1} \sum_{i=1}^{2d-1} b_i (r^{\frac{i}{2}-d})^{N+1} (1 - r^{\frac{i}{2}-d})^{-1}, \\
&\leq \frac{b}{(r^{\frac{1}{2}}-1)(N+1)r^{dN}} \sum_{i=1}^{2d-1} r^{\frac{iN}{2}},
\end{aligned}$$

and finally :

$$|S_3(N) - \sum_{i=1}^{2d-1} (-1)^{i+1} \sum_{j=1}^{b_i} \log \left(1 - r^{\frac{i}{2}-d}\omega_{i,j}\right)| \leq \frac{b}{(r^{\frac{1}{2}}-1)(N+1)(r^{\frac{N}{2}}-1)}.$$

■

Putting everything together :

We deduce then, that for N big enough,

$$\log \prod_{f=1}^{N} \left(1 - \frac{1}{r^{df}}\right)^{\Phi_{rf}} = -\log N - \gamma + \log\left(1 - \frac{1}{r^d}\right) - \log\left(1 - \frac{1}{r^d}\right) - \log\left(\log r \mathrm{Res}_{s=d}\zeta_X\right)$$

$$+\mathcal{O}\left(\frac{1}{N}\right) + b\,\mathcal{O}\left(\frac{r^{\frac{-N}{2}}}{N}\right),$$

where the constant involved in $\mathcal{O}$ does not depend on K. $\square$

3.4 Proof of the generalised BS theorem

3.4.1 Without GRH

If we do not believe in the generalised Riemann hypothesis, we have to take into account the conditions on x which forbid us to take the limit. Consider an asymptotically exact family (K_i) of number fields, and divide it into three subfamilies. The first one consists in all the fields that have no exceptional zeroes, we include in the second one the fields that do have exceptional zeroes but no Siegel zero, and the last one contains the fields that have a Siegel zero. If one of them is finite, we omit it.

Let us focus on the second and the third families, the case of the first one being much easier because of the absence of the ρ-term (or take $\rho = 0$ in the following). Let us specialise the Mertens theorem in $x = e^{C\,n\,g^2(1-\rho)^{-1}}$, where C is big enough to allow x verify all the three conditions. Thus, for g big enough and M an explicit constant :

$$\left| \sum_{q \le e^{C\,n\,g^2(1-\rho)^{-1}}} \frac{\Phi_q}{g} \log\left(\frac{q}{q-1}\right) - \frac{\log \varkappa}{g} \right| \le M\frac{\log g}{g} - \frac{\log(1-\rho)}{g}.$$

Lemma 3.21 *Consider the family (K_i) and its exceptional zeroes ρ_i. Suppose that*

$$\lim_i \log(1-\rho_i)/g_i = 0.$$

Then κ exists and we have

$$\kappa = \sum_q \phi_q \log \frac{q}{q-1}.$$

Let us assume the lemma. Look first at the second subfamily still denoted by (K_i). Each ζ_{K_i} has an exceptional zero verifying $1-(8g)^{-1} \le \rho < 1-(32g)^{-1}$, thus $(1-\rho)^{-1} \le 32g$. Taking the logarithm, we see that this family verifies the condition of the lemma.

The case of the third subfamily, which is still denoted by (K_i) for the sake of commodity, is not so easy, because ρ can go very close to 1. In order to control the magnitude of the term in ρ, we need to assume that the fields are almost normal (or some additional condition as below). Indeed, thanks to Stark we know that a Siegel zero ρ of an almost normal number field K is also a Siegel zero of a subextension of K of degree 2 over $\mathbb{Q}$ (see [Sta74]). In addition, we can estimate $(1-\rho)^{-1}$ as follows [Lou01] :

Lemma 3.22 *Let K be a number field of degree $n_K > 1$. Then*

$$\frac{1}{1-\rho_K} \leq \varkappa_K^{-1} \left(\frac{g_K}{n_K}\right)^{n_K}.$$

Let (k_i) be a family of quadratic extensions of $\mathbb{Q}$ having the same Siegel zeroes as (K_i) and let us apply this lemma :

$$-\log(1-\rho_{K_i}) = -\log(1-\rho_{k_i}) \leq -\log \varkappa_{k_i} + 2\log\left(\frac{g_{k_i}}{2}\right).$$

Thus we obtain

$$0 < -\frac{\log(1-\rho_{K_i})}{g_{K_i}} \leq -\frac{\log \varkappa_{k_i}}{g_{K_i}} + 2g_{K_i}^{-1}\log\frac{g_{k_i}}{2}.$$

As $k_i \subset K_i$, $g_{K_i} \geq g_{k_i}$; the first and the last term of the right side of the inequality tend to zero with i. The second term, if positive, can be bounded by $g_{k_i}^{-1}\log\kappa_i$ and we use the classical Brauer–Siegel theorem for quadratic fields which says that it tends to 0. We then apply the lemma to deduce the generalised Brauer–Siegel theorem.

We still have to prove the first lemma.
Proof of the lemma: Put

$$f_g(q) = \frac{\Phi_q}{g}\log\left(\frac{q}{q-1}\right)\delta_g(q),$$

where $\delta_g(q) = 1$ if $q \leq e^{C\,n\,g^2(1-\rho)^{-1}}$, 0 otherwise. Now let the genus tend to infinity (g_{K_i} being g_i again). As

$$\sup_{i>>1}\sum_q f_{g_i}(q) \leq \sup_i \frac{\log\varkappa_{K_i}}{g_i} + 1,$$

this last quantity being well defined because of basic inequality of [TV02], and we can apply the Fatou lemma, and obtain :

$$\sum_q \phi_q \log\left(\frac{q}{q-1}\right) = \sum_q \liminf_{i\to\infty} f_{g_i}(q) \leq \liminf_{i\to\infty}\sum_q f_{g_i}(q) = \liminf_{i\to\infty}\frac{\log\varkappa_{K_i}}{g_i}.$$

Combining this result with the Brauer–Siegel inequality (3.3), we deduce the existence of the limit of $\frac{\log\varkappa_{K_i}}{g_i}$, which equals $\sum_q \phi_q \log\left(\frac{q}{q-1}\right)$ ■

Remark that in the case of the first subfamily, the proof becomes easier, because we do not have to deal with the ρ-term. The bound in the Mertens theorem is only in $\log g/g$. Specialising in $x = e^{C\,n\,g^2}$ instead, and suppressing the ρ-term in $f_g(q)$ ($q > e^{C\,n\,g^2}$), we obtain the generalised Brauer–Siegel theorem. □

Let us now prove Proposition 3.8 :
i. Recall the following key-lemma of Stark.

Lemma 3.23 ([Sta74](lemma 8)) *Let k be a number field of degree $n_k > 1$. Assume that there is a $\beta \in \mathbb{R}$ such that*

$$1 - \frac{1}{8n_k!g_k} \leq \beta < 1$$

and $\zeta_k(\beta) = 0$. Then there is a quadratic subfield F of k such that $\zeta_F(\beta) = 0$.

Assume as before that (K_i) has an infinite number of Siegel zeroes which do not verify the condition of the lemma.

Let us split as before the family (K_i) into three subfamilies. The first one containing the fields that do not have an exceptional zero, the second one consisting in the fields that have zeroes that do not verify this lemma and the last one consisting in those whose Siegel zeroes verify the condition of the lemma. If one of these families is finite, we omit it. The first and the third cases have already been treated before, so let us consider the second subfamily. Let us call it (K_i) again. We still have to bound $g^{-1} \log \frac{1}{1-\rho}$. Their exceptional zeroes verify

$$\log \frac{1}{1-\rho} \leq 8 + \log n! + \log g.$$

As $\log n! \leq n \log n$, we deduce that

$$\frac{1}{g} \log \frac{1}{1-\rho} \leq \frac{n \log n}{g} + m \frac{\log g}{g},$$

where m is an explicit positive constant. Therefore this quantity tends to 0 and this completes the proof.

ii. Suppose now that the family (K_i) is asymptotically good, and that an infinite number of them admit a Siegel zero. Then, because of Louboutin's lemma, we obtain

$$\frac{1}{g_i} \log \frac{1}{1-\rho} \leq -\frac{\log \varkappa_i}{g_i} + \frac{n_i}{g_i} \log e \frac{g_i}{n_i}.$$

This leads to the result, since $\phi_\infty = \lim \frac{n_i}{g_i}$. □

3.4.2 Assuming GRH

In the number field case, let (K_i) be a family of fields with $g_i \to \infty$. Starting with the Mertens theorem, dividing by g_i, taking $g_i \to \infty$ (we can do it because this time there is no condition on x), we obtain the Brauer–Siegel theorem. Indeed, the last paragraph shows that the limit of $\log \varkappa_{K_i}/g_i$ exists, and the asymptotical result follow directly.

In the variety case, let (X_i) be a family of smooth absolutely irreducible projective algebraic varieties over $\mathbb{F}_r$. We now prove the result of Zykin using the bounds for Φ_{r^f} that we needed for the Mertens theorem.

Lemma 3.24 *The series*

$$\sum \phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1} \quad \textit{is convergent,}$$

Proof of the lemma: As

$$\phi_{r^m} \leq \frac{2\, r^{dm-\frac{1}{2}}}{m},$$

we have

$$\phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1} = \mathcal{O}\left(\frac{1}{m\, r^{\frac{-m}{2}}}\right).$$

The series $\sum_m \frac{1}{m\, r^{\frac{-m}{2}}}$ is convergent, thus we proved the lemma. ■

Let us prove now that

Lemma 3.25 *For any real function f of b verifying the conditions :*

$$\begin{cases} \lim\limits_{b\to\infty} f(b) = \infty, \\ \lim\limits_{b\to\infty} \dfrac{f(b)}{b} = 0, \end{cases},$$

we have

$$\lim_{b\to\infty} \frac{1}{b} \sum_{m=1}^{f(b)} \Phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1} = \sum_{m=1}^{\infty} \phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1}.$$

Proof of the lemma: For the case $d = 1$ see [Tsf92]). Let $\varepsilon > 0$. By Lemma 3.24 there is an integer $N_0 > 0$ such that, for any $m > N_0$,

$$|\sum_{m\geq N_0} \phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1}| < \frac{\varepsilon}{4}.$$

Thus we have to bound

$$|\sum_{m\leq f(b)} \frac{\Phi_{r^m}}{b} - \phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1}|.$$

Let N_1 be an integer such that

$$\sum_{m\geq N_1} \frac{1}{r^{\frac{m}{2}}} \leq \frac{\varepsilon}{32},$$

and b_1 an integer, such that, for any $b \geq b_1$,

$$\frac{f(b) - N_1 + 1 + \sum r^{-dm}}{b} \leq \frac{\varepsilon}{8}.$$

As $\log \frac{r^{dm}}{r^{dm}-1} \leq 2r^{-dm}$, we have, using the inequality on Φ_{r^m} :

$$\begin{aligned} \sum_{m=N_1}^{f(b)} |(\frac{\Phi_{r^m}}{b} - \phi_{r^m}) \log \frac{r^{dm}}{r^{dm}-1}| &\leq \sum_{m=N_1}^{f(b)} \left(|\frac{\Phi_{r^m}}{b}| + |\phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1}|\right) \\ &\leq 2 \sum_{m=N_1}^{f(b)} (\frac{r^{dm}+1}{b} + 2 \sum_{i=1}^{2d-1} r^{\frac{if}{2}}) r^{-dm} \\ &\leq 2 \frac{f(b) - N_1 + 1 + \sum r^{-dm}}{b} + 8 \sum_{m\geq N_1} r^{-\frac{m}{2}} \\ &\leq \frac{\varepsilon}{2}, \end{aligned}$$

for any $b \geq b_1$. Now, by definition of ϕ_{r^m}, there is some integer b_2, such that, for any $b \geq b_2$,

$$\sum_{m=1}^{N_1} \Big| \frac{\Phi_{r^m}}{b} - \phi_{r^m} \Big| \log \frac{r^{dm}}{r^{dm}-1} \leq \frac{\varepsilon}{4}.$$

Because of the first condition on f, there is an integer b_0 such that, for any $b \geq b_0$, $f(b) > \max\{N_0, N_1\}$. For any $b \geq \max\{b_0, b_1, b_2\}$, we have

$$\left| \frac{1}{b} \sum_{m=1}^{f(b)} \Phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1} - \sum_{m=1}^{\infty} \phi_{r^m} \log \frac{r^{dm}}{r^{dm}-1} \right| \leq \varepsilon.$$

■

Using this result in the Mertens theorem (put $N = f(b)$, divide by b and make $b \to \infty$) gives us that the limit of $\log \varkappa_{X_i}/b_{X_i}$ exists. We divide now by b_{X_i} (for any N) in the Mertens theorem and make $b_{X_i} \to \infty$ in order to obtain our version of the Brauer–Siegel theorem for varieties.

One could likely obtain similar results in the non-smooth case, using the virtual Betti numbers. We hope to do this in further work. Let us conclude by the following remark. The explicit Mertens theorem is much more interesting than its application to the generalised Brauer–Siegel theorem, because it contains more information, and can be therefore useful, for example if we would like to look at the problem in the classical way, putting all our attention to the residues $\varkappa_i$ instead of to the convergent series, and consider the limit of $\varkappa_i/g_i$ in the tower.

Acknowledgements

I would like to thank Gilles Lachaud, Michael Tsfasman and Alexei Zykin for very useful discussions, Mireille Car for letting me know her results on the Mertens theorem and Michel Balazard for having pointed out some mistakes in the first version of this paper.

Développements futurs

Le lecteur avisé se sera rendu compte que bien des problèmes restent ouverts après cette étude, et nous allons nous intéresser ici au travail qu'il conviendra de faire à l'avenir. Nous n'avons en effet pas répondu aux questions qui se posèrent concernant l'ensemble Φ. Nous ne pouvons ainsi toujours rien dire quant à sa topologie, et cela représentera le fil conducteur de nos futures recherches. Dans cette direction, nous nous efforcerons d'abord d'obtenir des exemples de corps dont on parvient à contrôler le support. Ainsi, on a pu construire des corps globaux infinis ayant un nombre fini donné d'invariants non nuls, d'autres ayant ces invariants nuls. Le problème se pose de savoir si on peut mêler ceux-ci, et montrer des résultats analogues à ceux de Labute et Schmidt pour les p-extensions où un ensemble de places est totalement décomposé. On peut également se demander si on peut montrer l'annulation d'un ensemble de places de densité nulle, et ainsi on obtiendrait un corps global infini asymptotiquement bon ayant tous ses invariants non-archimédiens nuls. Ces résultats récents sont également encourageants, dans la mesure où ils fournissent des exemples de groupes de Galois de corps de nombres asymptotiquement bons sans torsion, et donnent ainsi des informations sur ses invariants : ses ϕ_{p^m} sont nuls pour $m > 1$. Ce résultat est très important, car c'est sur cette voie qu'il faudrait probablement chercher les corps globaux infinis dont les défauts sont les plus faibles, parmi leurs sous-corps juste-infinis. Remarquons également qu'il apparaît comme très difficile de contrôler analytiquement les invariants pour $m > 1$ du fait que leur contribution dans les séries est finie.

Le problème de savoir si un corps global infini peut avoir un nombre infini d'invariants non nuls nous intéressera également au plus haut point. Toutefois, aucun résultat récent ne permet de construire un tel corps, et il faudrait probablement réussir à s'éloigner de la théorie du corps de classes pour y parvenir, et inventer quelque chose de révolutionnaire. En effet, en utilisant ces constructions, on se rend compte qu'on ne peut imposer à la fois une ramification finie et un nombre infini de places décomposées : c'est l'un, ou l'autre.

Concernant les inégalités qui confinent l'ensemble Φ, la question de la maximalité des conditions se pose toujours, en particulier dans le cas des corps de nombres où on ne sait pas si des corps de défaut nul existent. D'autres équations devant être vérifiées par les invariants peuvent être obtenues à partir des formules explicites. On peut se demander si l'inégalité fondamentale n'est pas une relation parmi tant d'autres qui décriraient totalement l'ensemble des invariants. On peut également se demander si deux corps globaux infinis ayant le même défaut ont les mêmes invariants, et, sinon, combien d'autres défauts faut-il définir pour obtenir quelque chose d'injectif ? En particulier, est-ce qu'un nombre fini suffit ? L'étude des valeurs possibles prises par le défaut sera également au centre de futures recherches. Est-ce un intervalle, est -il dense dans [0,1] ?

Pour conclure, attirons l'attention du lecteur sur la richesse des mathématiques qui interviennent dans l'étude des corps globaux infinis, allant de la théorie analytique des nombres à la géométrie algébrique, et de ses nombreuses applications à des problèmes liés à la théorie de l'information. La beauté de cette théorie provient peut-être du fait que notre esprit ne touche pas aisément les objets, que l'existence de certains d'entre eux est très hypothétique, aiguisant ainsi notre curiosité, ou bien de la multitude de constructions, d'angles d'attaque, d'intérêts mathématiques et informatiques qui s'y mêlent. Ainsi nous ne pouvons qu'encourager quiconque voudra s'intéresser de près ou de loin aux corps globaux infinis.

Bibliographie

[AHM05] Wayne Aitken, Farshid Hajir, et Christian Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.*, (14) :855–880, 2005.

[Car] Mireille Car. Euler constants for the ring of S-integers of a function field. *to be published in Portugaliae Math.*

[FPS92] G. Frey, M. Perret, et H. Stichtenoth. On the different of abelian extensions of global fields. Dans *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 de *Lecture Notes in Math.*, pages 26–32. Springer, Berlin, 1992.

[Gol70] Larry Joel Goldstein. A generalization of the Siegel-Walfisz theorem. *Trans. Amer. Math. Soc.*, 149 :417–429, 1970.

[Gra05] Georges Gras. *Class field Theory, from theory to practice.* SMM, Springer, 2005.

[GS95] Arnaldo García et Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-Vlăduţ bound. *Invent. Math.*, 121(1) :211–222, 1995.

[GS96] Arnaldo Garcia et Henning Stichtenoth. Asymptotically good towers of function fields over finite fields. *C. R. Acad. Sci. Paris Sér. I Math.*, 322(11) :1067–1070, 1996.

[HW79] G. H. Hardy et E. M. Wright. *An introduction to the theory of numbers.* The Clarendon Press Oxford University Press, New York, fifth édition, 1979.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3) :721–724 (1982), 1981.

[Iha83] Yasutaka Ihara. How many primes decompose completely in an infinite unramified Galois extension of a global field ? *J. Math. Soc. Japan*, 35(4) :693–709, 1983.

[Koc02] Helmut Koch. *Galois theory of p-extensions.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer.

[Lab06] John Labute. Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$. *J. Reine Angew. Math.*, 596 :155–182, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics.* Springer-Verlag, New York, second édition, 1994.

[Lan02] Serge LANG. *Algebra*, volume 211 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, third édition, 2002.

[Lou01] Stéphane LOUBOUTIN. Explicit upper bounds for residues of Dedekind zeta functions and values of L-functions at $s = 1$, and explicit lower bounds for relative class numbers of CM-fields. *Canad. J. Math.*, 53(6) :1194–1222, 2001.

[LT97] Gilles LACHAUD et Michael A. TSFASMAN. Formules explicites pour le nombre de points des variétés sur un corps fini. *J. Reine Angew. Math.*, 493 :1–60, 1997.

[Neu73] Jürgen NEUKIRCH. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.*, 21 :59–116, 1973.

[Neu99] Jürgen NEUKIRCH. *Algebraic number theory*, volume 322 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Nor76] Karl K. NORTON. On the number of restricted prime factors of an integer. I. *Illinois J. Math.*, 20(4) :681–705, 1976.

[NSW00] Jürgen NEUKIRCH, Alexander SCHMIDT, et Kay WINGBERG. *Cohomology of number fields*, volume 323 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[NX98] Harald NIEDERREITER et Chaoping XING. Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound. *Math. Nachr.*, 195 :171–186, 1998.

[NX01] Harald NIEDERREITER et Chaoping XING. *Rational points on curves over finite fields theory and applications*, volume 285 de *London Mathematical Society lecture note series*. Cambridge University Press, Cambridge, 2001.

[Ros99] Michael ROSEN. A generalization of Mertens' theorem. *J. Ramanujan Math. Soc.*, 14(1) :1–19, 1999.

[Sch06] Alexander SCHMIDT. Circular sets of prime numbers and p-extensions of the rationals. *J. Reine Angew. Math.*, 596 :115–130, 2006.

[SD01] H. P. F. SWINNERTON-DYER. *A brief guide to algebraic number theory*, volume 50 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2001.

[Ser68] Jean-Pierre SERRE. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser81] Jean-Pierre SERRE. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54) :323–401, 1981.

[Ser85] Jean-Pierre SERRE. *Rational Points on Curves over Finite Fields*. Harvard University, 1985.

[Ser94] Jean-Pierre SERRE. *Cohomologie galoisienne*, volume 5 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth édition, 1994.

[Sta74] H. M. STARK. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23 :135–152, 1974.

[Sti93] Henning STICHTENOTH. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

[Sti99] Henning STICHTENOTH. The Fermat curve in characteristic p. Dans *Finite fields : theory, applications, and algorithms (Waterloo, ON, 1997)*, volume 225 de *Contemp. Math.*, pages 123–129. Amer. Math. Soc., Providence, RI, 1999.

[Tsf92] Michael A. TSFASMAN. Some remarks on the asymptotic number of points. Dans *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 de *Lecture Notes in Math.*, pages 178–192. Springer, Berlin, 1992.

[TV02] M. A. TSFASMAN et S. G. VLĂDUŢ. Infinite global fields and the generalized Brauer-Siegel theorem. *Mosc. Math. J.*, 2(2) :329–402, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.

[TVZ82] M. A. TSFASMAN, S. G. VLĂDUŢ, et Th. ZINK. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109 :21–28, 1982.

[Vin65] È. B. VINBERG. On the theorem concerning the infinite-dimensionality of an associative algebra. *Izv. Akad. Nauk SSSR Ser. Mat.*, 29 :209–214, 1965.

[Zyk05] Alexei ZYKIN. The Brauer-Siegel and Tsfasman-Vlăduţ theorems for almost normal extensions of number fields. *Mosc. Math. J.*, 5(4) :961–967, 2005.