Conjecture de brumer-stark non abélienne

Gaëlle Dejou

▶ **To cite this version:**

Gaëlle Dejou. Conjecture de brumer-stark non abélienne. Mathématiques générales [math.GM]. Université Claude Bernard - Lyon I, 2011. Français. NNT : 2011LYO10103 . tel-00618624

HAL Id: tel-00618624

https://theses.hal.science/tel-00618624

Submitted on 2 Sep 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Numéro d'ordre : 103-2011 Année 2011

Université Claude Bernard - Lyon 1

Institut Camille Jordan - CNRS UMR 5208
École doctorale Infomaths

Thèse de l'université de Lyon

pour l'obtention du

Diplôme de doctorat
Spécialité : mathématiques pures
(arrêté du 7 août 2006)

présentée par

Gaelle DEJOU

Conjecture de Brumer-Stark non abélienne

Thèse dirigée par Xavier-François Roblot
soutenue publiquement le 24 juin 2011

Après avis de :

Christian MAIRE	Université de Franche-Comté	Rapporteur
Brett TANGEDAL	University of North Carolina Greensboro	Rapporteur

Devant le jury composé de :

Jean-Marc COUVEIGNES	Université Toulouse II	Examinateur
Christophe DELAUNAY	Université Lyon 1	Examinateur
Laurent HABSIEGER	Université Lyon 1	Examinateur
Christian MAIRE	Université de Franche-Comté	Rapporteur
Xavier-François ROBLOT	Tokyo Institute of Technology	Directeur de thèse
David SOLOMON	King's College London	Examinateur

Gaelle Dejou

CONJECTURE DE BRUMER-STARK NON ABÉLIENNE

G. Dejou

CONJECTURE DE BRUMER-STARK NON ABÉLIENNE

Gaelle Dejou

Résumé. — La recherche d'annulateurs du groupe des classes d'idéaux d'une extension abélienne de $\mathbb{Q}$ est un sujet classique et remonte à des travaux de Kummer et Stickelberger. La conjecture de Brumer-Stark porte sur les extensions abéliennes de corps de nombres et prédit qu'un élément de l'anneau de groupe du groupe de Galois, appelé élément de Brumer-Stickelberger, est un annulateur du groupe des classes de l'extension. De plus, elle stipule que les générateurs des idéaux principaux obtenus possèdent des propriétés bien particulières.

Cette thèse est dédiée à la généralisation de cette conjecture aux extensions de corps de nombres galoisiennes mais non abéliennes.

Dans un premier temps, nous nous focalisons sur l'étude de l'analogue non abélien de l'élément de Brumer, nécessaire à l'établissement d'une conjecture non abélienne.

La seconde partie est consacrée à l'énoncé de la conjecture de Brumer-Stark non abélienne et à ses reformulations, ainsi qu'aux propriétés qu'elle vérifie. Nous nous intéressons notamment aux propriétés de changement d'extension.

Nous étudions ensuite le cas spécifique des extensions dont le groupe de Galois possède un sous-groupe abélien H distingué d'indice premier. Sous la validité de la conjecture de Brumer-Stark associée à certaines extensions abéliennes, nous en déduisons deux résultats suivant la parité du cardinal de H : dans le cas impair, nous démontrons la conjecture de Brumer-Stark non abélienne, et dans le cas pair, nous établissons un résultat d'abélianité permettant d'obtenir, sous des hypothèses supplémentaires, la conjecture non abélienne.

Enfin nous effectuons, à l'aide du logiciel PARI-GP, des vérifications numériques de la conjecture non abélienne permettant de démontrer cette conjecture dans les exemples testés.

Mots clefs. — Théorie algébrique des nombres, Extensions non abéliennes, Conjecture de Brumer-Stark, Fonctions L d'Artin, Annulateurs du groupe des classes.

Abstract. — Finding annihilators of the ideal class group of an abelian extension of $\mathbb{Q}$ is a classical subject which goes back to work of Kummer and Stickelberger. The Brumer-Stark conjecture deals with abelian extensions of number fields and predicts that a group ring element, called the Brumer-Stickelberger element, annihilates the ideal class group of the extension under consideration. Moreover it specifies that the generators thus obtained have special properties.

The aim of this work is to generalize this conjecture to non-abelian Galois extensions.

We first focus on the study of a non-abelian analogue of the Brumer element, necessary to establish a non-abelian generalization of the conjecture.

The second part is devoted to the statement of our non-abelian conjecture, and the properties it satisfies. We are particularly interested in extension change properties.

We then study the specific case of extensions whose Galois group has an abelian normal subgroup H of prime index. If the Brumer-Stark conjecture associated to certain abelian subextensions holds, we prove two results according to the parity of the cardinal of H : in the odd case, we get the non-abelian Brumer-Stark conjecture, and in the even case, we establish an abelianity result implying under additional hypotheses the proof of the non-abelian conjecture.

Thanks to PARI-GP, we finally do some numerical verifications of the non-abelian conjecture, proving its validity in the tested examples.

Keywords. — Algebraic number theory, Non abelian extensions, Brumer-Stark conjecture, Artin L functions, Ideal class group annihilators.

REMERCIEMENTS

Au moment d'achever ma thèse, je souhaite remercier toutes les personnes qui ont contribué d'une manière ou d'une autre à l'aboutissement de ce travail.

Je tiens à exprimer en tout premier lieu mon immense gratitude envers mon directeur de thèse Xavier-François Roblot, qui a su à la fois me laisser toute liberté dans mes choix mathématiques, tout en étant présent et disponible pour me guider dans le monde de la recherche, ceci malgré la distance. En plus de sa patience et de sa gentillesse, ses nombreux conseils et suggestions m'ont toujours été d'une aide plus que précieuse au cours de ces années.

Je suis très sensible à l'honneur que m'ont fait Christian Maire et Brett Tangedal en acceptant d'être rapporteurs de ma thèse. Je suis d'autant plus reconnaissante envers ce dernier que ma thèse est rédigée en français. Je les remercie sincèrement pour la qualité de leur relecture ainsi que pour les commentaires effectués sur mon travail qui m'ont beaucoup touchée.

Je suis très heureuse que Jean-Marc Couveignes, Laurent Habsieger et David Solomon aient accepté de faire partie de mon jury de soutenance, et aient pris la peine de se déplacer pour l'occasion.

Je me dois de réserver une place spéciale à Christophe Delaunay, qui non seulement a accepté de faire partie de mon jury, mais dont la générosité et les traits d'humour m'ont permis de me sentir à l'aise aussi bien au sein du laboratoire que lors des conférences. Par ailleurs, ses remarques pertinentes sur le manuscrit de la thèse ont grandement amélioré son contenu.

Je dois aussi beaucoup aux doctorants de l'Institut Camille Jordan pour l'ambiance de travail agréable qui y règne. Tout d'abord je remercie mes collègues de bureau Alina, Fred, Ioana, Mickaël, Thomas, pour tous les moments studieux passés ensemble, mais aussi pour les moments de détente en dehors de l'université. Merci aussi à tous les autres Alain, Alexis, Amélie, Élodie, J-B, Julien, Marianne, Rémi, Vladimir... Je m'adresse en particulier à Laurent, Nico et Polina, qui ont pris une place beaucoup plus importante dans ma vie.

J'ai une pensée toute particulière pour ma famille, et plus spécialement pour mes parents et ma soeur, qui ont su me soutenir tout au long de mes études et qui m'ont aidée à ne jamais baisser les bras.

J'en profite pour adresser toute ma sympathie à mes amis de Lyon et d'ailleurs qui ont toujours été là pour moi.

Mes derniers remerciements et non les moindres sont pour Loïc, pour son amour et son soutien sans faille même dans les moments les plus difficiles, et pour tellement d'autres raisons qu'elles rempliraient des livres entiers...

TABLE DES MATIÈRES

Remerciements v

Introduction ix

0. Quelques notations et résultats 1
0.1. Représentations linéaires des groupes finis 1
0.2. Corps de nombres 3
0.2.1. Corps à multiplication complexe 3
0.2.2. Congruence $\mod^*$ 4
0.2.3. Théorème de densité de Čebotarev 4

1. Conjecture de Brumer-Stark abélienne 7
1.1. Élément de Brumer-Stickelberger 7
1.2. Énoncé de la conjecture de Brumer-Stark 9
1.3. État actuel de la conjecture de Brumer-Stark 11

2. Élément de Brumer non abélien 15
2.1. Fonctions L d'Artin non abéliennes 15
2.2. Définition de l'élément de Brumer non abélien 17
2.2.1. Caractérisation et propriétés de $\theta_{K/k,S}$ 17
2.2.2. Dépendance de l'élément de Brumer par rapport à S 19
2.3. Des annulateurs explicites de $\theta_{K/k,S}$ 20
2.3.1. Dimension du sous-espace stable par G 21
2.3.2. Application à la recherche d'annulateurs 22
2.4. Rationnalité des coefficients de $\theta_{K/k,S}$ 24
2.4.1. Conjecture principale de Stark de rang zéro 24
2.4.2. Démonstration de la rationnalité des coefficients de $\theta_{K/k,S}$ 26
2.5. Dénominateur de $\theta_{K/k,S}$ 27

3. Conjecture de Brumer-Stark non abélienne 31
3.1. Énoncé de la conjecture de Brumer-Stark non abélienne 31
3.1.1. Des équivalences utiles 31
3.1.2. Énoncé de la conjecture 37
3.2. Quelques propriétés du groupe des idéaux fractionnaires vérifiant $BS_{\text{non ab}}(K/k,S)$ 43
3.3. Dépendance de la conjecture par rapport au corps K 45
3.3.1. Cas où B est abélien 45

3.3.2. Cas où B est non abélien 48
3.4. Dépendance de la conjecture par rapport à l'ensemble S 51

4. Groupes possédant un sous-groupe abélien distingué d'indice premier 55
4.1. Écriture de $\theta_{K/k,S}$ à l'aide d'éléments de Brumer-Stickelberger abéliens 55
4.1.1. Étude des caractères irréductibles de G 55
4.1.2. Expression explicite de $\theta_{K/k,S}$ 58
4.2. Dénominateur de l'élément de Brumer 63
4.2.1. Calcul de m_G 64
4.2.2. Vérification d'une partie du postulat 67
4.3. Cas particulier où H est de cardinal impair 68
4.4. Un résultat d'abélianité dans le cas où H est de cardinal pair 69
4.4.1. Énoncé et démonstration du résultat 70
4.4.2. Cas impliquant la validité de $BS_{\text{non ab}}(K/k, S)$ 72

5. Quelques vérifications numériques 77
5.1. Décomposition rationnelle de $Z(\mathbb{Q}[G])$ 77
5.2. Cas où $\mathrm{Gal}(K/k)$ est isomorphe à $SL_2(\mathbb{F}_3)$ 78
5.2.1. Étude théorique de l'élément de Brumer 78
5.2.2. Un exemple détaillé 81
5.2.3. Résultats obtenus 83

Bibliographie 87

INTRODUCTION

Les conjectures de Stark portent sur les valeurs en $s = 0$ du terme dominant des fonctions L d'Artin de corps de nombres. Dans le cas où l'extension K/k considérée est abélienne, la conjecture correspondant au cas où les fonctions L ne sont pas toutes nulles s'appelle la conjecture de Brumer-Stark. Cette conjecture, due à Tate, combine une conjecture non publiée de Brumer avec des idées de Stark et prédit que les fonctions L en $s = 0$ possèdent des informations spécifiques sur le corps K. Elle stipule qu'un élément de l'anneau de groupe du groupe de Galois de l'extension, appelé élément de Brumer-Stickelberger, annule le groupe des classes de K. De surcroît, elle prévoit que les idéaux principaux obtenus (grâce à l'action de l'élément de Brumer-Stickelberger) possèdent des générateurs vérifiant des propriétés particulières, entraînant notamment une condition d'abélianité sur le corps de base k. Elle peut être vue comme une généralisation du théorème de Stickelberger concernant la factorisation des sommes de Gauss dans les corps cyclotomiques.

L'objet principal de cette thèse est la généralisation de la conjecture de Brumer-Stark au cas où l'extension K/k est galoisienne mais non abélienne. Il s'agit d'établir un énoncé satisfaisant de la conjecture non abélienne qui soit compatible avec la conjecture abélienne, puis de la tester de manière théorique et expérimentale. Ce travail est organisé de la manière suivante.

Après avoir rappelé la conjecture de Brumer-Stark abélienne, ainsi que les avancées actuelles concernant sa démonstration, nous étudions dans un deuxième temps l'analogue non abélien de l'élément de Brumer-Stickelberger défini par Hayes dans [**Hay04**], associé à l'extension K/k et à un certain ensemble S de places de k. Nous nous intéressons aux différentes propriétés de cet élément, appelé élément de Brumer, et analysons leurs similitudes avec les propriétés vérifiées dans le cas abélien. Nous démontrons que l'élément de Brumer, nécessaire pour la généralisation de la conjecture, est aussi rationnel dans le cas général. Une question centrale est de réussir à déterminer le dénominateur de cet élément, ce qui est essentiel pour pouvoir appliquer l'élément de Brumer aux idéaux fractionnaires du corps K. Nous établissons une conjecture sur ce dénominateur, que nous démontrons dans certains cas théoriques et qui est confirmée dans toutes les vérifications expérimentales que nous avons effectuées.

Le troisième chapitre est consacré à l'énoncé de la conjecture de Brumer-Stark non abélienne, ainsi qu'à l'étude de ses propriétés "fonctorielles". Une fois obtenu

le dénominateur de l'élément de Brumer, la partie concernant l'annulation du groupe des classes de K par cet élément se généralise naturellement. En revanche, l'adaptation des idées de Stark au cas non abélien est moins directe. L'extension K/k considérée n'étant pas abélienne, la condition d'abélianité donnée par la conjecture de Brumer-Stark abélienne ne peut pas être réalisée. Nous remplaçons cette condition d'abélianité par une condition dite "de centralité", faisant intervenir des extensions centrales de K/k. Nous établissons plusieurs formulations équivalentes de notre conjecture de Brumer-Stark non abélienne, similaires à celles obtenues par Tate dans le cas abélien ([**Tat81**]).

Nous démontrons ensuite que cette conjecture vérifie des propriétés semblables à celles du cas abélien. En particulier nous prouvons, dans le cas où le corps K est de type CM, que les idéaux principaux satisfont la conjecture, ce qui nous permet de considérer celle-ci comme une question de classes d'idéaux. Enfin, nous terminons le chapitre par l'étude de la dépendance de la conjecture par rapport au corps K et à l'ensemble de places S de k choisis.

Dans le chapitre suivant, nous nous concentrons sur les extensions de corps de nombres dont le groupe de Galois possède un sous-groupe abélien distingué H d'indice premier. L'examen des caractères irréductibles de ce type de groupe permet d'obtenir une expression explicite de l'élément de Brumer en fonction d'éléments de Brumer-Stickelberger associés à certaines sous-extensions abéliennes de K/k. Cette écriture donne aussi la preuve d'une partie de notre conjecture sur le dénominateur de l'élément de Brumer pour de telles extensions. Nous distinguons ensuite deux cas suivant la parité du cardinal du groupe H. Si H est de cardinal impair, nous prouvons la validité de la conjecture non abélienne, sous la condition que la conjecture de Brumer-Stark associée à une sous-extension abélienne soit vraie. Ce résultat implique en particulier la véracité de la conjecture non abélienne pour toutes les extensions de groupe de Galois diédral d'ordre $2n$ avec n impair. Dans le cas où H est de cardinal pair, nous établissons un résultat d'abélianité, qui entraîne sous certaines hypothèses la validité de la conjecture non abélienne, ceci en supposant une nouvelle fois que la conjecture abélienne associée à des sous-extensions particulières de K/k est vraie.

Le dernier chapitre est dédié à la mise en place de vérifications expérimentales de notre conjecture non abélienne pour des extensions de groupe de Galois isomorphe à $SL_2(\mathbb{F}_3)$, groupe n'appartenant pas à la famille considérée dans le chapitre précédent. À l'aide du logiciel PARI-GP, nous démontrons la validité de la conjecture pour certaines extensions. De plus, ces exemples numériques permettent d'observer que le dénominateur conjecturé de l'élément de Brumer, bien que pouvant être non optimal en ce qui concerne l'intégralité de ce dernier, possède toutefois des facteurs nécessaires à l'annulation du groupe des classes de K.

Pour conclure, nous donnons ici quelques perspectives de recherche que l'on pourra poursuivre. Il reste à démontrer la validité de notre hypothèse sur le dénominateur de l'élément de Brumer. Bien que ce soit le cas dans les exemples théoriques et expérimentaux que nous avons considérés, il se pourrait que ce dénominateur ne soit pas optimal. Il faudrait alors trouver l'élément optimum à la fois pour l'intégralité de l'élément de Brumer mais aussi pour obtenir la conjecture non abélienne tout en restant compatible avec les connaissances du cas abélien.

Il serait aussi intéressant d'explorer plus en détails les relations entre l'élément de Brumer non abélien et les éléments de Brumer-Stickelberger associés aux sous-extensions abéliennes de K/k. Ceci pourrait permettre par exemple d'adapter les progrès récents effectués sur la conjecture abélienne à la conjecture non abélienne. Inversement des avancées sur la démonstration de cette dernière pourraient permettre d'obtenir des résultats concernant la conjecture abélienne.

Enfin il reste bien évidemment à démontrer la conjecture de Brumer-Stark non abélienne. Si cette perspective est sans doute trop ambitieuse à l'heure actuelle dans le cas général, il faudrait au moins démontrer la conjecture pour le plus grand nombre d'extensions possible. Les vérifications numériques effectuées lors de ce travail ne faisant apparaître que des extensions pour lesquelles la condition de centralité se vérifie de manière immédiate, il serait utile d'utiliser des outils algorithmiques afin de tester la conjecture non abélienne pour de nombreuses extensions faisant intervenir des situations plus complexes.

CHAPITRE 0

QUELQUES NOTATIONS ET RÉSULTATS

On commence par effectuer une synthèse des résultats et notations utilisés dans la suite.

0.1. Représentations linéaires des groupes finis

Les références pour cette section sont [**Ser78**] et [**CR06**]. Soit G un groupe fini, de neutre noté 1 et de loi de composition notée multiplicativement. Une *représentation linéaire* de G dans V est un morphisme de groupes ρ de G dans $GL(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie. On appelle la dimension $\dim_{\mathbb{C}} V$ le *degré* de la représentation ρ. On dit que deux représentations linéaires (ρ, V) et (ρ', V') de G sont *isomorphes* s'il existe un isomorphisme $\tau : V \longrightarrow V'$ vérifiant pour tout g dans G, $\tau \circ \rho(g) = \rho'(g) \circ \tau$. Une *sous-représentation* de (ρ, V) est une représentation (η, W) où W est un sous-espace de V stable sous l'action de G donnée par ρ et pour tout $g \in G$, $\eta(g)$ est la restriction de $\rho(g)$ à W. La représentation $\rho : G \longrightarrow GL(V)$ est dite *irréductible* si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G. On peut décomposer toute représentation de G en une somme directe de représentations irréductibles.

Le *caractère de la représentation* ρ est la fonction χ_ρ de G dans $\mathbb{C}$, définie pour tout g dans G par $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$. On dit que le caractère χ est irréductible s'il provient d'une représentation irréductible de G. Le groupe G ne possède qu'un nombre fini de caractères irréductibles, égal au nombre de classes de conjugaison de G. Dans la suite, on notera $\widehat{G}$ l'ensemble des caractères irréductibles de G. Pour deux caractères χ, ψ de G, on définit le produit scalaire

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}).$$

Les caractères irréductibles sont caractérisés par ce produit scalaire : un caractère χ de G est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$. De plus, les caractères irréductibles de G sont deux à deux orthogonaux pour ce produit scalaire. Il découle de ces relations d'orthogonalité que deux représentations sont isomorphes si et seulement si elles ont le même caractère. En particulier, il n'y a qu'un nombre fini de représentations irréductibles à isomorphisme près. Si χ est le caractère

d'une représentation irréductible V, et ψ le caractère d'une représentation W de G, la quantité $\langle \chi, \psi \rangle$ représente le nombre de fois qu'une représentation isomorphe à V apparaît dans la décomposition en représentations irréductibles de W.

On peut obtenir différents renseignements sur les degrés des représentations irréductibles de G. On mentionne les relations suivantes, obtenues à partir de la décomposition en représentations irréductibles de la représentation régulière de G :

$$\sum_{\chi \in \widehat{G}} n_\chi^2 = |G|, \tag{0.1.1}$$

$$\sum_{\chi \in \widehat{G}} n_\chi \chi(g) = 0 \quad \text{pour tout } g \in G, g \neq 1, \tag{0.1.2}$$

où n_χ désigne le degré de la représentation dont χ est le caractère. En outre, les degrés des représentations irréductibles de G divisent le cardinal de G. On a même un résultat plus précis de divisibilité : si G possède un sous-groupe abélien distingué noté H, le degré de toute représentation irréductible de G divise l'indice $(G : H)$ de H dans G. Mentionnons au passage que le groupe G est abélien si et seulement si ses représentations irréductibles sont toutes de degré 1.

Soit $\rho : G \longrightarrow GL(V)$ une représentation linéaire de G et H un sous-groupe de G. Soit $\eta : H \longrightarrow GL(W)$ une sous-représentation de la restriction de ρ à H. On note G/H l'ensemble des classes à gauche modulo H. Pour un élément g de G, $\rho(g)(W)$ ne dépend que de la classe à gauche gH de G. On définit alors, pour toute classe à gauche σ modulo H, un sous-espace W_σ de V comme étant $\rho(g)(W)$, pour un élément quelconque g de σ. On dit que la représentation ρ de G dans V est *induite* par la représentation η de H dans W si on a l'identité

$$V = \bigoplus_{\sigma \in G/H} W_\sigma.$$

Dans ce cas, on a en particulier l'égalité $\dim_{\mathbb{C}} V = (G : H) \dim_{\mathbb{C}} W$. Pour toute représentation linéaire (η, W) de H, il existe une unique représentation linéaire (ρ, V) de G, à isomorphisme près, qui est induite par (η, W) ; on la note $\mathrm{Ind}_H^G(W)$. Le caractère de la représentation $\mathrm{Ind}_H^G(W)$ est le *caractère induit* par le caractère χ_η défini pour tout g dans G par

$$\mathrm{Ind}_H^G(\chi_\eta)(g) = \sum_{\substack{r \in R \\ r^{-1} g r \in H}} \chi_\eta(r^{-1} g r),$$

où R désigne un système de représentants des classes à gauche modulo H. La formule de réciprocité de Frobenius établit un lien entre les caractères induits de G et les caractères restreints à H.

Proposition 0.1 **(Formule de réciprocité de Frobenius)**
Soient χ un caractère de G et φ un caractère de H. On a l'identité

$$\langle \chi, \mathrm{Ind}_H^G(\varphi) \rangle_G = \langle \chi_{|H}, \varphi \rangle_H,$$

où $\chi_{|H}$ désigne la restriction de χ à H.

Le théorème suivant joue un rôle essentiel dans beaucoup d'applications de la théorie des représentations : il permet de ramener une question portant sur un caractère χ arbitraire au cas particulier où χ est de degré 1 (*i.e* χ provient d'un sous-groupe cyclique).

***Théorème 0.2* (Brauer).** — *Tout caractère de G est combinaison linéaire à coefficients entiers de caractères monomiaux, i.e induits par un caractère de degré 1 d'un sous-groupe convenable de G.*

Les coefficients intervenant dans la décomposition de Brauer précédente sont des entiers positifs ou négatifs. Il n'est pas possible en général d'écrire un caractère donné comme combinaison linéaire à coefficients entiers positifs de caractères monomiaux.

0.2. Corps de nombres

Soit K un corps de nombres, *i.e* une extension finie de $\mathbb{Q}$. On désigne par $\mathcal{O}_K$ l'anneau des entiers de K. On note $\mu(K)$ le groupe des racines de l'unité dans K et w_K son cardinal. À chaque plongement j de K dans $\mathbb{C}$, on associe une place infinie (ou archimédienne) notée $|.|_j$. Le *groupe des classes* de K, noté Cl_K, est le quotient des idéaux fractionnaires non nuls de K par les idéaux principaux non nuls. Pour tout idéal fractionnaire $\mathfrak{a}$ de K, on désigne par $\mathcal{N}(\mathfrak{a})$ la *norme absolue* de cet idéal, définie comme le cardinal du quotient $\mathcal{O}_K/\mathfrak{a}$ si $\mathfrak{a}$ est entier et étendue par multiplicativité à tous les idéaux fractionnaires. À chaque idéal premier $\mathfrak{P}$ de K, on associe une valuation notée $v_{\mathfrak{P}}$ et une place finie $|.|_{\mathfrak{P}}$. L'ensemble des *anti-unités* de K, noté K°, est l'ensemble des éléments x non nuls de K vérifiant $|x|_w = 1$ pour toute place infinie w de K.

Considérons K/k une extension finie de corps de nombres. Pour tout idéal premier $\mathfrak{P}$ de K, l'idéal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k$ est un idéal premier de k. On dit que $\mathfrak{p}$ est au-dessous de $\mathfrak{P}$ (resp. $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$) et on utilise le même vocabulaire pour les places infinies. L'*indice de ramification* $e(\mathfrak{P}/\mathfrak{p})$ est défini comme la valuation $v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_K)$. On dit que $\mathfrak{p}$ *ne se ramifie pas* dans K si $e(\mathfrak{P}/\mathfrak{p})$ est égal à 1 pour tout $\mathfrak{P}$ premier de K au-dessus de $\mathfrak{p}$, et qu'il *se ramifie* sinon. Enfin, si K/k est galoisienne, le *groupe de décomposition* d'une place w de K, noté $D_w(K/k)$, est l'ensemble $\{\sigma \in \mathrm{Gal}(K/k) \mid \sigma \cdot w = w\}$.

0.2.1. Corps à multiplication complexe. — Pour cette partie, on pourra se référer à [**Was97**] et [**Jau08**]. Un corps de nombres K est appelé *totalement réel* si l'image de tout plongement de K dans $\mathbb{C}$ est dans $\mathbb{R}$. Il est dit *totalement imaginaire* si aucun de ses plongements n'est à valeurs dans $\mathbb{R}$. Un *corps CM* (ou corps à multiplication complexe) est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Un tel corps peut être obtenu en partant d'un corps totalement réel et en lui adjoignant la racine carrée d'un nombre dont tous les conjugués sont négatifs. Dans la suite, on note K^+ le sous-corps réel maximal de K. Si K est un corps CM, la conjugaison complexe sur $\mathbb{C}$

induit un automorphisme de K qui est indépendant du plongement de K dans $\mathbb{C}$ considéré. On note τ cet automorphisme, appelé l'unique conjugaison complexe de K.

Soit K un corps CM galoisien sur un sous-corps totalement réel k. On note G le groupe de Galois de K/k. Alors la conjugaison complexe τ est dans le centre de G et le sous-corps de K fixé par $\langle\tau\rangle$ est le sous-corps réel maximal K^+ de K.

Pour un corps de nombres K, on note R_K le *régulateur* de K, à savoir le volume du réseau obtenu comme l'image du groupe des unités de K par le plongement logarithmique. Si K est un corps CM, le quotient des régulateurs de K et de K^+ est donné par la formule

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q} 2^{\frac{[K:\mathbb{Q}]}{2}-1}$$

où Q est l'indice du groupe des unités de K^+ multiplié par $\mu(K)$ dans le groupe des unités de K, qui vaut 1 ou 2.

0.2.2. Congruence mod *. — Pour plus de détails on pourra consulter [**Coh00**]. Un *module* de K est un couple $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ où $\mathfrak{m}_0$ est un idéal entier de K et $\mathfrak{m}_\infty$ est un ensemble de plongements réels de K dans $\mathbb{C}$. On le note formellement sous la forme $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.

Soit $\mathfrak{m}$ un module de K. Un idéal fractionnaire non nul $\mathfrak{a}$ de K est dit premier avec $\mathfrak{m}$ si la valuation $v_\mathfrak{P}(\mathfrak{a})$ est nulle pour tout idéal premier $\mathfrak{P}$ divisant $\mathfrak{m}_0$. On dit qu'un élément α non nul de K est premier avec $\mathfrak{m}$ si l'idéal principal $\alpha\mathcal{O}_K$ est premier avec $\mathfrak{m}$.

Soit α un élément non nul de K. On dit que $\alpha \equiv 1 \mod^*(\mathfrak{m})$ si pour tout idéal premier $\mathfrak{P}$ divisant $\mathfrak{m}_0$ on a l'inégalité $v_\mathfrak{P}(\alpha - 1) \geq v_\mathfrak{P}(\mathfrak{m}_0)$ et si pour tout plongement $\sigma_i \in \mathfrak{m}_\infty$ on a $\sigma_i(\alpha) > 0$. Pour deux éléments non nuls α, β de K, on dit alors que $\alpha \equiv \beta \mod^*(\mathfrak{m})$ si α et β sont premiers avec $\mathfrak{m}$ et si le quotient $\dfrac{\alpha}{\beta} \equiv 1 \mod^*(\mathfrak{m})$.

Dans la suite, on s'intéresse surtout à la congruence $\mod^*(\mathfrak{P})$, pour un idéal premier $\mathfrak{P}$ de K. L'ensemble des plongements réels de K sous-entendu est alors l'ensemble vide.

0.2.3. Théorème de densité de Čebotarev. — On pourra se reporter à [**Sam67**] pour la première partie et à [**Neu99**] pour la seconde.

Soit K/k une extension galoisienne finie de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de k qui ne se ramifie pas dans K. Soit $\mathfrak{P}$ un idéal premier de K au-dessus de $\mathfrak{p}$. Le groupe de décomposition $D_\mathfrak{P}(K/k)$ de $\mathfrak{P}$ est cyclique et engendré par l'unique élément $\sigma_\mathfrak{P}$ de $\mathrm{Gal}(K/k)$ vérifiant

$$\sigma_\mathfrak{P}(x) \equiv x^{\mathcal{N}(\mathfrak{p})} \mod (\mathfrak{P})$$

pour tout élément x dans $\mathcal{O}_K$. Ce générateur est appelé *automorphisme de Frobenius* de $\mathfrak{P}$. Si g appartient à $\mathrm{Gal}(K/k)$, le morphisme de Frobenius associé à $g(\mathfrak{P})$ est égal au conjugué $g \cdot \sigma_\mathfrak{P} \cdot g^{-1}$ de $\sigma_\mathfrak{P}$ par g. En particulier, si l'extension K/k est abélienne, le morphisme de Frobenius ne dépend pas de l'idéal premier $\mathfrak{P}$

au-dessus de $\mathfrak{p}$ et on le note dans ce cas $\sigma_{\mathfrak{p}}$. Si K' est une sous-extension de K/k, galoisienne sur k, la restriction de $\sigma_{\mathfrak{P}}$ à K' est égale au morphisme de Frobenius de l'idéal premier $\mathfrak{P} \cap \mathcal{O}_{K'}$ associé à l'extension K'/k.

Pour un ensemble M d'idéaux premiers de K, on définit la *densité de Dirichlet* comme la limite suivante, si elle existe :

$$d(M) = \lim_{s \to 1^+} \frac{\displaystyle\sum_{\mathfrak{P} \in M} \mathcal{N}(\mathfrak{P})^{-s}}{\displaystyle\sum_{\mathfrak{P}} \mathcal{N}(\mathfrak{P})^{-s}}.$$

Le théorème de densité de Čebotarev donne la densité de l'ensemble des premiers de K dont le Frobenius est égal à un élément σ fixé du groupe de Galois $\mathrm{Gal}(K/k)$.

Théorème 0.3 **(Théorème de densité de Čebotarev)**
Soit K/k une extension galoisienne de groupe de Galois G. Alors pour tout $\sigma \in G$, l'ensemble $P_{K/k}(\sigma) = \{\mathfrak{P}$ premiers de $K \mid \sigma_{\mathfrak{P}} = \sigma\}$ a pour densité

$$d\left(P_{K/k}(\sigma)\right) = \frac{|C_\sigma|}{|G|}$$

où C_σ désigne la classe de conjugaison de σ dans G.

En particulier, pour un élément σ de G donné, il existe une infinité d'idéaux premiers de K dont le morphisme de Frobenius associé à K/k est égal à σ.

CHAPITRE 1

CONJECTURE DE BRUMER-STARK ABÉLIENNE

La conjecture de Brumer-Stark porte sur les extensions abéliennes finies de corps de nombres. Elle prédit qu'un certain élément, appelé élément de Brumer-Stickelberger, construit à partir des valeurs en $s = 0$ des fonctions L d'Artin associées à cette situation, contient des informations sur le corps K dans le cas où au moins une des fonctions L intervenant ne s'annule pas en $s = 0$. Cette conjecture stipule l'annulation du groupe des classes de K par l'élément de Brumer-Stickelberger (partie "Brumer" de la conjecture). De surcroît, elle prévoit que les idéaux obtenus possèdent des générateurs possédant des propriétés bien particulières (partie "Stark" de la conjecture). Nous présentons dans ce chapitre cette conjecture ainsi que les progrès effectués à ce jour pour démontrer sa validité.

Pour la présentation générale de la conjecture de Brumer-Stark abélienne, nous suivons l'article de Tate [**Tat81**].

1.1. Élément de Brumer-Stickelberger

Soit K/k une extension galoisienne finie de corps de nombres, de groupe de Galois noté G abélien. On considère un ensemble fini S de places de k contenant les places archimédiennes ainsi que les places finies qui se ramifient dans K. On suppose le cardinal de S supérieur ou égal à 2. À un caractère χ de G, on associe la fonction L de Hecke partielle définie pour tout $\mathrm{Re}(s) > 1$ par

$$L_{K/k,S}(s,\chi) = \prod_{\mathfrak{p}\notin S}(1-\chi(\sigma_{\mathfrak{p}})\mathcal{N}(\mathfrak{p})^{-s})^{-1}$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de k qui ne sont pas dans S, $\sigma_{\mathfrak{p}}$ désigne le morphisme de Frobenius associé à $\mathfrak{p}$ et à l'extension K/k, et $\mathcal{N}(\mathfrak{p})$ la norme absolue de $\mathfrak{p}$. Cette fonction correspond à la fonction L abélienne où les facteurs d'Euler associés aux premiers de S ont été enlevés. Elle peut être prolongée de manière méromorphe à $\mathbb{C}$ tout entier (elle peut même être prolongée de manière holomorphe si le caractère χ n'est pas le caractère trivial). On définit à l'aide de ces fonctions L abéliennes un analogue de l'élément de Stickelberger cyclotomique

$$\theta_{K/k,S} = \sum_{\chi\in\widehat{G}} L_{K/k,S}(0,\chi)e_{\overline{\chi}}$$

où $e_{\overline{\chi}} = \dfrac{1}{|G|}\sum_{g\in G}\chi(g)g$ est l'idempotent associé à $\overline{\chi}$. A l'instar de Tate [**Tat81**], on appelle cet élément de $\mathbb{C}[G]$ l'élément de Brumer-Stickelberger associé à l'extension K/k et l'ensemble S.

Un caractère χ de G se prolonge par $\mathbb{C}$-linéarité en un morphisme de l'anneau de groupe $\mathbb{C}[G]$, que l'on note encore χ. L'élément $\theta_{K/k,S}$ est caractérisé de manière unique par l'égalité

$$\chi(\theta_{K/k,S}) = L_{K/k,S}(0,\overline{\chi}) \tag{1.1.1}$$

pour tout caractère χ dans $\widehat{G}$.

Il est bien connu que les fonctions L de Hecke partielles sont reliées aux fonctions ζ partielles définies pour tout élément g de G, pour tout $\mathrm{Re}(s) > 1$, par

$$\zeta_{K/k,S}(s,g) = \sum_{\substack{(\mathfrak{a},S)=1\\ \sigma_{\mathfrak{a}}=g}} \mathcal{N}(\mathfrak{a})^{-1}$$

où $\mathfrak{a}$ parcourt les idéaux entiers de K premiers avec les idéaux de S et dont le symbole d'Artin est égal à g. Ces fonctions admettent un prolongement méromorphe au plan complexe tout entier avec un unique pôle en $s = 1$. La relation entre les fonctions L et les fonctions ζ est alors donnée par les deux identités équivalentes

$$\begin{aligned} \zeta_{K/k,S}(s,g) &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}} L_{K/k,S}(s,\overline{\chi})\chi(g), \\ L_{K/k,S}(s,\chi) &= \sum_{g\in G}\zeta_{K/k,S}(s,g)\chi(g). \end{aligned}$$

Grâce à cette relation, l'élément de Brumer-Stickelberger peut aussi s'écrire sous la forme

$$\theta_{K/k,S} = \sum_{g\in G}\zeta_{K/k,S}(0,g)g^{-1}.$$

D'après un travail de Klingen [**Kli62**] et Siegel [**Sie70**], on sait que les valeurs en $s = 0$ des fonctions zeta partielles sont rationnelles. Il en découle la rationnalité de l'élément de Brumer-Stickelberger.

Proposition 1.1. — *L'élément $\theta_{K/k,S}$ se trouve dans $\mathbb{Q}[G]$.*

Un résultat plus raffiné dû indépendemment à Deligne et Ribet [**DR80**], Barsky [**Bar78**] et Cassou-Noguès [**CN79**] donne des renseignements sur le dénominateur de $\theta_{K/k,S}$.

Proposition 1.2. — *Notons $\mu(K)$ le groupe des racines de l'unité de K. Pour tout annulateur ξ de $\mu(K)$ dans $\mathbb{Z}[G]$, l'élément $\xi\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$.*

En particulier si l'on note w_K le cardinal de $\mu(K)$, l'élément $w_K\theta_{K/k,S}$ est à coefficients entiers. L'élément de Brumer-Stickelberger possède un certain nombre de propriétés remarquables.

Proposition 1.3 **(Tate).** —

1. *Pour un idéal premier $\mathfrak{p}_0$ n'appartenant pas à S, on a l'égalité*
$$\theta_{K/k,S\cup\{\mathfrak{p}_0\}} = (1 - {\sigma_{\mathfrak{p}_0}}^{-1})\theta_{K/k,S}.$$
2. *Pour toute place v de S, l'élément $N_v\theta_{K/k,S}$ est nul, où $N_v = \sum_{g\in D_v} g$ désigne la somme des éléments du groupe de décomposition D_v de v.*

Soit K' un corps intermédiaire entre k et K. Notons H le groupe de Galois de K/K' et G' celui de K'/k. On désigne par S' l'ensemble des places de K' au-dessus des places de S.

3. *Notons $\mathrm{res}_{K\to K'}$ l'extension $\mathbb{C}$-linéaire du morphisme de restriction naturel de G dans G'. On a l'identité*
$$\theta_{K'/k,S} = \mathrm{res}_{K\to K'}\left(\theta_{K/k,S}\right).$$
4. *Puisque $\mathbb{Q}[G]$ est un $\mathbb{Q}[H]$ module libre de rang $(G : H)$, l'indice de H dans G, on peut définir la norme d'un élément de $\mathbb{Q}[G]$ comme le déterminant de la matrice à coefficients dans $\mathbb{Q}[H]$ de la multiplication par cet élément. Notons $N_{\mathbb{Q}[G]/\mathbb{Q}[H]} : \mathbb{Q}[G] \longrightarrow \mathbb{Q}[H]$ cette norme. L'élément de Brumer-Stickelberger associé à l'extension K/K' et l'ensemble S' est donné par*
$$\theta_{K/K',S'} = N_{\mathbb{Q}[G]/\mathbb{Q}[H]}\left(\theta_{K/k,S}\right).$$

La première propriété découle de la caractérisation (1.1.1). Les autres propriétés proviennent des résultats connus sur les fonctions L de Hecke. Grâce à la propriété 2, on voit que l'élément de Brumer-Stickelberger est nul chaque fois qu'une place v de S est totalement décomposée dans K. Si $\theta_{K/k,S}$ est non nul, on est donc dans le cas où le corps de base k est totalement réel et K totalement imaginaire.

1.2. Énoncé de la conjecture de Brumer-Stark

On rappelle que l'on désigne par K° l'ensemble des anti-unités de K. On peut alors énoncer la conjecture de Brumer-Stark.

Conjecture 1.4 **($BS(K/k,S)$).** — *Pour tout idéal fractionnaire $\mathfrak{a}$ non nul de K, l'idéal $\mathfrak{a}^{w_K\theta_{K/k,S}}$ est un idéal principal de K, engendré par une anti-unité $\alpha \in K^\circ$, et pour toute racine w_K-ième γ de α, l'extension $K(\gamma)$ est abélienne sur k.*

La première partie stipulant l'annulation du groupe des classes de K par l'élément $w_K\theta_{K/k,S}$ (*i.e* que l'idéal $\mathfrak{a}^{w_K\theta_{K/k,S}}$ est toujours principal) est une conjecture non publiée de Brumer. L'idée supplémentaire que l'on peut toujours trouver un générateur qui est une anti-unité et dont une racine w_K-ième engendre sur K une extension abélienne de k est due à Stark. Il est à noter que le générateur α de la conjecture, s'il existe, est unique à une racine de l'unité de K près.

Dans [**Tat81**], Tate démontre des formulations équivalentes de la conjecture très utiles dans la suite.

***Proposition 1.5* (Tate).** — *Soit $\mathfrak{a}$ un idéal fractionnaire non nul de K. Les conditions suivantes sont équivalentes :*

(i). Il existe $\alpha \in K^\circ$ tel que $\mathfrak{a}^{w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$ et vérifiant $K(\alpha^{\frac{1}{w_K}})$ est abélienne sur k.

(ii). Il existe une extension L de K abélienne sur k et un élément $\beta \in L^\circ$ tel que $\mathfrak{a}^{\theta_{K/k,S}} = \beta \mathcal{O}_L$, où $\mathfrak{a}^{\theta_{K/k,S}}$ est défini par la formule $\mathfrak{a}^{\theta_{K/k,S}} = \left(\mathfrak{a}^{w_K \theta_{K/k,S}}\right)^{\frac{1}{w_K}}$ dans une extension convenable de K.

(iii). Pour presque tout idéal premier $\mathfrak{p}$ de k, il existe $\alpha_\mathfrak{p} \in K^\circ$ tel que $\alpha_\mathfrak{p} \equiv 1 \bmod^*(\mathfrak{p}\mathcal{O}_K)$ et que $\mathfrak{a}^{(\sigma_\mathfrak{p} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}} = \alpha_\mathfrak{p} \mathcal{O}_K$.

(iv). Il existe une famille finie de générateurs $(a_i)_{i \in I}$ de l'annulateur de $\mu(K)$ dans $\mathbb{Z}[G]$ et des éléments $(\alpha_i)_{i \in I}$ de K° tels que $\mathfrak{a}^{a_i \theta_{K/k,S}} = \alpha_i \mathcal{O}_K$ et que ${\alpha_i}^{a_j} = {\alpha_j}^{a_i}$ pour tous i, j dans I.

L'ensemble des idéaux fractionnaires non nuls vérifiant la conjecture de Brumer-Stark forme un groupe pour la multiplication qui est stable sous l'action du groupe de Galois G. On le note $\mathcal{I}^*_{K/k,S}$. La conjecture de Brumer-Stark stipule que le groupe $\mathcal{I}^*_{K/k,S}$ est égal au groupe des idéaux fractionnaires non nuls de K, noté $\mathcal{I}_K$. Grâce à l'assertion (iv) de la proposition 1.5, et à la propriété 2 de la proposition 1.3, on peut démontrer que $\mathcal{I}^*_{K/k,S}$ contient tous les idéaux principaux de K. Une conséquence remarquable de cette propriété est que la conjecture est une question de classes d'idéaux. Pour la démontrer, il suffit donc de considérer les idéaux engendrant le groupe des classes de K.

Étant donné un idéal premier $\mathfrak{p}_0$ de K n'appartenant pas à S, l'expression de l'élément de Brumer-Stickelberger associé à l'extension K/k et l'ensemble $S \cup \{\mathfrak{p}_0\}$ donnée par la propriété 1 de la proposition 1.3 permet de voir le groupe $\mathcal{I}^*_{K/k,S\cup\{\mathfrak{p}_0\}}$ comme l'ensemble

$$\mathcal{I}^*_{K/k,S\cup\{\mathfrak{p}_0\}} = \{\mathfrak{a} \in \mathcal{I}_K \mid \mathfrak{a}^{{\sigma_\mathfrak{p}}_0{}^{-1}} \in \mathcal{I}^*_{K/k,S}\}.$$

Puisque ce groupe contient en particulier $\mathcal{I}^*_{K/k,S}$, si la conjecture de Brumer-Stark associée à l'extension K/k donnée est vraie pour l'ensemble S, elle est vraie en particulier pour l'ensemble $S \cup \{\mathfrak{p}_0\}$. On remarque ainsi que si la conjecture est vraie pour l'ensemble S composé des places infinies de k et des places finies de k ramifiées dans K/k, elle est alors vraie quel que soit l'ensemble S considéré. On dit dans ce cas que la conjecture de Brumer-Stark associée à K/k est vraie sans indiquer l'ensemble de places S et on la note $BS(K/k)$.

Après avoir observé la dépendance de la conjecture par rapport à l'ensemble S, on étudie les conséquences du changement de l'extension K considérée. Soit K' un corps intermédiaire entre K et k.

***Proposition 1.6* (Tate).** — *Si la conjecture $BS(K/k, S)$ est vraie, alors $BS(K'/k, S)$ est aussi vraie.*

Ce résultat repose sur la propriété 3 de la proposition 1.3 et se démontre grâce à la formulation (ii) de la proposition 1.5. Cependant il est possible qu'un idéal

premier de k soit ramifié dans K mais ne le soit pas dans K', on ne peut donc pas dire que la validité de la conjecture de Brumer-Stark associée à l'extension K'/k est entraînée par la validité de la conjecture associée à K/k sans mentionner l'ensemble S.

1.3. État actuel de la conjecture de Brumer-Stark

De nombreux travaux théoriques et numériques ont été effectués sur la conjecture de Brumer-Stark. Nous exposons ici les différents cas dans lesquels la conjecture a été démontrée à notre connaissance, en respectant la chronologie des résultats.

Dans son article [**Tat81**], Tate démontre les résultats suivants.

Théorème 1.7 **(Tate)**. — *La conjecture de Brumer-Stark est vraie dans les cas suivants :*

1. *Si le corps de base k est le corps des nombres rationnels.*
2. *Si K/k est une extension quadratique.*
3. *Si le nombre de classes de K est 1.*
4. *Si G est de cardinal 4 et K/k est une sous-extension d'une extension Galoisienne non abélienne K/k_0 de degré 8.*

Puisque la conjecture est toujours vraie pour les idéaux principaux, l'assertion 3 est directe. La preuve du cas $k = \mathbb{Q}$ se traite en se ramenant au cas où K est un corps cyclotomique grâce aux propriétés de $\theta_{K/k,S}$, puis en utilisant le théorème de Stickelberger. Pour démontrer le cas quadratique, on prouve dans un premier temps que l'élément de Brumer-Stickelberger s'écrit sous la forme explicite

$$\theta_{K/k,S} = \frac{2^{|S|-2}|\mathrm{Coker}(\iota)|}{w_K}(1-\tau)$$

où $G = \{1, \tau\}$ et $\mathrm{Coker}(\iota)$ est le conoyau de l'application naturelle du groupe des classes de l'anneau $\mathcal{O}_{k,S}$ dans celui de $\mathcal{O}_{K,S}$. La démonstration de la conjecture découle de cette expression. Plus précisément, Tate démontre non seulement la validité de la conjecture dans le cas quadratique mais aussi que la conjecture reste encore vraie si l'on remplace $\theta_{K/k,S}$ par $\dfrac{\theta_{K/k,S}}{2^{|S|-2}}$.

En ce qui concerne les groupes de cardinal 4, Sands s'est intéressé ([**San84b**]) au cas où G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et de manière plus générale aux groupes d'exposant 2.

Théorème 1.8 **(Sands)**. — *Si $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, la conjecture $BS(K/k)$ est vraie. Plus généralement, si G est un groupe d'exposant 2, de cardinal $2^l > 4$, et si l'extension K/k est non ramifiée aux premiers de k divisant 2, la conjecture $BS(K/k)$ est vraie.*

La preuve repose sur l'expression de $\theta_{K/k,S}$ en fonction d'éléments de Brumer-Stickelberger associés à des sous-extensions quadratiques de K/k, éléments que l'on sait calculer. Tout comme Tate, Sands obtient dans ces cas précis un résultat plus fort que $BS(K/k)$, qui fait apparaître des puissances de 2 superflues.

D'autres résultats concernent les relations entre les cas où la conjecture de Brumer-Stark est démontrée. On a vu que la conjecture vérifie une propriété de changement d'extension, la question de l'existence d'une propriété similaire de changement du corps de base est soulevée par Tate dans [**Tat81**]. Sands obtient un premier résultat de changement de base ([**San84a**]) dans le cas où le corps de base k est le corps des nombres rationnels. Hayes répond affirmativement à la question en prouvant que les axiomes de la conjecture de Brumer-Stark sont invariants par changement de base ([**Hay98**]).

Théorème 1.9 **(Hayes)**. — *On considère un sous-corps k' de l'extension K/k et l'on désigne par S' l'ensemble des places de k' au-dessus des places de S. La validité de la conjecture $BS(K/k, S)$ implique la véracité de $BS(K/k', S')$.*

Ces deux résultats utilisent tous les deux la formulation de la conjecture donnée par l'assertion (iv) de la proposition 1.5 et reposent sur l'écriture de $\theta_{K/k',S'}$ comme le produit de $\theta_{K/k,S}$ par un élément β de $\mathbb{Q}[G]$ vérifiant des propriétés d'intégralité particulières. Ceci permet d'obtenir la validité de $BS(K/k, S)$ dès que l'on peut considérer K/k comme une sous-extension d'une extension abélienne K/k_0 pour laquelle la conjecture a été démontrée. Toutefois il est à noter que l'ensemble S_0 de places choisi pour K/k_0 peut contenir des premiers ramifiés dans k/k_0 et ainsi ne pas être minimal, comme pour la propriété de changement d'extension.

Wiles fait une grande avancée dans la démonstration de la partie "Brumer" de la conjecture dans [**Wil90**]. Pour chaque nombre premier p, il formule une conjecture locale concernant la p-partie du groupe des classes de K et démontre la validité de la conjecture de Brumer lorsque la conjecture locale est démontrée pour tout premier p. Greither dans [**Gre00**] démontre ensuite cette conjecture locale pour tous les premiers impairs pour une certaine classe d'extensions appelées "nice extensions". Sous les mêmes conditions, Popescu utilise les résultats de Greither afin d'obtenir aussi la démonstration de la partie "Stark" de la conjecture. Ces preuves reposant de manière décisive sur la Conjecture Principale de la Théorie d'Iwasawa, le nombre premier $p = 2$ pose des problèmes spécifiques.

De nombreux calculs numériques effectués dans les premiers cas où la conjecture de Brumer-Stark n'est pas démontrée sont publiés dans [**RT00**], dans le cas où k est un corps quadratique réel et K un corps totalement imaginaire vérifiant $\mathrm{Gal}(K/k) \simeq \mathbb{Z}/4\mathbb{Z}$. Roblot et Tangedal démontrent la validité de la conjecture de Brumer-Stark pour 379 telles extensions. Ils s'intéressent plus particulièrement à la "2-partie de $\theta_{K/k,S}$", définie comme la plus grande puissance de 2 pouvant être factorisée dans l'élément de Brumer-Stickelberger, et démontrent que dans un grand nombre de cas l'intégralité de cette 2-partie n'est pas nécessaire pour que

la conjecture de Brumer-Stark soit valide. Plus étonnant encore est que dans plus de 85% des cas traités, seulement la moitié ou moins de la moitié de la 2-partie est requise pour obtenir la vérification de la conjecture.

Ces résultats sont étendus dans [**GRT04**]. Les auteurs énoncent la conjecture de Brumer-Stark locale, pour tout nombre premier p.

Conjecture 1.10 ($\boldsymbol{BS_p(K/k)}$). — *Pour tout idéal fractionnaire non nul* $\mathfrak{a}$ *de* K *dont la classe est dans la* p*-partie du groupe des classes de* K*, l'idéal* $\mathfrak{a}^{w_K\theta_{K/k,S}}$ *est principal, engendré par une anti-unité* $\alpha \in K^\circ$*, telle que pour toute racine* w_p*-ième* γ *de* α*, l'extension* $K(\gamma)$ *est abélienne sur* k*, où* w_p *désigne le cardinal de la* p*-partie de* $\mu(K)$*.*

On a alors le principe de localisation suivant : la conjecture de Brumer-Stark $BS(K/k)$ est vraie si et seulement si la conjecture locale $BS_p(K/k)$ est vraie pour tout nombre premier p. Les auteurs établissent en outre un important lien entre $BS_p(K/k)$ et la conjecture de Brumer locale, notée $B_p(K/k)$, stipulant l'annulation de la p-partie du groupe des classes de K par $I_p\theta_{K/k,S}$, où I_p désigne l'annulateur de la p-partie de $\mu(K)$ dans $\mathbb{Z}_p[G]$. Sous certaines conditions, ils démontrent que $B_p(K/k)$ est vraie si et seulement si $BS_p(K/k)$ est vraie, permettant ainsi de traduire les progrès récents sur la conjecture de Brumer en résultats concernant la conjecture de Brumer-Stark. Dans le cas où le groupe de Galois G est d'ordre $2p$ avec p un nombre premier impair, ils démontrent qu'il suffit de vérifier les conjectures locales $BS_2(K/k)$ et $BS_p(K/k)$ pour prouver la conjecture de Brumer-Stark. De plus, dans ce cas $BS_p(K/k)$ est vraie sauf pour deux classes d'extensions particulières. Pour un grand nombre d'exemples appartenant à ces classes, ils donnent par ailleurs une preuve numérique complète de la conjecture de Brumer-Stark.

Très récemment [**Pop11**], Popescu a donné une formulation équivalente de la conjecture de Brumer-Stark en termes d'annulation par une L-valeur spéciale en 0 d'un certain groupe des classes d'Arakelov, et propose un raffinement de la conjecture de Brumer-Stark locale. Dans [**GP11**], Greither et Popescu démontrent une conjecture principale équivariante sous la condition que la conjecture principale d'Iwasawa concernant l'annulation des invariants μ appropriés soit vraie. En utilisant ce résultat et la co-descente d'Iwasawa, ils obtiennent la démonstration du raffinement de la conjecture de Brumer-Stark locale, excepté dans le cas où le premier p considéré est égal à 2.

CHAPITRE 2

ÉLÉMENT DE BRUMER NON ABÉLIEN

La conjecture de Brumer-Stark repose sur l'existence de l'élément de Brumer-Stickelberger de l'anneau de groupe abélien $\mathbb{Z}[G]$. Le but de ce chapitre est de construire un élément de Brumer généralisé dans le cas où le groupe de Galois G considéré n'est pas forcément abélien. Pour cela, on se base sur la définition des S-fonctions de Stickelberger donnée dans [**Hay04**] et utilisée aussi dans [**BJ11**]. Nous étudions ensuite les différentes propriétés de cet élément de Brumer non abélien et examinons leurs similitudes avec les propriétés démontrées dans le cas abélien.

2.1. Fonctions L d'Artin non abéliennes

Pour toute cette section, on pourra se reporter à [**Tat84**] ou [**Mar77**] pour des références complètes. Soit K/k une extension galoisienne finie de corps de nombres, de groupe de Galois noté G. Soit S un ensemble fini de places de k contenant les places infinies de k ainsi que les places finies de k qui se ramifient dans K. On considère le caractère $\chi : G \longrightarrow \mathbb{C}$ d'une représentation complexe $\rho : G \longrightarrow GL(V)$. Pour un idéal premier $\mathfrak{p}$ non ramifié de k, le déterminant $\det(1-\mathcal{N}(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{P}}))$ ne dépend pas du choix de l'idéal premier $\mathfrak{P}$ de K au-dessus de $\mathfrak{p}$, où l'on a noté $\sigma_{\mathfrak{P}}$ le morphisme de Frobenius de $\mathfrak{P}$ associé à l'extension K/k. De plus, ce déterminant prend la même valeur pour deux représentations isomorphes. La fonction L d'Artin partielle est alors définie pour $\mathrm{Re}(s) > 1$ par

$$L_{K/k,S}(s,\chi) = \prod_{\mathfrak{p}\notin S} \frac{1}{\det(1-\mathcal{N}(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{P}}))}$$

où $\mathfrak{p}$ parcourt les idéaux premiers de k qui ne sont pas dans S.

Les fonctions L d'Artin vérifient plusieurs propriétés formelles qui nous sont utiles dans la suite, la première étant une propriété d'additivité : pour deux caractères χ_1, χ_2 de G, on a :

$$L_{K/k,S}(s,\chi_1+\chi_2) = L_{K/k,S}(s,\chi_1)L_{K/k,S}(s,\chi_2). \tag{2.1.1}$$

Soit H un sous-groupe de G et φ un caractère de H. On note $\mathrm{Ind}_H^G(\varphi)$ le caractère de G induit par φ. Notons K^H le sous-corps de K fixé par H. Alors la

fonction L vérifie la propriété d'induction :

$$L_{K/k,S}(s, \mathrm{Ind}_H^G(\varphi)) = L_{K/K^H,S_H}(s, \varphi) \tag{2.1.2}$$

où S_H désigne l'ensemble des places de K^H au-dessus des places de S.

Si H désigne un sous-groupe distingué de G, notons G' le quotient G/H et ψ un caractère de G'. On désignera par $\mathrm{Infl}(\psi)$ le caractère relevé de ψ à G défini par

$$\begin{array}{rccccc} \mathrm{Infl}(\psi): & G & \longrightarrow & G' & \longrightarrow & \mathbb{C}. \\ & g & \longmapsto & \overline{g} & \longmapsto & \psi(\overline{g}) \end{array}$$

La fonction L vérifie la propriété d'inflation suivante :

$$L_{K/k,S}(s, \mathrm{Infl}(\psi)) = L_{K^H/k,S}(s, \psi). \tag{2.1.3}$$

Enfin, on s'intéresse à une dernière propriété des fonctions L dans le cas où le caractère considéré χ de G est de degré 1. Dans ce cas $\chi : G \longrightarrow \mathbb{C}^\times$ est un morphisme de groupes qui se factorise par l'abélianisé G^{ab} de G, *i.e* χ passe au quotient pour définir un caractère abélien $\widetilde{\chi} : G/D(G) \longrightarrow \mathbb{C}^\times$ où $D(G)$ désigne le groupe dérivé de G. La fonction L d'Artin partielle associée à χ est alors égale à la fonction L de Hecke partielle attachée à $\widetilde{\chi}$.

Grâce à ces différentes propriétés et au théorème de Brauer, on peut ainsi écrire chaque fonction L d'Artin sous la forme

$$L_{K/k,S}(s, \chi) = \prod_i L_{K/K^i,S_i}(s, \varphi_i)^{n_i} \tag{2.1.4}$$

où les n_i sont des entiers relatifs, les φ_i sont des caractères de degré 1 de sous-groupes convenables H_i de G, les K^i sont les sous-corps de K fixés par les H_i, et les S_i l' ensemble des places de K^i au-dessus des places de S.

Si on utilise alors la propriété d'inflation (2.1.3) vérifiée par les fonctions L d'Artin, on peut passer au quotient de H_i par $\mathrm{Ker}(\varphi_i)$ de sorte à obtenir des caractères $\widetilde{\varphi_i}$ de groupes cycliques. Ainsi la fonction L d'Artin s'écrit de la manière suivante :

$$L_{K/k,S}(s, \chi) = \prod_i L_{K^{\mathrm{Ker}_i}/K^i,S_i}(s, \widetilde{\varphi_i})^{n_i} \tag{2.1.5}$$

où l'on à noté Ker_i le noyau $\mathrm{Ker}(\varphi_i)$. Les fonctions L intervenant dans le produit ci-dessus sont toutes des fonctions L de Hecke.

L'écriture précédente n'est pas unique. Les entiers n_i intervenant ne peuvent pas toujours être choisis positifs, cependant cette écriture de la fonction L d'Artin montre qu'elle admet un prolongement méromorphe à $\mathbb{C}$ tout entier. La conjecture suivante due à Artin porte sur un prolongement holomorphe à tout le plan complexe.

***Conjecture 2.1* (Artin).** — *La fonction $L_{K/k,S}(\cdot, \chi)$ admet un prolongement analytique à $\mathbb{C}$ tout entier si le caractère χ ne contient pas de composante triviale 1_G.*

Pour la construction de l'élément de Brumer non abélien, seule la valeur en $s = 0$ de ces fonctions nous intéresse. On rappelle ici la formule donnant l'ordre d'annulation en $s = 0$ de la fonction $L_{K/k,S}(\cdot, \chi)$, noté $r(\chi)$ (l'extension K/k et l'ensemble S étant sous-entendus). Pour une place v de S, on choisit arbitrairement une place w de K divisant v et on note D_w le groupe de décomposition de la place w associé à l'extension K/k. Le résultat suivant peut être trouvé dans [**Tat84**].

Proposition 2.2. — *L'ordre d'annulation en $s = 0$ de $L_{K/k,S}(\cdot, \chi)$ est*

$$r(\chi) = \left(\sum_{v \in S} \dim V^{D_w} \right) - \dim V^G.$$

2.2. Définition de l'élément de Brumer non abélien

Dans son article [**Hay04**], D. Hayes définit des fonctions méromorphes sur $\mathbb{C}$, appelées les S-fonctions de Stickelberger associées à des extensions galoisiennes non abéliennes K/k et démontre que ces fonctions vérifient des propriétés fonctorielles similaires à celles vérifiées par les fonctions de Stickelberger abéliennes. L'élément de Brumer non abélien est défini comme la valeur en 0 de ces S-fonctions. On rappelle que l'on note $\widehat{G}$ l'ensemble des caractères irréductibles de G.

Définition 2.3. — Soit χ un caractère irréductible de G. On définit l'*idempotent central* associé à χ par $e_\chi = \dfrac{\chi(1)}{|G|} \displaystyle\sum_{g \in G} \chi(g^{-1}) g = \dfrac{\chi(1)}{|G|} \sum_{g \in G} \overline{\chi(g)} g$.

Grâce aux relations d'orthogonalité des caractères irréductibles de G, on peut montrer facilement que ces idempotents sont deux à deux orthogonaux. Si χ, ψ sont deux éléments de $\widehat{G}$, on a donc $e_\chi \cdot e_\psi = \delta_{\chi,\psi} e_\chi$, où $\delta_{\chi,\psi}$ désigne le symbole de Kronecker.

L'élément de Brumer associé à l'extension K/k et à l'ensemble S est alors construit à partir des valeurs en $s = 0$ des fonctions L d'Artin partielles associées à K/k et des idempotents centraux de la manière suivante.

Définition 2.4. — L'élément appartenant au centre de $\mathbb{C}[G]$

$$\theta_{K/k,S} = \sum_{\chi \in \widehat{G}} L_{K/k,S}(0, \chi) e_{\overline{\chi}}$$

est appelé *élément de Brumer* associé à l'extension K/k et à l'ensemble S.

2.2.1. Caractérisation et propriétés de $\boldsymbol{\theta_{K/k,S}}$. — Tous les résultats de cette sous-partie sont issus de [**Hay04**].

2.2.1.1. Caractérisation. — Notons $C_1, \dots, C_r$ les différentes classes de conjugaison de G. On sait que r est aussi égal au nombre de caractères irréductibles de G. On identifie dans la suite la classe C_i avec l'élément $\sum_{g \in C_i} g$ de l'anneau de groupe complexe $\mathbb{C}[G]$. De même, on note C_i^{-1} la somme $\sum_{g \in C_i} g^{-1}$ pour désigner la classe inverse de C_i. Le centre de $\mathbb{C}[G]$, noté $Z(\mathbb{C}[G])$, est l'anneau $\mathbb{C}[C_1, \dots, C_r]$ engendré sur $\mathbb{C}$ par les classes C_i.

Pour un caractère irréductible χ de G, on désigne encore par χ la fonction de $\mathbb{C}[G]$ étendue par $\mathbb{C}$-linéarité, de sorte que $\chi(C_i)$ désigne l'élément

$$\chi(C_i) = \sum_{g \in C_i} \chi(g) = |C_i| \chi(g_i)$$

où g_i désigne un élément quelconque de C_i. On peut alors construire la fonction ϕ_χ comme l'application $\mathbb{C}$-linéaire de $\mathbb{C}[C_1, \dots, C_r]$ dans $\mathbb{C}$ qui vérifie

$$\phi_\chi(C_i) = \frac{\chi(C_i)}{\chi(1)}, \tag{2.2.1}$$

pour toute classe de conjugaison C_i de G.

Théorème 2.5. — *Pour tout caractère χ appartenant à $\widehat{G}$, l'application ϕ_χ définie ci-dessus est un morphisme d'anneaux de $Z(\mathbb{C}[G])$ dans $\mathbb{C}$. De plus tout morphisme d'anneaux de $Z(\mathbb{C}[G])$ dans $\mathbb{C}$ est égal à l'un des ϕ_χ.*

D. Hayes démontre alors une caractérisation de l'élément de Brumer à l'aide de ces morphismes ϕ_χ.

Proposition 2.6. — *Pour tout caractère irréductible χ de G, on a l'égalité*

$$\phi_\chi(\theta_{K/k,S}) = L_{K/k,S}(0, \overline{\chi}).$$

De plus, cette propriété définit de manière unique l'élément $\theta_{K/k,S}$.

Ceci découle du fait que pour deux caractères χ et ψ dans $\widehat{G}$, le morphisme ϕ_χ appliqué à e_ψ, $\phi_\chi(e_\psi)$, est nul si χ et ψ sont différents et vaut 1 sinon.

Puisque l'élément de Brumer est dans le centre de $\mathbb{C}[G]$, on peut aussi l'écrire sous la forme d'une combinaison linéaire des classes de G. Hayes définit ainsi des fonctions zeta partielles non abéliennes associées aux classes C_i, vérifiant

$$\theta_{K/k,S} = \sum_{i=1}^{r} \zeta_{K/k,S}(0, C_i) \frac{1}{|C_i|} C_i^{-1}.$$

2.2.1.2. Propriété de restriction. — Une fois cet élément de Brumer non abélien défini, il est naturel de se demander s'il vérifie des propriétés fonctorielles similaires au cas abélien. On commence par regarder sa dépendance par rapport à l'extension K. Soit H un sous-groupe distingué de G de sous-corps fixé K^H, on note G' le groupe de Galois de K^H sur k. On désigne par $\mathrm{res}_{K \to K^H} : G \longrightarrow G'$ le morphisme naturel de restriction. On obtient alors comme dans le cas abélien une relation entre l'élément de Brumer associé à l'extension K/k et celui attaché à K^H/k.

Théorème 2.7. — $\theta_{K^H/k,S} = \mathrm{res}_{K\to K^H}(\theta_{K/k,S})$

Ce résultat s'obtient grâce à la caractérisation de l'élément de Brumer donnée par la proposition 2.6 ainsi que la propriété d'inflation (2.1.3) des fonctions L d'Artin.

2.2.1.3. Propriété de réduction. — Hayes s'intéresse ensuite à la dépendance par rapport au corps de base k. Soit H un sous-groupe de G. Notons k' le sous-corps fixé par H et S' l'ensemble des places de k' au-dessus des places de S. Afin de déterminer les liens entre les éléments de Brumer associés aux extensions K/k et K/k' munies de leurs ensembles respectifs S et S', on définit une norme inhomogène $\mathrm{INorm}_{G\to H} : Z(\mathbb{C}[G]) \longrightarrow Z(\mathbb{C}[H])$. On a alors le résultat suivant :

Théorème 2.8. — $\theta_{K/k',S'} = \mathrm{INorm}_{G\to H}(\theta_{K/k,S})$

De plus, lorsque le groupe H est abélien, cette norme inhomogène peut se calculer comme un déterminant, à l'instar du calcul habituel des applications normes standard.

2.2.2. Dépendance de l'élément de Brumer par rapport à S. — On s'intéresse désormais au comportement de l'élément de Brumer lorsque l'on modifie certaines places finies dans l'ensemble S. Soit $\mathfrak{p}_0$ un idéal premier non ramifié de k qui n'appartient pas à S. Notre but est d'exprimer l'élément $\theta_{K/k,S\cup\{\mathfrak{p}_0\}}$ en fonction de $\theta_{K/k,S}$. Puisque les fonctions L d'Artin associées à l'extension K/k et à l'ensemble $S\cup\{\mathfrak{p}_0\}$ déterminent entièrement $\theta_{K/k,S\cup\{\mathfrak{p}_0\}}$, on commence par expliciter la fonction $L_{K/k,S\cup\{\mathfrak{p}_0\}}(\cdot,\chi)$ pour un caractère $\chi\in\widehat{G}$ donné. Pour un nombre complexe s vérifiant $\mathrm{Re}(s)>1$, on a

$$\begin{aligned} L_{K/k,S\cup\{\mathfrak{p}_0\}}(s,\chi) &= \prod_{\mathfrak{p}\notin S\cup\{\mathfrak{p}_0\}} \frac{1}{\det(1-\mathcal{N}(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{p}}))} \\ &= \prod_{\mathfrak{p}\notin S} \frac{1}{\det(1-\mathcal{N}(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{p}}))} \det(1-\mathcal{N}(\mathfrak{p}_0)^{-s}\rho(\sigma_{\mathfrak{P}_0})) \\ &= L_{K/k,S}(s,\chi)\det(1-\mathcal{N}(\mathfrak{p}_0)^{-s}\rho(\sigma_{\mathfrak{P}_0})) \end{aligned}$$

où $\mathfrak{P}_0$ désigne un idéal premier de K au-dessus de $\mathfrak{p}_0$. On obtient alors par prolongement méromorphe

$$L_{K/k,S\cup\{\mathfrak{p}_0\}}(0,\chi) = L_{K/k,S}(0,\chi)\det(1-\rho(\sigma_{\mathfrak{P}_0})).$$

Le résultat suivant nous donne le lien entre l'élément de Brumer associé à S et celui associé à $S\cup\{\mathfrak{p}_0\}$.

Proposition 2.9. — *Si $\mathfrak{p}_0$ est un idéal premier de k n'appartenant pas à l'ensemble S, on a l'égalité*

$$\theta_{K/k,S\cup\{\mathfrak{p}_0\}} = \theta_{K/k,S}\cdot\sum_{\chi\in\widehat{G}}\det(1-\rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}}$$

où ρ_χ désigne une représentation irréductible dont χ est le caractère.

Démonstration. — Pour démontrer cette égalité, nous nous servons de la caractérisation de l'élément de Brumer donnée précédemment. Posons

$$\alpha = \sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}}.$$

L'élément α étant une combinaison linéaire des idempotents centraux, il appartient au centre de $\mathbb{C}[G]$, donc il en est de même de $\theta_{K/k,S} \cdot \alpha$. Soit ψ un caractère irréductible de G. On a $\phi_{\overline{\psi}}(\theta_{K/k,S} \cdot \alpha) = \phi_{\overline{\psi}}(\theta_{K/k,S})\phi_{\overline{\psi}}(\alpha)$. De plus, d'après la proposition 2.6, $\phi_{\overline{\psi}}(\theta_{K/k,S})$ n'est rien d'autre que la fonction L associée à ψ calculée en $s = 0$, $L_{K/k,S}(0, \psi)$. Il nous reste donc à expliciter l'autre terme :

$$\phi_{\overline{\psi}}(\alpha) = \phi_{\overline{\psi}}\left(\sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}}\right) = \sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0}))\phi_{\overline{\psi}}(e_{\overline{\chi}}).$$

Puisque $\phi_{\overline{\psi}}(e_{\overline{\chi}})$ est égal à 1 lorsque χ et ψ sont égaux, et est nul le reste du temps, on obtient finalement $\phi_{\overline{\psi}}(\alpha) = \det(1 - \rho_\psi(\sigma_{\mathfrak{P}_0}))$. Ainsi, on trouve que pour tout $\psi \in \widehat{G}$, $\phi_{\overline{\psi}}(\theta_{K/k,S} \cdot \alpha) = L_{K/k,S}(0, \psi)\det(1 - \rho_\psi(\sigma_{\mathfrak{P}_0})) = L_{K/k,S\cup\{\mathfrak{p}_0\}}(0, \psi)$. On conclut grâce à la proposition 2.6 puisque $\theta_{K/k,S\cup\{\mathfrak{p}_0\}}$ est l'unique élément de $Z(\mathbb{C}[G])$ vérifiant cette propriété. □

Remarque. — En particulier, lorsque l'élément de Brumer $\theta_{K/k,S}$ est nul pour un ensemble donné S, ceci implique la nullité de l'élément de Brumer associé à n'importe quel ensemble S' contenant S.

Dans le cas où G est abélien, toutes les représentations sont de degré 1, et les termes de la forme $\det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0}))$ s'écrivent alors $1 - \chi(\sigma_{\mathfrak{P}_0})$. La somme intervenant dans la proposition précédente devient donc

$$\begin{aligned}\sum_{\chi \in \widehat{G}}(1 - \chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}} &= \sum_{\chi \in \widehat{G}}(1 - \chi(\sigma_{\mathfrak{P}_0}))\frac{1}{|G|}\sum_{g \in G}\chi(g)g \\ &= \frac{1}{|G|}\sum_{g \in G}\left(\sum_{\chi \in \widehat{G}}\chi(g) - \sum_{\chi \in \widehat{G}}\chi(\sigma_{\mathfrak{P}_0}g)\right)g.\end{aligned}$$

En utilisant ensuite les relations données par l'expression du caractère de la représentation régulière de G (cf. [**Ser78**]), on trouve que la somme $\sum_{\chi \in \widehat{G}}\chi(\sigma)$ est nulle si σ est un élément non trivial de G et vaut $|G|$ sinon. Finalement l'élément α est égal à $1 - \sigma_{\mathfrak{P}_0}^{-1}$. On retrouve ainsi le résultat de dépendance par rapport à S de l'élément de Brumer dans le cas abélien.

2.3. Des annulateurs explicites de $\theta_{K/k,S}$

On cherche à démontrer que l'élément de Brumer non abélien vérifie des propriétés similaires à celles vérifiées par l'élément de Brumer abélien. En particulier, on aimerait connaître des annulateurs explicites de $\theta_{K/k,S}$. Pour cela, on va créer pour chaque place v de S un analogue de l'élément N_v défini dans le cas abélien.

Afin d'établir que la multiplication de $\theta_{K/k,S}$ par un tel élément donne l'élément nul, on a besoin d'énoncer un lemme général sur les représentations des groupes finis utile pour la suite.

2.3.1. Dimension du sous-espace stable par G. — Soit G un groupe fini quelconque, et $\rho : G \longrightarrow GL(V)$ une représentation linéaire de G. On note χ le caractère de G associé à ρ, et 1_G le caractère trivial de G, que l'on identifie aussi avec la représentation unité de G. On désigne par $n_{1_G}(\chi)$ le produit scalaire sur G entre χ et 1_G, donné par

$$n_{1_G}(\chi) = \langle 1_G, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

La quantité $n_{1_G}(\chi)$ représente le nombre de représentations irréductibles isomorphes à la représentation unité dans la décomposition de (ρ, V) en représentations irréductibles de G. Dans la suite, on notera V^G l'ensemble des éléments de V stables par G, *i.e* l'ensemble $\{v \in V : \forall g \in G, \rho(g)(v) = v\}$.

Lemme 2.10. — *La dimension de V^G est $n_{1_G}(\chi)$.*

Démonstration. — Pour éviter d'alourdir les notations, notons $n = \dim_{\mathbb{C}} V^G$ la dimension de V^G. On considère une base $\{e_1, \ldots, e_n\}$ de V^G. Alors pour $i \in \{1, \ldots, n\}$, on a pour tout v appartenant à $\mathbb{C}e_i$, $\rho(g)(v) = v$, quel que soit g dans G. En particulier, le sous-espace vectoriel $\mathbb{C}e_i$ de V est stable pour les opérations de G, c'est donc une sous-représentation de V que l'on note W_i, isomorphe à la représentation unité de G par construction. Ainsi, on peut écrire V sous la forme

$$V = \bigoplus_{i=1}^{n} W_i \oplus W$$

où W est une représentation de G, donc la decomposition de V en représentations irréductibles contient au moins n représentations isomorphes à 1_G.

Pour l'inégalité inverse, on sait que l'on peut décomposer V sous la forme

$$V = \bigoplus_{i=1}^{n_{1_G}(\chi)} X_i \oplus Y$$

où les X_i sont isomorphes à 1_G et Y est une représentation de G. Pour tout i appartenant à $\{1, \ldots, n_{1_G}(\chi)\}$, il existe alors un isomorphisme τ_i de X_i dans $\mathbb{C}$ tel que l'on ait pour tout g dans G, $\rho(g) = {\tau_i}^{-1} 1_G(g) \tau_i = 1_G(g)$. Ainsi, tout élément x_i de X_i vérifie $\rho(g)(x_i) = 1_G(x_i) = x_i$, et X_i est inclus dans V^G. Les X_i étant en somme directe et de dimension 1, on trouve donc que la dimension de V^G est supérieure ou égale à $n_{1_G}(\chi)$ ce qui termine la preuve.

□

2.3.2. Application à la recherche d'annulateurs. — Revenons désormais à notre extension K/k de corps de nombres considérée. On va construire l'analogue de la norme formelle du groupe de décomposition d'une place v de S qui intervient dans le cas abélien. Pour une place v de S, on choisit une place w de K au-dessus de v et on pose

$$N_v = \sum_{\sigma \in D_w} \frac{1}{|C_\sigma|} C_\sigma \tag{2.3.1}$$

où $D_w = D_w(K/k) = \{\sigma \in G : \sigma \cdot w = w\}$ désigne le groupe de décomposition de la place w et C_σ la classe de conjugaison de σ dans G.

Vérifions que cet élément est bien défini. Soit w' une autre place de K au-dessus de v. Il existe alors g dans G tel que $w' = g \cdot w$. En utilisant les propriétés des groupes de décomposition, on obtient $D_{w'} = gD_w g^{-1}$. On a alors

$$\sum_{\sigma' \in D_{w'}} \frac{1}{|C_{\sigma'}|} C_{\sigma'} = \sum_{\sigma \in D_w} \frac{1}{|C_{g\sigma g^{-1}}|} C_{g\sigma g^{-1}}.$$

Or, la classe de conjugaison de $g\sigma g^{-1}$ est la même que celle de σ :

$$C_{g\sigma g^{-1}} = \{g' g\sigma g^{-1} g'^{-1} : g' \in G\} = \{\mu\sigma\mu^{-1} : \mu \in G\} = C_\sigma.$$

On obtient donc $\displaystyle\sum_{\sigma' \in D_{w'}} \frac{1}{|C_{\sigma'}|} C_{\sigma'} = \sum_{\sigma \in D_w} \frac{1}{|C_\sigma|} C_\sigma$, et la quantité N_v est bien définie.

Remarque. — Cette définition de N_v est compatible avec celle déjà existante dans le cas où le groupe G est abélien. En effet, dans ce cas, les groupes de décomposition des places de K au-dessus de v sont tous identiques au même groupe et on note celui-ci D_v. Puisque G est un groupe abélien, les classes de conjugaison sont composées d'un seul élément et on retrouve bien $N_v = \displaystyle\sum_{\sigma \in D_v} \sigma$.

Proposition 2.11. — *On suppose que S est de cardinal supérieur ou égal à 2. Alors pour toute place v de S, l'élément $N_v \theta_{K/k,S}$ est nul.*

Démonstration. — Puisque N_v est une combinaison linéaire de classes de conjugaison, N_v appartient au centre de $\mathbb{C}[G]$, $Z(\mathbb{C}[G])$. Ainsi le produit $N_v \theta_{K/k,S}$ est aussi dans $Z(\mathbb{C}[G])$ (en fait $N_v \theta_{K/k,S}$ est même dans $Z(\mathbb{Q}[G])$ comme nous le verrons ultérieurement). Pour un caractère irréductible $\chi \in \widehat{G}$, on peut donc lui appliquer le morphisme d'anneaux ϕ_χ défini en (2.2.1). On obtient alors

$$\begin{aligned} \phi_\chi(N_v \theta_{K/k,S}) &= \phi_\chi(N_v)\phi_\chi(\theta_{K/k,S}) \\ &= \phi_\chi(N_v) L_{K/k,S}(0, \overline{\chi}) \end{aligned}$$

d'après la proposition 2.6.

Explicitons le terme $\phi_\chi(N_v)$:

$$\begin{aligned}
\phi_\chi(N_v) &= \phi_\chi\left(\sum_{\sigma\in D_w}\frac{1}{|C_\sigma|}C_\sigma\right)\\
&= \sum_{\sigma\in D_w}\frac{1}{|C_\sigma|}\phi_\chi(C_\sigma)\\
&= \sum_{\sigma\in D_w}\frac{1}{|C_\sigma|}\frac{|C_\sigma|\chi(\sigma)}{\chi(1)}\\
&= \frac{1}{\chi(1)}\sum_{\sigma\in D_w}\chi(\sigma)\\
&= \frac{|D_w|}{\chi(1)}\, n_{1_{D_w}}\left(\chi_{|D_w}\right)
\end{aligned}$$

en adaptant les notations du lemme 2.10 au groupe D_w. On note $\rho : G \longrightarrow GL(V)$ une représentation irréductible de G dont χ est le caractère associé. Alors la restriction $\rho_{|D_w} : D_w \longrightarrow GL(V)$ est une représentation de D_w et son caractère est $\chi_{|D_w}$. La quantité $n_{1_{D_w}}\left(\chi_{|D_w}\right)$ est donc le nombre de représentations isomorphes à la représentation unité de D_w dans la décomposition en irréductibles de $\rho_{|D_w}$. Si cette quantité est nulle, on a bien $\phi_\chi(N_v\theta_{K/k,S}) = 0$. Sinon, on va montrer qu'en fait la fonction L associée à $\overline{\chi}$ calculée en $s = 0$, $L_{K/k,S}(0,\overline{\chi})$, est nulle. Pour cela, on utilise la proposition 2.2 donnant l'ordre d'annulation de la fonction L d'Artin en 0 :

$$r(\chi) = \sum_{v'\in S}\dim V^{D_{w'}} - \dim V^G$$

où w' est une place arbitraire de K au dessus de v'.

Soit donc χ un caractère irréductible de G pour lequel $n_{1_{D_w}}\left(\chi_{|D_w}\right)$ est non nul. Commençons par traiter le cas où χ est le caractère trivial de G. Dans ce cas, le caractère χ est réel, donc égal à $\overline{\chi}$. De plus, tous les éléments de V sont stables par G, donc en particulier il sont stables par n'importe quel sous-groupe de G. Puisque V est de dimension 1, on obtient alors $r(\overline{\chi}) = r(\chi) = |S| - 1$. L'ensemble S étant supposé de cardinal supérieur ou égal à 2, $L_{K/k,S}(0,\chi)$ est nulle.

On suppose maintenant que χ est non trivial et vérifie $n_{1_{D_w}}\left(\chi_{|D_w}\right) \neq 0$. Puisque χ est irréductible et non trivial, on sait d'après les propriétés d'orthogonalité des caractères irréductibles que le produit scalaire sur G entre χ et 1_G est nul. Ainsi $n_{1_G}(\chi)$ est nul et par le lemme 2.10, V^G est de dimension nulle. En appliquant encore le lemme 2.10 mais cette fois-ci au groupe D_w et au caractère $\chi_{|D_w}$, on obtient $\dim_{\mathbb{C}} V^{D_w} \geq 1$, et donc

$$\begin{aligned}
r(\chi) &= \sum_{v'\in S}\dim V^{D_{w'}} - \dim V^G\\
&= \sum_{v'\in S}\dim V^{D_{w'}} \geq 1.
\end{aligned}$$

Ainsi, lorsque $n_{1_{D_w}}\left(\chi_{|D_w}\right) \neq 0$, $L_{K/k,S}(0,\chi)$ est nulle. Comme la somme $\sum_{\sigma\in D_w}\chi(\sigma)$ peut s'écrire aussi comme $\sum_{\sigma^{-1}\in D_w}\chi(\sigma^{-1})$ qui n'est rien d'autre que $\sum_{\sigma\in D_w}\chi(\sigma^{-1})$, on dispose aussi de l'identité

$$n_{1_{D_w}}\left(\chi_{|D_w}\right) = \frac{1}{|D_w|}\sum_{\sigma\in D_w}\overline{\chi(\sigma)} = n_{1_{D_w}}\left(\overline{\chi}_{|D_w}\right),$$

ce qui nous permet de conclure que lorsque $n_{1_{D_w}}\left(\chi_{|D_w}\right)$ est différent de 0, $L_{K/k,S}(0,\overline{\chi})$ est aussi nulle.

Finalement, on obtient toujours $\phi_\chi(N_v) = 0$, ou $L_{K/k,S}(0,\overline{\chi}) = 0$. Ainsi, dans tous les cas, l'élément $\phi_\chi(N_v\theta_{K/k,S})$ est toujours nul, quel que soit le caractère $\chi \in \widehat{G}$ choisi. Puisque

$$Z(\mathbb{C}[G]) \simeq \bigoplus_{\chi\in\widehat{G}} \mathbb{C}e_\chi,$$

$N_v\theta_{K/k,S}$ s'écrit de manière unique sous la forme $N_v\theta_{K/k,S} = \sum_{\chi\in\widehat{G}} x_\chi e_\chi$ avec $x_\chi \in \mathbb{C}$. En utilisant le fait que pour tout $\chi,\psi \in \widehat{G}$, $\phi_\chi(e_\psi) = \delta_{\chi,\psi}e_\psi$, on trouve donc que pour tout $\chi \in \widehat{G}$, le coefficient x_χ est nul. En conclusion, on obtient bien $N_v.\theta_{K/k,S} = 0$.

□

Remarque. — S'il existe une place v de S qui se décompose totalement dans K, le groupe de décomposition de n'importe quelle place w de K divisant v est trivial. La quantité N_v est alors réduite à 1, et le résultat précédent implique que l'élément de Brumer $\theta_{K/k,S}$ est nul.

Puisqu'une place infinie complexe est totalement décomposée dans n'importe quelle extension, et que l'existence dans K d'une place réelle w implique que la place réelle de k au-dessous de w est totalement décomposée dans K, pour que $\theta_{K/k,S}$ soit non nul, force est de supposer, comme dans le cas abélien, que le corps de base k est totalement réel et K totalement complexe.

2.4. Rationnalité des coefficients de $\theta_{K/k,S}$

On se pose à présent la question de la rationnalité ou non des coefficients de l'élément de Brumer. À ce stade, on sait simplement que $\theta_{K/k,S}$ est dans le centre de $\mathbb{C}[G]$. On va démontrer que comme dans le cas abélien, les coefficients de $\theta_{K/k,S}$ sont tous rationnels. Pour cela, on va faire appel à la conjecture principale de Stark de rang zéro, qui a été démontrée (cf. [**Tat84**]).

2.4.1. Conjecture principale de Stark de rang zéro. — Soit χ un caractère de G. On suppose que l'ordre d'annulation en $s = 0$ de la fonction $L_{K/k,S}(\cdot,\chi)$ est nul (*i.e* $L_{K/k,S}(0,\chi) \neq 0$). Dans ce cas la conjecture principale de Stark s'écrit :

$$L_{K/k,S}(0,\chi^\alpha) = L_{K/k,S}(0,\chi)^\alpha \text{ pour tout } \alpha \in \mathrm{Aut}(\mathbb{C}) \tag{2.4.1}$$

où χ^α désigne le caractère de G défini par $\chi^\alpha = \alpha \circ \chi$. Le résultat suivant ainsi que sa démonstration sont issus de [**Tat84**]. On reprend ici un élément de la démonstration qui nous permet d'obtenir un renseignement supplémentaire sur $\theta_{K/k,S}$.

Théorème 2.12 **(Conjecture principale de Stark de rang zéro)**
Si $r(\chi) = 0$, alors on a $L_{K/k,S}(0, \chi^\alpha) = L_{K/k,S}(0, \chi)^\alpha$ pour tout $\alpha \in Aut(\mathbb{C})$.

Fragment de démonstration. — On s'intéresse seulement à la partie de la démonstration qui concerne le cas où le caractère χ considéré n'est pas le caractère trivial. La conjecture principale de Stark ne dépendant pas de l'ensemble S considéré, on peut supposer que S est l'ensemble constitué des places infinies de k et des places finies ramifiées dans K. Grâce aux propriétés des fonctions L d'Artin, on peut se restreindre au cas où χ est le caractère d'une représentation irréductible et fidèle (ρ, V) de G. Puisque χ n'est pas trivial, la dimension de l'ensemble V^G est nulle, la proposition 2.2 implique alors l'identité $V^{D_w} = \{0\}$ pour toute place infinie w de K. Ceci impose en particulier que le groupe de décomposition de w est de la forme $D_w = \{1, \tau_w\}$ et que τ_w agit sur V comme la multiplication par -1. Puisque la représentation est fidèle, tous les τ_w sont alors égaux, disons à τ. Ainsi K est un corps CM et l'unique conjugaison complexe τ est dans le centre de G.

J. Tate utilise alors un raffinement du théorème de Brauer afin de pouvoir se ramener au cas où G est abélien et χ est un morphisme injectif de G dans $\mathbb{C}^*$. En utilisant l'expression des fonctions L abéliennes à l'aide des fonctions zeta partielles, le résultat fondamental de la rationnalité en zéro des fonctions zeta partielles permet de conclure. □

Remarque. — On a vu que lorsque l'ensemble S est de cardinal supérieur ou égal à 2, pour que l'élément de Brumer soit non nul, il faut supposer le corps k totalement réel et K totalement imaginaire. De plus, la démonstration précédente permet de s'apercevoir que pour un caractère irréductible de G, le fait que la fonction $L_{K/k,S}(\cdot, \chi)$ ne s'annule pas en zéro implique que χ provient d'une sous-extension CM de K/k. En particulier, pour que $\theta_{K/k,S}$ soit non nul, il faut que l'extension K/k contienne une sous-extension CM galoisienne sur k.

Corollaire 2.13. — *On suppose que l'ensemble S contient aux moins deux places. Si le groupe de Galois de K/k est un groupe simple non abélien, l'élément de Brumer $\theta_{K/k,S}$ est nul.*

Démonstration. — Si k n'est pas totalement réel, le résultat est vrai d'après la remarque suivant la proposition 2.11. Supposons k totalement réel. Si G est un groupe simple non abélien, les seuls sous-groupes distingués de G sont $\{1\}$ et G lui-même. Par conséquent, il n'y a aucun sous-corps non trivial de l'extension K/k galoisiens sur le corps de base k. Si K était de type CM, l'unique conjugaison complexe de K serait dans le centre de G, qui est trivial, donc K n'est pas un

corps CM. C'est pourquoi K/k ne contient aucune sous-extension galoisienne CM, donc $\theta_{K/k,S}$ est nul. □

En particulier, si G est le groupe des permutations de n éléments, $\mathfrak{S}_n$, avec n supérieur ou égal à 5, les seules sous-extensions galoisiennes sur k de K sont K, qui n'est pas de type CM vu que son centre est trivial, le sous-corps fixé par le groupe alterné $\mathcal{A}_n$ noté $K^{\mathcal{A}_n}$, et k lui-même. Puisque $\mathcal{A}_n$ est simple, $K^{\mathcal{A}_n}$ ne contient aucune sous-extension CM galoisienne. On en conclut donc que K/k ne contient aucune sous-extension galoisienne CM, ce qui prouve que $\theta_{K/k,S}$ est nul.

2.4.2. Démonstration de la rationnalité des coefficients de $\theta_{K/k,S}$. — Afin de prouver que l'élément de Brumer appartient à $\mathbb{Q}[G]$, nous allons démontrer que chaque coefficient de $\theta_{K/k,S}$ est fixé par tous les automorphismes de $\mathbb{C}$. Pour conclure, nous utiliserons le résultat suivant que l'on peut trouver par exemple dans [**Mil11**].

Théorème 2.14. — *Soient Ω un corps séparablement clos et F un sous-corps parfait de Ω. Si un élément x de Ω est fixé par tous les F-automorphismes de Ω, alors x appartient à F.*

L'intérêt du résultat qui suit est de pouvoir appliquer l'élément de Brumer, sous réserve de connaître son dénominateur, à des idéaux fractionnaires de K. Cela nous permettra de généraliser simplement la partie "Brumer" de la conjecture $BS(K/k,S)$ au cas non abélien.

Théorème 2.15. — *L'élément de Brumer $\theta_{K/k,S}$ appartient à $\mathbb{Q}[G]$.*

Démonstration. — On commence par écrire $\theta_{K/k,S}$ sous la forme d'une somme formelle d'éléments de G, $\sum_{g\in G} x_g g$, où les x_g sont pour l'instant dans $\mathbb{C}$. Puisque l'élément de Brumer $\theta_{K/k,S}$ est défini comme la somme

$$\theta_{K/k,S} \;=\; \sum_{\chi\in\widehat{G}} L_{K/k,S}(0,\chi)e_{\overline{\chi}},$$

remplacer les idempotents par leur expression explicite donne

$$\begin{aligned}\theta_{K/k,S} &= \sum_{\substack{\chi\in\widehat{G}\\ r(\chi)=0}} L_{K/k,S}(0,\chi)\frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g)g\\ &= \sum_{g\in G}\left(\frac{1}{|G|}\sum_{\substack{\chi\in\widehat{G}\\ r(\chi)=0}}\chi(1)L_{K/k,S}(0,\chi)\chi(g)\right)g.\end{aligned}$$

Appelons X l'ensemble des caractères irréductibles de G dont la fonction d'Artin associée ne s'annule pas en $s=0$, *i.e* $X=\{\chi\in\widehat{G} : r(\chi)=0\}$. On pose alors

$$x_g = \frac{1}{|G|}\sum_{\chi\in X}\chi(1)L_{K/k,S}(0,\chi)\chi(g).$$

Soient g un élément quelconque de G et α un automorphisme de $\mathbb{C}$. On peut écrire

$$\begin{aligned}\alpha(x_g) &= \alpha\left(\frac{1}{|G|}\sum_{\chi\in X}\chi(1)L_{K/k,S}(0,\chi)\chi(g)\right)\\ &= \frac{1}{|G|}\sum_{\chi\in X}\alpha(\chi(1))\alpha(L_{K/k,S}(0,\chi))\alpha(\chi(g))\\ &= \frac{1}{|G|}\sum_{\chi\in X}\chi^{\alpha}(1)L_{K/k,S}(0,\chi^{\alpha})\chi^{\alpha}(g)\end{aligned}$$

d'après la conjecture principale de Stark de rang zéro. D'autre part, si χ est un caractère irréductible appartenant à X, le caractère χ^{α} est aussi dans l'ensemble X. En effet, χ^{α} est irréductible puisque que le produit scalaire sur G de χ^{α} par lui-même est

$$\begin{aligned}\langle\chi^{\alpha},\chi^{\alpha}\rangle_G &= \frac{1}{|G|}\sum_{g\in G}\chi^{\alpha}(g)\chi^{\alpha}(g^{-1})\\ &= \alpha\left(\frac{1}{|G|}\sum_{g\in G}\chi(g)\chi(g^{-1})\right)\\ &= \alpha\left(\langle\chi,\chi\rangle_G\right)\\ &= 1.\end{aligned}$$

De plus, si $L_{K/k,S}(0,\chi)$ est non nulle, puisque $L_{K/k,S}(0,\chi^{\alpha}) = L_{K/k,S}(0,\chi)^{\alpha}$, on a aussi $L_{K/k,S}(0,\chi^{\alpha})$ non nulle. De cette manière, l'application

$$\begin{array}{ccc} X & \longrightarrow & X\\ \chi & \longmapsto & \chi^{\alpha}\end{array}$$

réalise une bijection de X dans lui-même. En effet, comme α est bijectif, cette application est clairement surjective puisque $\chi = \alpha\circ\alpha^{-1}\circ\chi = (\chi^{\alpha^{-1}})^{\alpha}$. L'ensemble X étant fini, cela donne directement la bijectivité. On obtient donc finalement pour tout $\alpha\in\mathrm{Aut}(\mathbb{C})$

$$\alpha(x_g) = \frac{1}{|G|}\sum_{\chi\in X}\chi(1)L_{K/k,S}(0,\chi)\chi(g) = x_g.$$

Ainsi pour tout g dans G, x_g est fixé par tous les automorphismes de $\mathbb{C}$, donc en particulier par tous les $\mathbb{Q}$-automorphismes. Le théorème 2.14 permet donc de conclure que le coefficient x_g est rationnel pour tout $g\in G$, ce qui termine la preuve. □

L'élément de Brumer étant à coefficients rationnels, nous nous intéressons dans la section suivante à son dénominateur.

2.5. Dénominateur de $\theta_{K/k,S}$

La question du dénominateur de $\theta_{K/k,S}$ est certainement plus complexe. On peut se demander si tout comme dans le cas abélien, l'élément $w_K\theta_{K/k,S}$ est à

coefficients entiers. Des exemples numériques nous ont permis de voir que multiplier par w_K n'est pas suffisant en général, mais ont semblé indiquer que la multiplication de l'élément de Brumer par $|G|w_K$ appartenait à $\mathbb{Z}[G]$. Malheureusement cette expression ne nous permet pas de retrouver le dénominateur de $\theta_{K/k,S}$ lorsque G est abélien.

Nous allons en fait introduire un objet un peu plus fin que $|G|$, qui sera compatible avec nos connaissances du cas abélien. Notons m_G le plus petit commun multiple des cardinaux des classes de conjugaison de G :

$$m_G = \text{ppcm}\{|C| : C \text{ classe de conjugaison de } G\}.$$

On voit immédiatement que si le groupe G est abélien, la quantité m_G est triviale. Soit $\mathfrak{P}$ un idéal premier non ramifié de K, et $\sigma_{\mathfrak{P}}$ son morphisme de Frobenius associé à l'extension K/k. On note $\mathfrak{p}$ l'idéal premier de k au-dessous de $\mathfrak{P}$ et $\mathcal{N}(\mathfrak{p})$ la norme absolue de cet idéal.

Postulat. — *Pour presque tout idéal premier $\mathfrak{P}$ de K, $m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$.*

Le lemme suivant est une adaptation directe du lemme 1.1 de [**Tat84**] et porte sur le lien entre w_K et les termes de la forme $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))$.

Lemme 2.16. — *Soit $\mathcal{T}$ un ensemble contenant tous les idéaux premiers non ramifiés de K qui sont premiers avec w_K, excepté éventuellement un nombre fini d'entre eux. Alors l'annulateur du $\mathbb{Z}[G]$-module $\mu(K)$ est engendré sur $\mathbb{Z}$ par les éléments $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ où $\mathfrak{P}$ parcourt les idéaux premiers dans $\mathcal{T}$. De plus, on a l'égalité*

$$w_K \quad = \quad \text{pgcd}_{\substack{\mathfrak{P}\in\mathcal{T}\\ \sigma_{\mathfrak{P}}=1}}(1 - \mathcal{N}(\mathfrak{p})).$$

Démonstration. — Soit $\mathfrak{P}$ un idéal premier dans $\mathcal{T}$ et ζ une racine de l'unité dans K. Par définition du morphisme de Frobenius, on a $\zeta^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} \equiv 1 \mod (\mathfrak{P})$. Ainsi, il existe un élément y appartenant à $\mathfrak{P}$ vérifiant $\zeta^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} = 1 + y$. Mais alors

$$\left(\zeta^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}\right)^{w_K} = (1+y)^{w_K} = \sum_{l=0}^{w_K} \binom{w_K}{l} y^l$$

Supposons y non nul. Puisque ζ^{w_K} est triviale, en isolant les deux premiers termes de la somme et en simplifiant, on obtient donc

$$w_K = -\sum_{l=2}^{w_K} \binom{w_K}{l} y^{l-1} = -y \cdot \sum_{l=2}^{w_K} \binom{w_K}{l} y^{l-2}.$$

Ainsi lorsque y est non nul, w_K appartient à $\mathfrak{P}$, ce qui est contradictoire. On en conclut donc que $\zeta^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} = 1$. Par conséquent, pour tout $\mathfrak{P}$ appartenant à $\mathcal{T}$, $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ est un annulateur de $\mu(K)$. En particulier, si le Frobenius d'un idéal $\mathfrak{P}$ de $\mathcal{T}$ est trivial, alors w_K divise $(1 - \mathcal{N}(\mathfrak{p}))$.

En outre, puisque K/k est galoisienne, le théorème de Čebotarev implique que chaque élément g de G s'écrit comme le Frobenius $\sigma_{\mathfrak{P}}$ d'un certain idéal premier $\mathfrak{P}$ que l'on peut choisir dans $\mathcal{T}$. C'est pourquoi tout élément x de $\mathbb{Z}[G]$ peut s'écrire sous la forme $x = \sum_{\mathfrak{P}\in\mathcal{T}} \lambda_{\mathfrak{P}}\sigma_{\mathfrak{P}}$, où les $\lambda_{\mathfrak{P}}$ sont des éléments de $\mathbb{Z}$ presque tous nuls. On peut encore transformer ceci de manière à obtenir

$$x = \sum_{\mathfrak{P}\in\mathcal{T}} \lambda_{\mathfrak{P}}(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})) + \sum_{\mathfrak{P}\in\mathcal{T}} \lambda_{\mathfrak{P}}\mathcal{N}(\mathfrak{p}) = \sum_{\mathfrak{P}\in\mathcal{T}} \lambda_{\mathfrak{P}}(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})) + n$$

où n est un entier. On voit donc que x est un annulateur de $\mu(K)$ si et seulement si w_K divise n. Pour obtenir le résultat du lemme, il suffit donc de démontrer l'égalité sur w_K. En effet, w_K s'écrit alors sous la forme

$$w_K = \sum_{\substack{\mathfrak{P}\in\mathcal{T}\\ \sigma_{\mathfrak{P}}=1}} \mu_{\mathfrak{P}}(1 - \mathcal{N}(\mathfrak{p})),$$

pour une certaine suite à support fini $(\mu_{\mathfrak{P}})_{\mathfrak{P}}$ de $\mathbb{Z}$. Par suite, tout annulateur de $\mu(K)$ est combinaison linéaire à coefficients entiers de termes de la forme $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ pour $\mathfrak{P} \in \mathcal{T}$, ce qui prouve que les $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ pour $\mathfrak{P}$ parcourant $\mathcal{T}$ engendrent sur $\mathbb{Z}$ l'annulateur de $\mu(K)$ dans $\mathbb{Z}[G]$.

On a déjà vu que pour tout $\mathfrak{P}$ de $\mathcal{T}$ dont le morphisme de Frobenius $\sigma_{\mathfrak{P}}$ est trivial, w_K divise $1 - \mathcal{N}(\mathfrak{p})$. Soit w' un diviseur commun aux $1 - \mathcal{N}(\mathfrak{p})$, et ζ une racine primitive w'-ième de l'unité. Notre but est de démontrer que ζ appartient à K. On considère une extension finie L de K, galoisienne sur k qui contient ζ (on peut prendre par exemple la clôture galoisienne de $K(\zeta)/k$). Pour un morphisme ρ de $\mathrm{Gal}(L/k)$, il existe un idéal premier $\widetilde{\mathfrak{P}}$ de L dont ρ est le Frobenius associé à l'extension L/k. On peut de plus choisir $\widetilde{\mathfrak{P}}$ premier avec w' et au-dessus d'un idéal premier de K appartenant à $\mathcal{T}$, puisqu'il n'existe qu'un nombre fini de premiers de L ne vérifiant pas cette condition. Soit ρ un élément de $\mathrm{Gal}(L/K)$. Puisque $\rho_{|_K}$ est trivial, en notant $\mathfrak{P}$ l'idéal premier de K au-dessous de $\widetilde{\mathfrak{P}}$, le morphisme $\sigma_{\widetilde{\mathfrak{P}}_{|_K}} = \sigma_{\mathfrak{P}}$ est trivial. Par hypothèse sur w', l'élément w' divise donc $1-\mathcal{N}(\mathfrak{p})$, ce qui entraîne l'égalité entre $\zeta^{\mathcal{N}(\mathfrak{p})}$ et ζ. En utilisant alors la propriété du morphisme de Frobenius $\sigma_{\widetilde{\mathfrak{P}}}$ et l'égalité précédente, on trouve que $\zeta^{\rho} \equiv \zeta \mod (\widetilde{\mathfrak{P}})$. Puisque l'on a choisi $\widetilde{\mathfrak{P}}$ premier avec w', il en découle alors l'égalité $\zeta^{\rho} = \zeta$. Ainsi ζ appartient à K, ce qui implique que w' divise w_K. Le pgcd recherché est donc bien w_K. □

Remarque. — Ce résultat implique en particulier que pour tout élément ξ de $\mathbb{Z}[G]$ annulant $\mu(K)$, il existe une suite de $\mathbb{Z}$ à support fini, $(\lambda_{\mathfrak{P}}(\xi))_{\mathfrak{P}}$, vérifiant

$$\xi = \sum_{\mathfrak{P}\in\mathcal{T}} \lambda_{\mathfrak{P}}(\xi)(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})).$$

Ceci nous donne une formulation équivalente de notre postulat concernant l'élément de Brumer, explicitée dans le corollaire ci-dessous.

Corollaire 2.17. — *Les conditions suivantes sont équivalentes :*

1. *Pour presque tout idéal premier $\mathfrak{P}$ de K, $m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$.*
2. *Pour tout ξ appartenant à l'annulateur dans $\mathbb{Z}[G]$ de $\mu(K)$, l'élément $m_G\xi\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$.*

Lorsque le groupe G est abélien, on retrouve le résultat d'intégralité de $\xi\theta_{K/k,S}$, pour tout élément ξ dans $\mathbb{Z}[G]$ annulant $\mu(K)$. Ce résultat n'est pas facile à démontrer et repose sur l'étude des fonctions ζ partielles abéliennes. Les fonctions ζ partielles qui interviennent dans le cas non abélien ne sont définies pour l'instant qu'à l'aide des fonctions L d'Artin, ce qui rend leur étude délicate.

On supposera dans la suite le postulat concernant l'élément de Brumer vérifié. On verra plus tard que c'est effectivement le cas dans tous les exemples numériques effectués. Ceci implique que l'élément $m_G w_K \theta_{K/k,S}$ est à coefficients entiers. Ainsi dans l'optique d'établir une généralisation de la conjecture de Brumer-Stark au cas non abélien, on pourra appliquer cet élément aux idéaux fractionnaires de K.

CHAPITRE 3

CONJECTURE DE BRUMER-STARK NON ABÉLIENNE

Le but de ce chapitre est de généraliser la conjecture de Brumer-Stark au cas où l'extension de corps de nombres K/k considérée n'est plus supposée abélienne mais simplement galoisienne. On note comme précédemment G le groupe de Galois de K/k. De même, S désigne un ensemble fini de places de k contenant les places archimédiennes ainsi que les places finies qui se ramifient dans K, de cardinal supérieur ou égal à 2.

Dans tout le chapitre, on suppose le postulat concernant l'élément de Brumer vérifié. La validité de ce postulat entraîne l'appartenance de l'élément $m_G w_K \theta_{K/k,S}$ à l'anneau de groupe $\mathbb{Z}[G]$, ce qui permet d'étendre facilement la partie "Brumer" de la conjecture au cas non abélien. En revanche, la généralisation de la partie "Stark" est un peu plus technique. Nous allons voir que les extensions abéliennes vont continuer à jouer un rôle important dans la conjecture, cependant la condition d'abélianité est remplacée par une condition de centralité faisant intervenir des extensions galoisiennes centrales possédant des propriétés particulières.

3.1. Énoncé de la conjecture de Brumer-Stark non abélienne

3.1.1. Des équivalences utiles. — Avant de chercher à énoncer une conjecture non abélienne, on commence par démontrer plusieurs équivalences qui nous permettront de traduire autrement une condition d'abélianité analogue à celle intervenant dans la conjecture de Brumer-Stark abélienne. On rappelle que pour un idéal premier $\mathfrak{P}$ de K, on désigne par $\mathfrak{p}$ l'idéal premier de k vérifiant $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$ et par $\sigma_{\mathfrak{P}}$ le morphisme de Frobenius associé au premier $\mathfrak{P}$ et à l'extension K/k.

Proposition 3.1. — *Soient H un sous-groupe abélien de G et $\mathfrak{a}$ un idéal fractionnaire non nul de K. Les propositions suivantes sont équivalentes :*

(*i*). *Il existe $\alpha \in K^\circ$ tel que $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$ et tel que pour tout γ vérifiant $\gamma^{w_K} = \alpha$, l'extension $K(\gamma)$ est abélienne sur K^H.*

(*ii*). *Il existe une extension L de K, abélienne sur K^H ainsi qu'un élément $\gamma \in L^\circ$ tels que $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} \mathcal{O}_L = \gamma^{w_K} \mathcal{O}_L$.*

(*iii*). *Pour presque tout idéal premier* $\mathfrak{P}$ *de* K *tel que* $\sigma_{\mathfrak{P}}$ *appartient à* H*, il existe* $\alpha_{\mathfrak{P}} \in K^{\circ}$ *tel que* $\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta_{K/k,S}} = \alpha_{\mathfrak{P}}\mathcal{O}_K$ *et tel que* $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{Q})$ *pour tout idéal premier* $\mathfrak{Q}$ *de* K *vérifiant* $\mathfrak{Q} \cap \mathcal{O}_{K^H} = \mathfrak{P} \cap \mathcal{O}_{K^H}$*.*

(*iv*). *Il existe une famille finie de générateurs* $(a_i)_{i\in I}$ *de l'annulateur dans* $\mathbb{Z}[H]$ *de* $\mu(K)$*, noté* $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$*, et des éléments* $(\alpha_i)_{i\in I}$ *de* K° *tels que* $\mathfrak{a}^{m_G a_i \theta_{K/k,S}} = \alpha_i\mathcal{O}_K$ *et* ${\alpha_j}^{a_i} = {\alpha_i}^{a_j}$ *pour tous* i, j *dans* I*.*

Démonstration. — Cette proposition est une généralisation de la proposition 1.5. Dans le but de ne pas alourdir les notations, dans toute la preuve on note θ l'élément de Brumer au lieu de $\theta_{K/k,S}$.
$(i) \Rightarrow (ii)$: Posons γ tel que $\gamma^{w_K} = \alpha$. Si l'on nomme L l'extension $K(\gamma)$, γ est une anti-unité de L et L est abélienne sur K^H. De plus on a bien $\mathfrak{a}^{m_G w_K \theta}\mathcal{O}_L = \alpha\mathcal{O}_K\mathcal{O}_L = \gamma^{w_K}\mathcal{O}_L$.

$(ii) \Rightarrow (iii)$: Soit M une extension finie de L galoisienne sur k (on peut prendre par exemple pour M la clôture galoisienne de l'extension L/k). On considère les idéaux premiers $\mathfrak{P}$ de K non ramifiés, premiers avec w_K ainsi qu'avec $\mathfrak{a}^{m\theta}$ pour tout entier non nul $m \in \mathbb{Z}$ vérifiant $m\theta \in \mathbb{Z}[G]$, et dont le morphisme de Frobenius, $\sigma_{\mathfrak{P}}$ est dans H. On suppose de plus que $\mathfrak{P}$ ne se ramifie pas dans M. Pour un tel idéal premier $\mathfrak{P}$, on choisit un idéal premier de M, noté $\widetilde{\mathfrak{P}}$, divisant $\mathfrak{P}$, et on note $\sigma_{\widetilde{\mathfrak{P}}}$ son morphisme de Frobenius associé à l'extension M/k. Puisque $\sigma_{\mathfrak{P}}$ appartient à H, il laisse fixe K^H, et il en va de même pour $\sigma_{\widetilde{\mathfrak{P}}}$ qui est un relèvement de $\sigma_{\mathfrak{P}}$ à M. Ainsi, $\sigma_{\widetilde{\mathfrak{P}}}$ est dans le groupe de Galois de M/K^H, et puisque L est galoisienne sur K^H, la restriction de $\sigma_{\widetilde{\mathfrak{P}}}$ à L, $\sigma_{\widetilde{\mathfrak{P}}_{|_L}}$, appartient à $\mathrm{Gal}(L/K^H)$. On obtient

$$\begin{aligned}
\mathfrak{a}^{m_G w_K(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\mathcal{O}_L &= \left(\mathfrak{a}^{m_G w_K\theta}\right)^{(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))}\mathcal{O}_L \\
&= \left(\mathfrak{a}^{m_G w_K\theta}\mathcal{O}_L\right)^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))} \\
&= \left(\gamma^{w_K}\mathcal{O}_L\right)^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))} \\
&= \left(\gamma^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))}\mathcal{O}_L\right)^{w_K}.
\end{aligned}$$

Ceci donne ensuite, en utilisant l'égalité entre les idéaux $\mathcal{O}_L^{w_K}$ et $\mathcal{O}_L$, puis en mettant en facteur la puissance w_K dans le terme de gauche

$$\left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\mathcal{O}_L\right)^{w_K} = \left(\gamma^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))}\mathcal{O}_L\right)^{w_K},$$

d'où finalement

$$\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\mathcal{O}_L = \gamma^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))}\mathcal{O}_L.$$

Posons alors $\alpha_{\mathfrak{P}} = \gamma^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))} = \gamma^{(\sigma_{\widetilde{\mathfrak{P}}_{|_L}}-\mathcal{N}(\mathfrak{p}))}$. On remarque que l'élément $\alpha_{\mathfrak{P}}$ ne dépend pas du choix de l'idéal premier $\widetilde{\mathfrak{P}}$ au-dessus de $\mathfrak{P}$. En effet, si l'on prend $\widetilde{\mathfrak{P}}'$ un tel autre idéal, alors il existe $\rho \in \mathrm{Gal}(M/K)$ tel que $\widetilde{\mathfrak{P}}' = \rho(\widetilde{\mathfrak{P}})$. De plus, $\sigma_{\widetilde{\mathfrak{P}}}$ et $\sigma_{\widetilde{\mathfrak{P}}'}$ sont conjugués par ρ. Or ces trois morphismes appartiennent au groupe de Galois $\mathrm{Gal}(M/K^H)$, donc leurs restrictions à L respectives sont dans $\mathrm{Gal}(L/K^H)$ qui est abélien. Ceci implique en particulier que les restrictions $\sigma_{\widetilde{\mathfrak{P}}_{|_L}}$ et $\sigma_{\widetilde{\mathfrak{P}}'_{|_L}}$

sont égales, ainsi $\alpha_{\mathfrak{P}}$ ne dépend pas du choix de $\widetilde{\mathfrak{P}}$. En fait on a même l'égalité $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{Q}}$ pour tout $\mathfrak{Q}$ premier de K conjugué à $\mathfrak{P}$ dans H. On considère un idéal premier $\mathfrak{Q}$ de K vérifiant $\mathfrak{Q} \cap \mathcal{O}_{K^H} = \mathfrak{P} \cap \mathcal{O}_{K^H}$, et l'on choisit un idéal premier $\widetilde{\mathfrak{Q}}$ de M au-dessus de $\mathfrak{Q}$. Alors $\widetilde{\mathfrak{P}}$ et $\widetilde{\mathfrak{Q}}$ divisent le même idéal premier de K^H, ils sont donc conjugués par un élément de $\mathrm{Gal}(M/K^H)$. On peut donc trouver un élément ρ de $\mathrm{Gal}(M/K^H)$ tel que $\widetilde{\mathfrak{Q}} = \rho\left(\widetilde{\mathfrak{P}}\right)$. Comme précédemment, l'abélianité de $\mathrm{Gal}(L/K^H)$ implique alors l'égalité entre $\sigma_{\widetilde{\mathfrak{P}}|_L}$ et $\sigma_{\widetilde{\mathfrak{Q}}|_L}$, ce qui démontre que les éléments $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{Q}}$ sont égaux, pour tout $\mathfrak{Q}$ premier de K conjugué à $\mathfrak{P}$ dans H.

Montrons maintenant que $\alpha_{\mathfrak{P}}$ est dans K. Pour cela, on montre que $\alpha_{\mathfrak{P}}$ est fixé par tout automorphisme ρ de $\mathrm{Gal}(L/K)$. Soit ρ appartenant au groupe de Galois de L/K. On a le diagramme suivant :

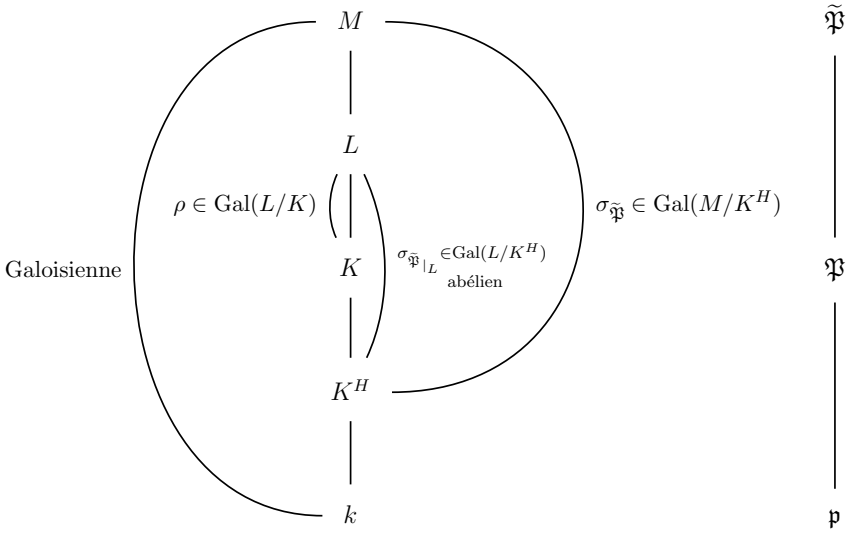


FIGURE 3.1. Diagramme des corps intervenant dans l'implication $(ii) \Rightarrow (iii)$

Puisque $\mathfrak{a}$ est un idéal fractionnaire de K, $\mathfrak{a}$ est fixé par ρ, donc $\mathfrak{a}^{\rho-1} = \mathcal{O}_K$. On a d'une part

$$\begin{aligned} \left(\mathfrak{a}^{m_G w_K \theta}\mathcal{O}_L\right)^{(\rho-1)} &= \mathfrak{a}^{m_G(\rho_{|K}-1)w_K\theta}\mathcal{O}_L \\ &= \mathcal{O}_K\mathcal{O}_L \\ &= \mathcal{O}_L, \end{aligned}$$

et d'autre part

$$\begin{aligned} \left(\mathfrak{a}^{m_G w_K \theta}\mathcal{O}_L\right)^{(\rho-1)} &= \left(\gamma^{w_K}\mathcal{O}_L\right)^{(\rho-1)} \\ &= \left(\gamma^{\rho-1}\mathcal{O}_L\right)^{w_K}. \end{aligned}$$

Ainsi $\gamma^{\rho-1}\mathcal{O}_L = \mathcal{O}_L$ et donc $\gamma^{\rho-1}$ est une unité de L. Or les anti-unités qui sont inversibles dans L sont en fait les racines de l'unité de L. Comme γ appartient à L°, il en est de même pour $\gamma^{\rho-1}$, ce qui prouve que $\gamma^{\rho-1}$ est une racine de l'unité de L.

Puisque $\sigma_{\widetilde{\mathfrak{P}}}$ est le morphisme de Frobenius de $\widetilde{\mathfrak{P}}$ associé à l'extension M/k, la quantité $\sigma_{\widetilde{\mathfrak{P}}} - \mathcal{N}(\mathfrak{p})$ est dans l'annulateur $\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(M/k)]}(\mu(M))$. En particulier, cette quantité est aussi un annulateur de $\mu(L)$. C'est pourquoi $\left(\gamma^{\rho-1}\right)^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} = 1$. D'un autre côté, on a aussi

$$\left(\gamma^{\rho-1}\right)^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} = \gamma^{(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))(\rho-1)} = \gamma^{(\sigma_{\widetilde{\mathfrak{P}}|_L}-\mathcal{N}(\mathfrak{p}))(\rho-1)}.$$

Puisque ρ est dans $\mathrm{Gal}(L/K)$ qui est lui-même un sous-groupe du groupe abélien $\mathrm{Gal}(L/K^H)$, on peut alors permuter ρ et $\sigma_{\widetilde{\mathfrak{P}}|_L}$ pour finalement obtenir $(\gamma^{\rho-1})^{\sigma_{\widetilde{\mathfrak{P}}|_L}-\mathcal{N}(\mathfrak{p})} = \left(\gamma^{\sigma_{\widetilde{\mathfrak{P}}|_L}-\mathcal{N}(\mathfrak{p})}\right)^{\rho-1}$, d'où l'égalité $\alpha_{\mathfrak{P}}^{\rho-1} = 1$, ce qui prouve que l'élément $\alpha_{\mathfrak{P}}$ est dans K. En outre, comme γ est une anti-unité, α est aussi une anti-unité, donc appartient à K°.

Étant donné que nous avons supposé la quantité $m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta$ dans $\mathbb{Z}[G]$, l'idéal $\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}$ est un idéal fractionnaire de K. L'égalité suivante, valable pour tout idéal premier $\check{\mathfrak{Q}}$ de L, devient donc

$$\begin{aligned} v_{\check{\mathfrak{Q}}}\left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\mathcal{O}_L\right) &= v_{\check{\mathfrak{Q}}}\left(\alpha_{\mathfrak{P}}\mathcal{O}_L\right) \\ i.e \quad v_{\mathfrak{Q}}\left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\right) e\left(\check{\mathfrak{Q}}/\mathfrak{Q}\right) &= v_{\mathfrak{Q}}\left(\alpha_{\mathfrak{P}}\right) e\left(\check{\mathfrak{Q}}/\mathfrak{Q}\right), \end{aligned}$$

où $\mathfrak{Q}$ désigne l'idéal premier de K au-dessous de $\check{\mathfrak{Q}}$ et $e\left(\check{\mathfrak{Q}}/\mathfrak{Q}\right)$ l'indice de ramification de $\check{\mathfrak{Q}}$ sur $\mathfrak{Q}$. On obtient finalement $v_{\mathfrak{Q}}\left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\right) = v_{\mathfrak{Q}}\left(\alpha_{\mathfrak{P}}\right)$ pour tout idéal premier $\mathfrak{Q}$ de K. L'idéal fractionnaire de K, $\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}$, est donc principal et engendré par $\alpha_{\mathfrak{P}}$.

Il reste à montrer la condition de congruence. On commence par établir que $\alpha_{\mathfrak{P}}$ est congru à 1 modulo* $\mathfrak{P}$. Pour cela, il suffit que $\alpha_{\mathfrak{P}}$ s'écrive comme un quotient de deux éléments entiers de K, notés a, b, premiers avec $\mathfrak{P}$ et qui vérifient $a \equiv b \bmod^*(\mathfrak{P})$. L'idéal $\mathfrak{P}$ ayant été choisi premier avec les idéaux divisant $\mathfrak{a}^{m\theta}$ pour m un entier relatif non nul vérifiant $m\theta \in \mathbb{Z}[G]$, $\mathfrak{P}$ est en particulier premier avec $\mathfrak{a}^{m_G w_K \theta}\mathcal{O}_L = \gamma^{w_K}\mathcal{O}_L$. Ainsi, γ est premier avec $\mathfrak{P}$. Il existe donc $x, y \in \mathcal{O}_L$, premiers avec $\mathfrak{P}$, tels que $\gamma = x \cdot y^{-1}$, ce qui nous permet d'écrire $\alpha_{\mathfrak{P}}$ sous la forme $\alpha_{\mathfrak{P}} = \gamma^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} = x^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} \cdot \left(y^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})}\right)^{-1}$. Comme x et y sont des entiers de L, donc des entiers de M, par définition du morphisme de Frobenius, on a $x^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} \equiv 1 \mod(\widetilde{\mathfrak{P}})$ ainsi que $y^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} \equiv 1 \mod(\widetilde{\mathfrak{P}})$. On obtient $\alpha_{\mathfrak{P}} \equiv 1 \bmod^*(\widetilde{\mathfrak{P}})$. Ce qui signifie que $v_{\widetilde{\mathfrak{P}}}(\alpha_{\mathfrak{P}} - 1) \geq v_{\widetilde{\mathfrak{P}}}\left(\widetilde{\mathfrak{P}}\right) = 1$. De plus, comme $\alpha_{\mathfrak{P}}$ appartient à K, on a l'égalité $v_{\widetilde{\mathfrak{P}}}(\alpha_{\mathfrak{P}} - 1) = v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - 1)\, e\left(\widetilde{\mathfrak{P}}/\mathfrak{P}\right) = v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - 1)$ puisque $\mathfrak{P}$ ne se ramifie pas dans M. On trouve donc $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - 1) \geq 1 = v_{\mathfrak{P}}(\mathfrak{P})$, ce qui prouve que $\alpha_{\mathfrak{P}} \equiv 1 \bmod^*(\mathfrak{P})$. Puisque l'on a montré précédemment que pour tout idéal premier $\mathfrak{Q}$ de K divisant le même idéal premier de K^H que $\mathfrak{P}$, les éléments $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{Q}}$ sont égaux, l'identité $\alpha_{\mathfrak{Q}} \equiv 1 \bmod^*(\mathfrak{Q})$ nous donne la relation $\alpha_{\mathfrak{P}} \equiv 1 \bmod^*(\mathfrak{Q})$, et le résultat voulu.

$(iii) \Rightarrow (iv)$: On veut montrer qu'il existe une famille finie de générateurs $(a_i)_{i\in I}$ de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$ et des éléments $(\alpha_i)_{i\in I}$ de K° tels que $\mathfrak{a}^{m_G a_i \theta} = \alpha_i \mathcal{O}_K$ et ${\alpha_i}^{a_j} = {\alpha_j}^{a_i}$ pour tous i, j dans I. Appelons $\mathcal{T}$ l'ensemble des idéaux premiers

de K vérifiant la condition (iii) et premiers avec w_K, alors d'après le lemme 2.16, on sait que les éléments $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ pour $\mathfrak{P} \in \mathcal{T}$ engendrent l'annulateur $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$. De plus, la condition (iii) nous donne la condition de principalité concernant $\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta}$. Il ne reste plus qu'à prouver que pour deux idéaux premiers distincts de $\mathcal{T}$, $\mathfrak{P}$ et $\mathfrak{P}'$, les éléments $\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')}$ et $\alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}$ sont égaux.

En premier lieu, on remarque qu'ils engendrent le même idéal de K. En effet,

$$\begin{aligned} \alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}\mathcal{O}_K &= (\alpha_{\mathfrak{P}'}\mathcal{O}_K)^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} \\ &= \left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}'))\theta}\right)^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} \\ &= \mathfrak{a}^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))(\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}'))\theta}. \end{aligned}$$

Comme les morphismes $\sigma_{\mathfrak{P}}$ et $\sigma_{\mathfrak{P}'}$ appartiennent tous deux au groupe H qui est abélien, on peut permuter $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))$ et $(\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}'))$, ce qui nous permet d'obtenir

$$\begin{aligned} \alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}\mathcal{O}_K &= \mathfrak{a}^{m_G(\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}'))(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta} \\ &= \left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta}\right)^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \\ &= (\alpha_{\mathfrak{P}}\mathcal{O}_K)^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \\ &= \alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')}\mathcal{O}_K. \end{aligned}$$

Puisqu'ils engendrent le même idéal, il existe une unité u de K vérifiant $\alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} = u\,\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')}$. Du reste, $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{P}'}$ étant des anti-unités de K, il en est de même de $\alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}$ et $\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')}$. Ainsi u est aussi une anti-unité de K, c'est donc finalement une racine de l'unité de K. Notre but est de montrer que cette racine de l'unité est triviale, en nous servant des conditions de congruences vérifiées par $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{P}'}$. De la même manière que dans la preuve de l'implication $(i) \Rightarrow (ii)$, en utilisant uniquement la définition du morphisme de Frobenius on montre facilement que $\alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} \equiv 1 \mod^*(\mathfrak{P})$. D'autre part, puisque $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{Q})$ pour tout idéal $\mathfrak{Q}$ conjugué à $\mathfrak{P}$ par un élément de H, on peut écrire $\alpha_{\mathfrak{P}}$ sous la forme $\alpha_{\mathfrak{P}} = x \cdot y^{-1}$ avec x et y des entiers de K vérifiant $x \equiv y \mod (\mathfrak{Q})$ pour de tels idéaux premiers $\mathfrak{Q}$. Puisque $\sigma_{\mathfrak{P}'}$ appartient à H, l'idéal premier ${\sigma_{\mathfrak{P}'}}^{-1}(\mathfrak{P})$ est conjugué à $\mathfrak{P}$ par un élément de H, et ainsi on a en particulier $x \equiv y \mod ({\sigma_{\mathfrak{P}'}}^{-1}(\mathfrak{P}))$. En appliquant $\sigma_{\mathfrak{P}'}$ à cette identité, on trouve $x^{\sigma_{\mathfrak{P}'}} \equiv y^{\sigma_{\mathfrak{P}'}} \mod (\mathfrak{P})$, ce qui nous donne $x^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \equiv y^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \mod^*(\mathfrak{P})$. Par conséquent, on obtient $\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \equiv 1 \mod^*(\mathfrak{P})$. Alors

$$u\,\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} = \alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} \equiv 1 \mod^*(\mathfrak{P})$$

et puisque $\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p}')} \equiv 1 \mod^*(\mathfrak{P})$, on trouve en définitive $u \equiv 1 \mod^*(\mathfrak{P})$. L'idéal $\mathfrak{P}$ ayant été choisi premier avec w_K, on en déduit que la racine u est égale à 1, ce qui nous donne l'égalité voulue entre $\alpha_{\mathfrak{P}}^{\sigma_{\mathfrak{P}'} - \mathcal{N}(\mathfrak{p})}$ et $\alpha_{\mathfrak{P}'}^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})}$.

$(iv) \Rightarrow (i)$: On suppose qu'il existe une famille finie de générateurs $(a_i)_{i \in I}$ de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$ et des anti-unités de K, $(\alpha_i)_{i \in I}$, telles que $\mathfrak{a}^{m_G a_i \theta} = \alpha_i \mathcal{O}_K$ et

$\alpha_i^{a_j} = \alpha_j^{a_i}$ pour tous i, j dans I. Commençons par démontrer que s'il existe des α_i vérifiant ces deux conditions pour un système de générateurs de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$ donné, alors de tels éléments existent pour tout autre système de générateurs. Soit $(b_j)_{j\in J}$ une famille finie de générateurs de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$. Alors pour tout j dans J, on peut écrire b_j sous la forme $b_j = \sum_{i\in I} b_{j,i}a_i$, où les $b_{j,i}$ sont des éléments de $\mathbb{Z}[H]$. Si l'on remplace b_j par cette expression dans le calcul de $\mathfrak{a}^{m_G b_j\theta}$, on obtient

$$\begin{aligned}
\mathfrak{a}^{m_G b_j\theta} &= \mathfrak{a}^{m_G\left(\sum_{i\in I} b_{j,i}a_i\right)\theta} \\
&= \prod_{i\in I}\left(\mathfrak{a}^{m_g a_i\theta}\right)^{b_{j,i}} \\
&= \prod_{i\in I}\left(\alpha_i\mathcal{O}_K\right)^{b_{j,i}} \\
&= \left(\prod_{i\in I}\alpha_i^{b_{j,i}}\right)\mathcal{O}_K.
\end{aligned}$$

On pose alors, pour tout j dans J, $\beta_j = \prod_{i\in I}\alpha_i^{b_{j,i}}$ qui appartient à K° d'après les propriétés des α_i. En outre, pour j appartenant à J,

$$\beta_j^{b_l} = \left(\prod_{i\in I}\alpha_i^{b_{j,i}}\right)^{b_l} = \prod_{i\in I}\alpha_i^{\sum_{k\in I} b_{l,k}a_k b_{j,i}}.$$

L'anneau de groupe $\mathbb{Z}[H]$ étant commutatif, on peut permuter les $b_{j,i}$, $b_{l,k}$ ainsi que les a_k entre eux, d'où

$$\begin{aligned}
\beta_j^{b_l} &= \prod_{i\in I}\alpha_i^{\sum_{k\in I} b_{l,k}b_{j,i}a_k} \\
&= \prod_{i\in I}\prod_{k\in I}(\alpha_i^{a_k})^{b_{j,i}b_{l,k}} \\
&= \prod_{i\in I}\prod_{k\in I}(\alpha_k^{a_i})^{b_{j,i}b_{l,k}} \\
&= \prod_{k\in I}\left(\prod_{i\in I}\alpha_k^{b_{j,i}a_i}\right)^{b_{l,k}}.
\end{aligned}$$

Ce qui donne

$$\beta_j^{b_l} = \prod_{k\in I}\left(\alpha_k^{\sum_{i\in I} b_{j,i}a_i}\right)^{b_{l,k}} = \prod_{k\in I}(\alpha_k^{b_j})^{b_{l,k}} = \left(\prod_{k\in I}\alpha_k^{b_{l,k}}\right)^{b_j} = \beta_l^{b_j}.$$

Ainsi si la condition (iv) est vraie pour un système de générateurs de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$, elle est vraie pour n'importe quel autre système de générateurs donc on peut choisir le système qui nous convient. Pour tout élément h de H, on choisit un entier n_h vérifiant pour toute racine de l'unité $\zeta \in \mu(K)$, $\zeta^h = \zeta^{n_h}$. L'existence de tels n_h provient du fait que l'image d'une racine de l'unité par un automorphisme est une racine de l'unité du même ordre et que

le groupe des racines de l'unité est cyclique. On prend alors comme système de générateurs de $\mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K))$, w_K et les $(h-n_h)_{h\in H}$. Par hypothèse, il existe $\alpha \in K^\circ$ et $\alpha_h \in K^\circ$ tels que $\mathfrak{a}^{m_G w_K \theta} = \alpha\mathcal{O}_K$ et $\mathfrak{a}^{m_G(h-n_h)\theta} = \alpha_h\mathcal{O}_K$ pour tout h dans H. Considérons γ une racine w_K-ième de α et posons $L = K(\gamma)$. Cette extension ne dépend pas du choix de γ. Prenons h dans H et désignons par $\widetilde{h}$ un prolongement quelconque de h à L. On a alors

$$(\gamma^{\widetilde{h}})^{w_K} = \widetilde{h}(\gamma^{w_K}) = h(\alpha),$$

d'où

$$(\gamma^{\widetilde{h}-n_h})^{w_K} = \alpha^{h-n_h}.$$

En utilisant alors l'hypothèse d'égalité entre α^{h-n_h} et $\alpha_h^{w_K}$, on obtient finalement $(\gamma^{\widetilde{h}-n_h})^{w_K} = \alpha_h^{w_K}$. Il existe donc une racine de l'unité de K, notée ζ, telle que $\gamma^{\widetilde{h}-n_h} = \zeta\alpha_h$, ce qui entraîne

$$\gamma^{\widetilde{h}} = \gamma^{n_h}\zeta\alpha_h \in L = K(\gamma).$$

Donc si l'on choisit n'importe quel relèvement d'un élément de H à L, l'image de L par ce relèvement reste encore dans L, donc L est galoisienne sur K^H.

Montrons que l'extension L/K^H est abélienne. Soient $\widetilde{h}$, $\widetilde{g}$ deux éléments de $\mathrm{Gal}(L/K^H)$. On note h (resp. g) la restriction de $\widetilde{h}$ (resp. $\widetilde{g}$) à K. Puisque $\widetilde{h}$ et $\widetilde{g}$ commutent lorsqu'ils agissent sur un élément de K, il reste à étudier leur comportement sur γ. On a

$$\begin{aligned}
(\gamma^{\widetilde{h}-n_h})^{(\widetilde{g}-n_g)} &= (\zeta\alpha_h)^{(\widetilde{g}-n_g)} \\
&= \zeta^{\widetilde{g}-n_g}\alpha_h^{\widetilde{g}-n_g} \\
&= \zeta^{g-n_g}\alpha_h^{g-n_g} \\
&= \alpha_h^{g-n_g} \qquad \text{puisque } g-n_g \in \mathrm{Ann}_{\mathbb{Z}[H]}(\mu(K)) \\
&= \alpha_g^{h-n_h} \\
&= (\gamma^{\widetilde{g}-n_g})^{(\widetilde{h}-n_h)}.
\end{aligned}$$

On en déduit donc que $\gamma^{\widetilde{h}\widetilde{g}} = \gamma^{\widetilde{g}\widetilde{h}}$. Ainsi $\widetilde{h}\widetilde{g} = \widetilde{g}\widetilde{h}$ et $\mathrm{Gal}(L/K^H)$ est abélien, ce qui termine la preuve. □

3.1.2. Énoncé de la conjecture. — Avant d'énoncer notre conjecture de Brumer-Stark non abélienne, on commence par démontrer l'équivalence de plusieurs propositions qui nous donnent des formulations équivalentes de la conjecture. Pour cela, il nous faut introduire du vocabulaire supplémentaire.

Définition 3.2. — Soit L une extension de K. On dira que l'extension L est une *extension centrale* de K/k si L est galoisienne sur k et si le groupe $\mathrm{Gal}(L/k)$ est une extension centrale du groupe $\mathrm{Gal}(K/k)$, *i.e* on a une suite exacte $1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$ telle que $\mathrm{Gal}(L/K)$ est inclus dans le centre de $\mathrm{Gal}(L/k)$.

Définition 3.3. — Pour une extension L de K, galoisienne sur k, on notera I_L l'ensemble des commutateurs du groupe de Galois de L/k. On dira que L vérifie la *propriété de centralité* si l'intersection entre I_L et le groupe de Galois $\mathrm{Gal}(L/K)$ est triviale.

Proposition 3.4. — *Si L vérifie la propriété de centralité, alors L est une extension centrale de K/k.*

Démonstration. — Notons Γ_L le groupe de Galois de L/k et C_L celui de L/K. Puisque L est galoisienne sur k, on dispose de la suite exacte suivante

$$1 \longrightarrow C_L \longrightarrow \Gamma_L \xrightarrow{s} G \longrightarrow 1$$

où s désigne l'application de restriction à K. On veut montrer que C_L est inclus dans le centre de Γ_L. Soit ρ un élément de Γ_L et c dans C_L. Alors on a $s(\rho c \rho^{-1} c^{-1}) = s(\rho)s(c)s(\rho)^{-1}s(c)^{-1}$, et comme C_L est le noyau de s, on obtient $s(\rho c \rho^{-1} c^{-1}) = s(\rho)s(\rho)^{-1} = \mathrm{Id}_G$. Le commutateur $[\rho, c]$ appartient donc à $C_L \cap I_L$, et d'après l'hypothèse sur L, il est trivial. Ceci implique que ρ et c commutent et démontre que L est bien une extension centrale de K/k. □

La seconde observation que l'on peut faire lorsque L vérifie la propriété de centralité concerne des liens entre les cardinaux des classes de conjugaisons de G et de celles de Γ_L.

Proposition 3.5. — *Soit L une extension de K vérifiant la propriété de centralité. Notons m_{Γ_L} le plus petit commun multiple des classes de conjugaison de $\Gamma_L = \mathrm{Gal}(L/k)$. Alors les nombres m_G et m_{Γ_L} sont égaux.*

Démonstration. — Considérons une classe de conjugaison notée C_ρ de Γ_L. On peut écrire C_ρ sous la forme $C_\rho = \{\delta\rho\delta^{-1} \mid \delta \in \Gamma_L\} = \{\delta_1, \ldots, \delta_r\}$ où les éléments δ_i sont tous distincts deux à deux. Si l'on désigne par $\mathrm{Res}_K(C_\rho)$ l'ensemble des éléments de C_ρ restreints à K, on s'aperçoit aisément que $\mathrm{Res}_K(C_\rho)$ correspond à la classe de conjugaison dans G de l'élement $\rho_{|K}$. Notre but est de comparer les cardinaux de C_ρ et de $\mathrm{Res}_K(C_\rho)$. Supposons que pour $i, j \in \{1, \ldots, r\}$ les restrictions à K des automorphismes δ_i et δ_j soient égales, alors en particulier $\delta_{i|_K}$ et $\delta_{j|_K}$ commutent. Le commutateur $[\delta_{i|_K}, \delta_{j|_K}] = [\delta_i, \delta_j]_{|K}$ est donc trivial. Ainsi $[\delta_i, \delta_j]$ fixe K, donc appartient à C. Puisque L vérifie la propriété de centralité, ce commutateur est en réalité trivial, ce qui implique l'égalité entre δ_i et δ_j. Ceci n'étant possible que si les entiers i et j sont égaux, on en déduit que le nombre d'éléments de C_ρ et celui de $\mathrm{Res}_K(C_\rho)$ sont les mêmes. Comme toute classe de conjugaison de G peut être vue comme la restriction de la classe de conjugaison d'un élément de Γ_L, on obtient une bijection entre l'ensemble des classes de G et l'ensemble des restrictions à K des classes de Γ_L. On en déduit en particulier que l'ensemble des cardinaux des classes de conjugaison de Γ_L est le même que l'ensemble des cardinaux des classes de G, ce qui nous permet d'aboutir à l'égalité entre m_G et m_{Γ_L}. □

Le résultat suivant donne des caractérisations équivalentes des idéaux principaux de la forme $\mathfrak{a}^{m_G w_K \theta_{K/k,s}}$ pour un certain idéal fractionnaire $\mathfrak{a}$ de K, admettant des générateurs dont les racines w_K-ièmes engendrent sur K des extensions vérifiant la propriété de centralité.

Théorème 3.6. — *Soit $\mathfrak{a}$ un idéal fractionnaire non nul de K. Les propositions suivantes sont équivalentes :*

1. *Il existe $\alpha \in K^\circ$ tel que $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$ et pour tout γ tel que $\gamma^{w_K} = \alpha$, l'extension $K(\gamma)$ est galoisienne sur k et vérifie la propriété de centralité.*
2. *Pour presque tout idéal premier $\mathfrak{P}$ de K, il existe $\alpha_\mathfrak{P} \in K^\circ$ tel que $\mathfrak{a}^{m_G(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}} = \alpha_\mathfrak{P} \mathcal{O}_K$ et $\alpha_\mathfrak{P} \equiv 1 \mod^*(\mathfrak{Q})$ pour tout idéal premier $\mathfrak{Q}$ de K au-dessus de $\mathfrak{p}$ tel que $\sigma_\mathfrak{Q} = \sigma_\mathfrak{P}$.*
3. *Il existe $\alpha \in K^\circ$ tel que $\alpha^{m_G w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$ et pour tout γ vérifiant $\gamma^{w_K} = \alpha$, pour tout sous-groupe abélien H de G, l'extension $K(\gamma)$ est abélienne sur le sous-corps fixé par H, noté K^H.*

Démonstration. — On note à nouveau de manière simplifiée l'élément de Brumer θ tout au long de la preuve.
$(1 \Rightarrow 2)$: On suppose l'assertion 1 vraie. Notons L l'extension $K(\gamma)$. Soit $\mathfrak{P}$ un idéal premier de K non ramifié. On suppose de plus que $\mathfrak{P}$ ne se ramifie pas dans L et est premier avec w_K, ainsi qu'avec $\mathfrak{a}^{m\theta}$ pour tout entier m non nul vérifiant $m\theta \in \mathbb{Z}[G]$.

Soient $\widetilde{\mathfrak{P}}$ un idéal premier de L au-dessus de $\mathfrak{P}$ et $\sigma_{\widetilde{\mathfrak{P}}}$ le morphisme de Frobenius associé à $\widetilde{\mathfrak{P}}$ et à l'extension L/k. La restriction de $\sigma_{\widetilde{\mathfrak{P}}}$ à K, notée $\sigma_{\widetilde{\mathfrak{P}}|_K}$, correspond au morphisme de Frobenius de $\mathfrak{P}$ associé à l'extension K/k.

Posons alors $\alpha_\mathfrak{P} = \gamma^{\sigma_{\widetilde{\mathfrak{P}}} - \mathcal{N}(\mathfrak{p})}$ et vérifions que l'élément $\alpha_\mathfrak{P}$ est bien défini. On est donc ramené à démontrer que $\alpha_\mathfrak{P} = \gamma^{\sigma_{\widetilde{\mathfrak{P}}} - \mathcal{N}(\mathfrak{p})}$ ne dépend pas du premier $\widetilde{\mathfrak{P}}$ de L choisi au-dessus de $\mathfrak{P}$.

$$\begin{array}{ccc} L = K(\gamma) & & \widetilde{\mathfrak{P}}, \widetilde{\mathfrak{P}}' \\ | & & \\ K & & \mathfrak{P} \\ | & & \\ k & & \mathfrak{p} \end{array}$$

Soient donc $\widetilde{\mathfrak{P}}$ et $\widetilde{\mathfrak{P}}'$ deux idéaux premiers de L au-dessus de $\mathfrak{P}$. Alors il existe ρ dans $\mathrm{Gal}(L/K)$ tel que $\widetilde{\mathfrak{P}}' = \rho\left(\widetilde{\mathfrak{P}}\right)$, d'où l'identité suivante entre les morphismes de Frobenius $\sigma_{\widetilde{\mathfrak{P}}'} = \rho \sigma_{\widetilde{\mathfrak{P}}} \rho^{-1}$. Or l'extension L est une extension centrale de K/k donc ρ commute avec tous les éléments de $\mathrm{Gal}(L/k)$, et ainsi $\rho \sigma_{\widetilde{\mathfrak{P}}} \rho^{-1} = \sigma_{\widetilde{\mathfrak{P}}}$. On trouve donc finalement que les idéaux premiers de L au-dessus de $\mathfrak{P}$ ont tous le même morphisme de Frobenius, et donc l'élément $\alpha_\mathfrak{P}$ ne dépend pas de l'idéal premier de L choisi au-dessus de $\mathfrak{P}$.

Montrons que $\alpha_{\mathfrak{P}}$ appartient à K. Soit g un élément de $\mathrm{Gal}(L/K)$. Notre but est d'établir que $\alpha_{\mathfrak{P}}^{g-1}$ est trivial. On a

$$\left(\alpha_{\mathfrak{P}}^{(g-1)}\right)^{w_K} = \gamma^{w_K(g-1)(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))} = \left(\gamma^{w_K}\right)^{(g-1)(\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p}))}.$$

Puisque γ élevé à la puissance w_K est égal à α, on obtient donc

$$\left(\alpha_{\mathfrak{P}}^{(g-1)}\right)^{w_K} = \left(\alpha^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})}\right)^{(g-1)} = \underbrace{\left(\alpha^{\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p})}\right)}_{\in K}^{(g-1)} = 1.$$

Donc, il existe une racine de l'unité ζ dans K, telle que $\alpha_{\mathfrak{P}}^{(g-1)} = \zeta$. Par définition du morphisme de Frobenius, il est facile de voir que $\gamma^{\sigma_{\widetilde{\mathfrak{P}}}-\mathcal{N}(\mathfrak{p})} \equiv 1 \mod^*(\widetilde{\mathfrak{P}})$, ainsi $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\widetilde{\mathfrak{P}})$ quel que soit $\widetilde{\mathfrak{P}}$ au-dessus de $\mathfrak{P}$. En particulier, pour $\widetilde{\mathfrak{P}}$ fixé au-dessus de $\mathfrak{P}$, on a $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(g^{-1}(\widetilde{\mathfrak{P}}))$, d'où $g(\alpha_{\mathfrak{P}}) \equiv 1 \mod^*(\widetilde{\mathfrak{P}})$. Ceci nous permet de voir que $\alpha_{\mathfrak{P}}^{(g-1)} \equiv 1 \mod^*(\widetilde{\mathfrak{P}})$, *i.e* que $\zeta \equiv 1 \mod^*(\widetilde{\mathfrak{P}})$. Les racines de l'unité de K étant dans l'anneau des entiers de K, on en déduit que $\zeta \equiv 1 \mod (\widetilde{\mathfrak{P}})$. Puisque l'on a choisi $\mathfrak{P}$ premier avec w_K, $\widetilde{\mathfrak{P}}$ est aussi premier avec w_K et ceci entraîne que ζ est triviale, ce qui prouve que $\alpha_{\mathfrak{P}}$ est fixé par tous les automorphismes ρ de $\mathrm{Gal}(L/K)$ donc appartient bien à K.

Comme on a aussi supposé que α est une anti-unité, γ et par conséquent $\alpha_{\mathfrak{P}}$ sont aussi des anti-unités.

Montrons maintenant que $\alpha_{\mathfrak{P}}$ est en fait congru à $1 \mod^*(\mathfrak{P})$. Pour tout idéal premier $\widetilde{\mathfrak{P}}$ de L au dessus de $\mathfrak{P}$, la valuation $v_{\widetilde{\mathfrak{P}}}(\alpha_{\mathfrak{P}} - 1)$ est supérieure ou égale à $v_{\widetilde{\mathfrak{P}}}\left(\widetilde{\mathfrak{P}}\right)$, d'où

$$v_{\widetilde{\mathfrak{P}}}(\alpha_{\mathfrak{P}} - 1) = v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - 1)\, e\left(\widetilde{\mathfrak{P}}/\mathfrak{P}\right) \geq 1,$$

où $e\left(\widetilde{\mathfrak{P}}/\mathfrak{P}\right)$ désigne l'indice de ramification de $\widetilde{\mathfrak{P}}$ dans L/K. L'idéal $\mathfrak{P}$ ne se ramifiant pas dans L, on obtient ainsi $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - 1) \geq 1 = v_{\mathfrak{P}}(\mathfrak{P})$, *i.e* $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{P})$. Considérons désormais un idéal premier $\mathfrak{Q}$ de K au-dessus de $\mathfrak{p}$ dont le morphisme de Frobenius $\sigma_{\mathfrak{Q}}$ est égal à celui de $\mathfrak{P}$. Il existe alors un élément g de G tel que $\mathfrak{Q} = g(\mathfrak{P})$, l'égalité sur les Frobenius donne $g\sigma_{\mathfrak{P}}g^{-1} = \sigma_{\mathfrak{P}}$, ce qui signifie que g commute avec $\sigma_{\mathfrak{P}}$. Si l'on choisit un idéal premier $\widetilde{\mathfrak{Q}}$ de L au-dessus de $\mathfrak{Q}$, il existe donc un élément de $\mathrm{Gal}(L/k)$, que l'on notera $\widetilde{g}$, tel que $\widetilde{\mathfrak{Q}} = \widetilde{g}(\widetilde{\mathfrak{P}})$. La restriction à K du commutateur de $\sigma_{\widetilde{\mathfrak{P}}}$ avec $\widetilde{g}$, qui est en fait le commutateur de $\sigma_{\mathfrak{P}}$ avec g, est triviale. Ainsi le commutateur $[\sigma_{\widetilde{\mathfrak{P}}}, \widetilde{g}]$ appartient au groupe de Galois $\mathrm{Gal}(L/K)$. Comme l'extension L vérifie la propriété de centralité, ce commutateur est trivial, et $\widetilde{g}$ commute avec $\sigma_{\widetilde{\mathfrak{P}}}$. Finalement les morphismes $\sigma_{\widetilde{\mathfrak{Q}}}$ et $\sigma_{\widetilde{\mathfrak{P}}}$ sont égaux, ce qui entraîne aussi l'égalité entre les éléments $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{Q}}$. Puisque la démonstration précédente donne aussi l'identité $\alpha_{\mathfrak{Q}} \equiv 1 \mod^*(\mathfrak{Q})$, on en déduit que $\alpha_{\mathfrak{P}}$ est lui-aussi congru à 1 modulo$^*(\mathfrak{Q})$, ce qui donne bien la condition de congruence voulue.

Il nous reste enfin à montrer que l'idéal $\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}$ est principal et engendré par $\alpha_{\mathfrak{P}}$. Pour cela, on commence par calculer $\left(\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta}\right)^{w_K}$ qui est égal à

$\left(\mathfrak{a}^{m_G w_K \theta}\right)^{(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))} = (\alpha \mathcal{O}_K)^{(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))}$. On obtient alors

$$\left(\mathfrak{a}^{m_G(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))\theta}\right)^{w_K} = \left(\gamma^{w_K}\mathcal{O}_K\right)^{(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))} = \left(\gamma^{(\sigma_{\tilde{\mathfrak{P}}} - \mathcal{N}(\mathfrak{p}))}\mathcal{O}_K\right)^{w_K} = \left(\alpha_\mathfrak{P}\mathcal{O}_K\right)^{w_K}.$$

On en déduit, puisque $\alpha_\mathfrak{P}$ appartient à K, l'égalité $\mathfrak{a}^{m_G(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))\theta} = \alpha_\mathfrak{P}\mathcal{O}_K$.

$(2 \Rightarrow 3)$: On suppose que la proposition 2 est vraie. Soit H un sous-groupe abélien de G, alors en particulier pour presque tout idéal premier $\mathfrak{P}$ de K tel que $\sigma_\mathfrak{P}$ soit dans H, on sait qu'il existe une anti-unité de K, notée $\alpha_\mathfrak{P}$, vérifiant $\mathfrak{a}^{m_G(\sigma_\mathfrak{P} - \mathcal{N}(\mathfrak{p}))\theta} = \alpha_\mathfrak{P}\mathcal{O}_K$ et $\alpha_\mathfrak{P} \equiv 1 \mod^*(\mathfrak{Q})$ pour tout idéal premier $\mathfrak{Q}$ de K au-dessus de $\mathfrak{p}$ tel que $\sigma_\mathfrak{Q} = \sigma_\mathfrak{P}$. D'autre part, si $\mathfrak{Q}$ est un idéal premier de K au-dessus du même idéal premier de K^H que $\mathfrak{P}$, on peut écrire $\mathfrak{Q}$ sous la forme $h(\mathfrak{P})$ avec h dans H. Le morphisme de Frobenius de $\mathfrak{Q}$ est alors $h\sigma_\mathfrak{P}h^{-1} = \sigma_\mathfrak{P}$ puisque h et $\sigma_\mathfrak{P}$ appartiennent tous deux à H qui est abélien. Ainsi, on trouve que $\alpha_\mathfrak{P} \equiv 1 \mod^*(\mathfrak{Q})$ pour tout idéal premier $\mathfrak{Q}$ de K vérifiant $\mathfrak{Q} \cap \mathcal{O}_{K^H} = \mathfrak{P} \cap \mathcal{O}_{K^H}$. En utilisant l'équivalence donnée par la proposition 3.1, l'idéal $\mathfrak{a}^{m_G w_K \theta}$ est principal et engendré par une anti-unité de K, que l'on notera α_H. De plus, l'extension $K(\gamma_H)$ est abélienne sur K^H pour toute racine w_K-ième γ_H de α_H.

Par ailleurs, la preuve de la proposition 3.1 nous donne aussi l'expression d'un élément α_H convenant en fonction des $\alpha_\mathfrak{P}$. En effet, d'après le lemme 2.16, on sait que $w_K = \underset{\substack{\mathfrak{P}\in\mathcal{T}\\ \sigma_\mathfrak{P}=1}}{\operatorname{pgcd}}(1 - \mathcal{N}(\mathfrak{p}))$ où $\mathcal{T}$ est l'ensemble des idéaux premiers de K vérifiant l'assertion 2 et premiers avec w_K. Ainsi, il existe une suite de $\mathbb{Z}$ à support fini, $(\lambda_\mathfrak{P})_\mathfrak{P}$, vérifiant $w_K = \sum_\mathfrak{P} \lambda_\mathfrak{P}(1 - \mathcal{N}(\mathfrak{p}))$. On peut alors prendre pour α_H le produit $\alpha_H = \prod_\mathfrak{P} {\alpha_\mathfrak{P}}^{\lambda_\mathfrak{P}}$ qui ne dépend pas du sous-groupe abélien H considéré. On obtient de cette manière une anti-unité α de K, qui est telle que $\mathfrak{a}^{m_G w_K \theta} = \alpha\mathcal{O}_K$. En outre, pour toute racine w_K-ième de α, notée γ, l'extension $K(\gamma)$ est abélienne sur K^H, quel que soit le sous-groupe abélien H de G choisi.

$(3 \Rightarrow 1)$: Supposons l'assertion 3 vraie. Notons γ une racine w_K-ième de α et $L = K(\gamma)$ l'extension engendrée par γ sur K. Montrons que L est galoisienne sur k. Soit ρ un k-isomorphisme de L. La restriction de ρ à K est un élément, noté σ, du groupe de Galois G. Puisque par hypothèse l'extension L est abélienne, donc galoisienne sur $K^{\langle\sigma\rangle}$, l'image de L par tout relèvement de σ à L est encore incluse dans L, ce qui implique que ρ est en fait un k-automorphisme de L. Ainsi, l'extension L est galoisienne sur k.

Il reste enfin à montrer que l'extension L vérifie la propriété de centralité. Pour un sous-groupe abélien H de G, on note C le groupe de Galois de L/K, Γ le groupe de Galois de L/k et Γ_H le groupe de Galois de L/K^H. On rappelle que ce groupe est abélien d'après l'assertion 3. Pour visualiser les groupes intervenant, on peut se reporter à la figure 3.2 ci-dessous. Soient ρ_1, ρ_2 deux éléments de Γ. On note $[\rho_1, \rho_2] = \rho_1\rho_2\rho_1^{-1}\rho_2^{-1}$ le commutateur de ρ_1 avec ρ_2. Supposons que $[\rho_1, \rho_2]$ appartienne à C. Alors la restriction de $[\rho_1, \rho_2]$ à K est triviale, donc les restrictions $\rho_{1|_K}$ et $\rho_{2|_K}$ commutent. Ainsi le groupe engendré par $\rho_{1|_K}$ et $\rho_{2|_K}$, que

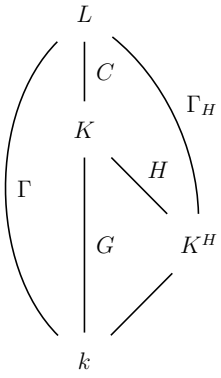


FIGURE 3.2. Groupes de Galois considérés dans l'implication $(3 \Rightarrow 1)$

l'on notera H, est un sous-groupe abélien de G, donc Γ_H est lui-même abélien. Le groupe Γ_H ayant été construit de manière à contenir les morphismes ρ_1 et ρ_2, on trouve que $\rho_1\rho_2 = \rho_2\rho_1$, ce qui prouve que l'intersection entre l'ensemble des commutateurs de Γ, I_L, et $\mathrm{Gal}(L/K)$ est triviale et conclut la preuve.

□

On peut désormais énoncer notre conjecture de Brumer-Stark non abélienne.

Conjecture 3.7 **($\mathbf{BS_{non\ ab}(K/k, S)}$).** — *Pour tout idéal fractionnaire non nul de K, il existe $\alpha \in K^\circ$ tel que $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} = \alpha\mathcal{O}_K$ et si l'on note γ une racine w_K-ième de α, l'extension $K(\gamma)$ est galoisienne sur k et vérifie la propriété de centralité.*

Remarque. — Grâce à l'assertion 3 du théorème 3.6, on voit facilement que lorsque le groupe G est abélien, on retrouve la conjecture de Brumer-Stark abélienne.

Remarque. — Lorsque l'élément de Brumer $\theta_{K/k,S}$ est nul, la conjecture de Brumer-Stark non abélienne est trivialement vérifiée. On a vu que si l'extension K/k ne contient pas de sous-extension CM, alors $\theta_{K/k,S}$ est nul. Si l'on désire obtenir des résultats non triviaux grâce à cette conjecture, il faut donc supposer que K/k contient une extension CM. La partie "intéressante" de l'élément de Brumer provenant des sous-extensions CM, dans toute la suite, on fera l'hypothèse supplémentaire que le corps K est un corps CM.

Cependant, tout comme dans le cas abélien, il ne semble pas y avoir de signe évident que la véracité de la conjecture $BS_{\text{non ab}}$ pour les corps CM implique la validité de la conjecture pour n'importe quelle extension K/k.

On dira qu'un idéal fractionnaire non nul de K vérifie la conjecture $BS_{\text{non ab}}(K/k, S)$ s'il vérifie l'une des conditions équivalentes du théorème 3.6. Les idéaux fractionnaires non nuls de K qui satisfont $BS_{\text{non ab}}(K/k, S)$ forment un groupe, que l'on notera $\mathcal{I}^*_{K/k,S}$. Notre conjecture de Brumer-Stark non abélienne équivaut à l'égalité entre $\mathcal{I}^*_{K/k,S}$ et le groupe des idéaux fractionnaires non nuls de K.

Nous montrons dans la partie suivante que le groupe $\mathcal{I}^*_{K/k,S}$ vérifie des propriétés similaires à celles satisfaites dans le cas abélien.

3.2. Quelques propriétés du groupe des idéaux fractionnaires vérifiant $BS_{\text{non ab}}(K/k, S)$

On suppose désormais que le corps K est un corps CM. On désigne par τ son unique conjugaison complexe.

À l'aide de l'assertion 2 du théorème 3.6 par exemple, il est aisé de démontrer que $\mathcal{I}^*_{K/k,S}$ est stable par le centre de G. On a en fait un résultat un peu plus fort.

Proposition 3.8. — *Le groupe $\mathcal{I}^*_{K/k,S}$ est stable par G.*

Démonstration. — Soit $\mathfrak{a}$ un idéal de $\mathcal{I}^*_{K/k,S}$ et g un élément de G. On cherche à savoir si l'idéal fractionnaire $g(\mathfrak{a})$ vérifie aussi $BS_{\text{non ab}}(K/k, S)$. Pour cela, on va se servir de la caractérisation 1 du théorème 3.6. Notons α un générateur de l'idéal principal $\mathfrak{a}^{m_G w_K \theta_{K/k,S}}$ vérifiant la propriété 1. On a alors

$$g(\mathfrak{a})^{m_G w_K \theta_{K/k,S}} = \mathfrak{a}^{m_G w_K \theta_{K/k,S} g}$$

Puisque $\theta_{K/k,S}$ est dans le centre de $\mathbb{Q}[G]$, on peut intervertir $\theta_{K/k,S}$ et g, ce qui donne

$$\begin{aligned} g(\mathfrak{a})^{m_G w_K \theta_{K/k,S}} &= \mathfrak{a}^{m_G w_K g \theta_{K/k,S}} \\ &= \left(\mathfrak{a}^{m_G w_K \theta_{K/k,S}}\right)^g \\ &= (\alpha \mathcal{O}_K)^g \\ &= g(\alpha)\mathcal{O}_K. \end{aligned}$$

L'élément α étant une anti-unité de K, il en est de même de $g(\alpha)$. Notons γ une racine w_K-ième de α et δ une racine w_K-ième de $g(\alpha)$. On considère un relèvement ρ de g à $K(\gamma)$. Alors on a l'égalité

$$\delta^{w_K} = g(\alpha) = g(\gamma^{w_K}) = \rho(\gamma)^{w_K}.$$

Il existe donc $\zeta \in \mu(K)$ vérifiant $\delta = \zeta\rho(\gamma)$. Puisque $K(\gamma)$ est galoisienne sur k, on remarque que δ appartient à $K(\gamma)$ donc on a l'inclusion $K(\delta) \subset K(\gamma)$. Or l'extension $K(\delta)$ contient K, le groupe de Galois $\mathrm{Gal}(K(\gamma)/K(\delta))$ est donc inclus dans $\mathrm{Gal}(K(\gamma)/K)$. Comme $K(\gamma)$ vérifie la propriété de centralité, c'est une extension centrale de K/k, donc $\mathrm{Gal}(K(\gamma)/K)$ est un sous-groupe du centre de $\mathrm{Gal}(K(\gamma)/k)$. Par conséquent, le groupe $\mathrm{Gal}(K(\gamma)/K(\delta))$ est distingué dans $\mathrm{Gal}(K(\gamma)/k)$, et ainsi l'extension $K(\delta)$ est galoisienne sur K. Mais alors de l'égalité $\delta = \zeta\rho(\gamma)$, on tire $\gamma = \rho^{-1}(\zeta^{-1})\rho^{-1}(\delta) = \rho^{-1}_{|K}(\zeta^{-1})\rho^{-1}_{|K(\delta)}(\delta)$. L'élément $\rho^{-1}_{|K(\delta)}(\delta)$ appartenant à $K(\delta)$, on en déduit que γ appartient aussi à $K(\delta)$, ce qui donne l'égalité entre les extensions $K(\gamma)$ et $K(\delta)$. Ainsi $K(\delta)$ vérifie bien la propriété de centralité, donc $g(\mathfrak{a})$ est bien un idéal de $\mathcal{I}^*_{K/k,S}$. □

Le lemme suivant permet de caractériser les anti-unités de K et nous est utile dans la suite pour étudier une autre propriété de $\mathcal{I}^*_{K/k,S}$.

Lemme 3.9. — *Soit α appartenant à $K^\times$. L'élément α est une anti-unité si et seulement si $\alpha^{1+\tau} = 1$.*

Démonstration. — Soit w une place infinie de K, alors $|x|_w = |x|_{\tau\cdot w} = |\tau^{-1}(x)|_w = |\tau(x)|_w$, donc $|x^{1+\tau}|_w = |x|_w{}^2$. De plus puisque τ est l'unique conjugaison complexe de K, l'élément $x^{1+\tau}$ est un nombre réel positif. Supposons que x soit une anti-unité, alors pour toute place infinie w de K, on a $|x|_w = 1$. Ainsi $|x^{1+\tau}| = 1$ et donc $x^{1+\tau} = 1$. Réciproquement, si $x^{1+\tau} = 1$, alors pour toute place infinie w de K, $|x|_w{}^2 = |x^{1+\tau}|_w = 1$, ce qui entraîne $|x|_w = 1$. □

Proposition 3.10. — *Le groupe $\mathcal{I}^*_{K/k,S}$ contient le groupe des idéaux principaux de K.*

Démonstration. — Soit β un élément non nul de K. On cherche à démontrer que l'idéal principal $\beta\mathcal{O}_K$ vérifie l'assertion 3 du théorème 3.6. On a l'égalité

$$(\beta\mathcal{O}_K)^{m_G w_K \theta_{K/k,S}} = \beta^{m_G w_K \theta_{K/k,S}}\mathcal{O}_K.$$

Posons alors $\alpha = \beta^{m_G w_K \theta_{K/k,S}}$. Puisque l'on a supposé que le postulat concernant l'élément de Brumer est vérifié, $m_G w_K \theta_{K/k,S}$ est dans $\mathbb{Z}[G]$ et l'élément α appartient bien à K. Démontrons à l'aide du lemme 3.9 que α est une anti-unité de K. On écrit

$$\begin{aligned} \alpha^{1+\tau} &= \left(\beta^{m_G w_K \theta_{K/k,S}}\right)^{(1+\tau)} \\ &= \beta^{m_G w_K (1+\tau)\theta_{K/k,S}}. \end{aligned}$$

Prenons alors v une place infinie de S et w une place arbitraire de K au-dessus de v. Puisque K est un corps CM, le groupe de décomposition de w, D_w, est le groupe engendré par la conjugaison complexe. De plus, l'unique conjugaison complexe appartient au centre de G, donc on obtient finalement

$$N_v = \sum_{g\in D_w} \frac{1}{|C_g|} C_g = \sum_{g\in\langle\tau\rangle} \frac{1}{|C_g|} C_g = 1 + \tau.$$

La proposition 2.11 stipulant l'annulation de $\theta_{K/k,S}$ par N_v implique donc que $(1+\tau)\theta_{K/k,S} = 0$. Ainsi, on a $\alpha^{1+\tau} = \beta^0 = 1$, donc α est bien une anti-unité de K.

Notons à présent γ une racine w_K-ième de α. Soit H un sous-groupe abélien de G. Afin de prouver que l'extension $K(\gamma)$ est abélienne sur K^H, on utilise une reformulation de la proposition 1.2 de [**Tat84**, p. 83] :

Proposition 3.11 **(Tate)**. — *Soit $\{h_i\}_{i\in I}$ un système de générateurs de H. Soit $\{n_i\}_{i\in I}$ un système d'entiers vérifiant pour tout $\zeta \in \mu(K)$, $\zeta^{h_i - n_i} = 1$ pour tout $i \in I$. Alors l'extension $K(\gamma)/K^H$ est abélienne si et seulement s'il existe un système d'éléments $\{\alpha_i\}_{i\in I}$ de $K^\times$ tel que pour tous $i, j \in I$, $\alpha^{h_i - n_i} = \alpha_i^{w_K}$ et $\alpha_i^{h_j - n_j} = \alpha_j^{h_i - n_i}$.*

On considère un système $\{h_i\}_{i\in I}$ de générateurs de H. Soit i appartenant à I. Puisque H est un sous-groupe de G, d'après le théorème de densité de Čebotarev, on peut écrire h_i comme le Frobenius associé à l'extension K/k d'un idéal premier

$\mathfrak{P}$ de K. On peut alors prendre pour l'entier n_i la norme absolue $\mathcal{N}(\mathfrak{p})$ de $\mathfrak{p}$. Ainsi l'élément $m_G(h_i - n_i)\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$ puisque l'on a supposé le postulat sur le dénominateur de $\theta_{K/k,S}$ vérifié. On a alors

$$\begin{aligned} \alpha^{h_i-n_i} &= \left(\beta^{m_G w_K \theta_{K/k,S}}\right)^{h_i-n_i} \\ &= \beta^{m_G w_K (h_i-n_i)\theta_{K/k,S}} \\ &= \left(\beta^{m_G (h_i-n_i)\theta_{K/k,S}}\right)^{w_K}. \end{aligned}$$

En outre $\beta^{m_G(h_i-n_i)\theta_{K/k,S}}$ appartient à K puisque $m_G(h_i - n_i)\theta_{K/k,S}$ est à coefficients entiers. On pose alors $\alpha_i = \beta^{m_G(h_i-n_i)\theta_{K/k,S}}$. Soient i, j dans I. On a

$$\begin{aligned} {\alpha_i}^{h_j-n_j} &= \left(\beta^{m_G(h_i-n_i)\theta_{K/k,S}}\right)^{(h_j-n_j)} \\ &= \beta^{m_G(h_j-n_j)(h_i-n_i)\theta_{K/k,S}}. \end{aligned}$$

Puisque H est abélien, on peut intervertir h_i et h_j, d'où l'identité

$$\begin{aligned} {\alpha_i}^{h_j-n_j} &= \left(\beta^{m_G(h_j-n_j)\theta_{K/k,S}}\right)^{(h_i-n_i)} \\ &= {\alpha_j}^{h_i-n_i}. \end{aligned}$$

Ainsi l'extension $K(\gamma)/K^H$ est abélienne. La condition 3 du théorème 3.6 est vérifiée et $BS_{\text{non ab}}(K/k, S)$ est vraie pour l'idéal principal $\beta\mathcal{O}_K$. □

Remarque. — Ceci nous permet comme dans le cas abélien de considérer la conjecture de Brumer-Stark comme une question de classes d'idéaux. Pour la vérifier il suffit donc de montrer que les idéaux engendrant le groupe des classes vérifient $BS_{\text{non ab}}(K/k, S)$.

3.3. Dépendance de la conjecture par rapport au corps K

À ce stade, on se demande si la conjecture de Brumer-Stark non abélienne vérifie des propriétés de changement d'extension similaires à celles de la conjecture abélienne. Soit K' une sous-extension de K/k galoisienne sur le corps de base k. On note dans cette section B le groupe de Galois de l'extension K/K' et G' celui de K'/k. La question est de savoir si la véracité de $BS_{\text{non ab}}(K/k, S)$ implique la validité de $BS_{\text{non ab}}(K'/k, S)$.

3.3.1. Cas où B est abélien. — Si l'intersection entre le sous-groupe $B = \text{Gal}(K/K')$ et l'ensemble des commutateurs de G est réduite à l'identité, *i.e* si K vérifie la propriété de centralité par rapport à l'extension K'/k, la proposition 3.5 appliquée à l'extension K de K'/k implique l'égalité entre m_G et $m_{G'}$.

De plus, dans ce cas, pour tout sous-groupe abélien H' de G', l'image réciproque de H' par la restriction à K', notée $s' : G \longrightarrow G'$, est un sous-groupe abélien de G. En effet, prenons g_1 et g_2 deux éléments de ${s'}^{-1}(H')$. On a $s'([g_1, g_2]) = [s'(g_1), s'(g_2)] = \text{Id}$ puisque $s'(g_1)$ et $s'(g_2)$ appartiennent tous deux à H' qui est abélien. Ainsi le commutateur $[g_1, g_2]$ est trivial sur K' donc appartient à $\text{Gal}(K/K')$. L'intersection entre les commutateurs de G et ce groupe de Galois

étant supposée triviale, on obtient que g_1 et g_2 commutent entre eux, ce qui prouve que $s'^{-1}(H')$ est un sous-groupe abélien de G. Autrement dit, lorsque H' est un sous-groupe abélien de G', le groupe de Galois $\mathrm{Gal}(K/K'^{H'})$ est un sous-groupe abélien de G.

On peut alors démontrer le résultat suivant :

Théorème 3.12. — *Si l'intersection entre le sous-groupe $B = \mathrm{Gal}(K/K')$ et l'ensemble des commutateurs de G est réduite à l'identité, alors $BS_{non\ ab}(K/k, S)$ implique $BS_{non\ ab}(K'/k, S)$.*

Démonstration. — Supposons la véracité de la conjecture $BS_{\text{non ab}}(K/k, S)$. Pour simplifier les notations, on notera θ l'élément de Brumer associé à l'extension K/k et l'ensemble S, ainsi que θ' celui associé à l'extension K'/k et à S. Soit $\mathfrak{a}'$ un idéal fractionnaire non nul de K'. On va chercher à démontrer que l'idéal $\mathfrak{a}'$ vérifie l'assertion 2 du théorème 3.6. La conjecture $BS_{\text{non ab}}(K/k, S)$ étant vérifiée par l'idéal fractionnaire $\mathfrak{a}'\mathcal{O}_K$ de K, la formulation 2 du théorème 3.6 implique, pour presque tout idéal premier $\mathfrak{P}$ de K, l'existence d'une anti-unité $\alpha_{\mathfrak{P}} \in K^\circ$ telle que $(\mathfrak{a}'\mathcal{O}_K)^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta} = \alpha_{\mathfrak{P}}\mathcal{O}_K$ et $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{Q})$ pour tout idéal premier $\mathfrak{Q}$ de K au-dessus de $\mathfrak{p}$ tel que $\sigma_{\mathfrak{Q}} = \sigma_{\mathfrak{P}}$. Appelons $\mathcal{P}'$ l'idéal premier de K' en-dessous de $\mathfrak{P}$. On a

$$\begin{aligned}(\mathfrak{a}'\mathcal{O}_K)^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta} &= \mathfrak{a}'^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta}\mathcal{O}_K \\ &= \mathfrak{a}'^{m_G(\sigma_{\mathfrak{P}|_{K'}} - \mathcal{N}(\mathfrak{p}))\theta|_{K'}}\mathcal{O}_K.\end{aligned}$$

La restriction à K' du morphisme de Frobenius associé à $\mathfrak{P}$ et à l'extension K/k n'est rien d'autre que le morphisme de Frobenius de l'idéal $\mathcal{P}'$ associé à l'extension K'/k, que l'on désignera par $\sigma_{\mathcal{P}'}$. On utilise ensuite les propriétés de changement d'extension de l'élément de Brumer, à savoir que la restriction de θ à K' est justement θ', afin de faire apparaître le terme recherché pour l'extension K'/k. De plus, la condition sur l'intersection entre l'ensemble des commutateurs de G et le groupe B implique l'égalité entre m_G et m'_G. On obtient donc

$$(\mathfrak{a}'\mathcal{O}_K)^{m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta} = \mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K.$$

En conséquence, pour presque tout idéal premier $\mathcal{P}'$ de K', on a

$$\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K = \alpha_{\mathfrak{P}}\mathcal{O}_K,$$

ceci pour tout premier $\mathfrak{P}$ de K divisant $\mathcal{P}'$. Notre but est de montrer que cet élément $\alpha_{\mathfrak{P}}$ appartient en réalité à K'. Soit b appartenant à $\mathrm{Gal}(K/K')$. Puisque les éléments de K' sont fixés par b, on a d'une part

$$\begin{aligned}\left(\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K\right)^b &= \left(\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\right)^b\mathcal{O}_K \\ &= \mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K \\ &= \alpha_{\mathfrak{P}}\mathcal{O}_K\end{aligned}$$

et d'autre part

$$\begin{aligned}\left(\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'}-\mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K\right)^b &= (\alpha_{\mathfrak{P}}\mathcal{O}_K)^b \\ &= b(\alpha_{\mathfrak{P}})\mathcal{O}_K.\end{aligned}$$

Ainsi l'idéal engendré par $b(\alpha_{\mathfrak{P}})$ est le même que celui engendré par $\alpha_{\mathfrak{P}}$, donc ils diffèrent d'une unité de K, mais puisque ce sont tous les deux des anti-unités de K, il existe une racine de l'unité $\zeta \in \mu(K)$ telle que $b(\alpha_{\mathfrak{P}}) = \zeta\alpha_{\mathfrak{P}}$. Puisque b fixe K', il appartient en particulier au groupe de Galois de $K/K'^{\langle\sigma_{\mathcal{P}'}\rangle}$, où $K'^{\langle\sigma_{\mathcal{P}'}\rangle}$ désigne le sous-corps de K' fixé par le sous-groupe engendré par $\sigma_{\mathcal{P}'}$, et il en est de même de b^{-1}. Or $\langle\sigma_{\mathcal{P}'}\rangle$ est un sous-groupe abélien de G', donc $\mathrm{Gal}(K/K'^{\langle\sigma_{\mathcal{P}'}\rangle})$ est un sous-groupe abélien de G. Puisque $\sigma_{\mathfrak{P}|_{K'}}$ est égale à $\sigma_{\mathcal{P}'}$, $\sigma_{\mathfrak{P}}$ est dans $\mathrm{Gal}(K/K'^{\langle\sigma_{\mathcal{P}'}\rangle})$ et ainsi commute avec b^{-1}. Les idéaux premiers $\mathfrak{P}$ et $b^{-1}(\mathfrak{P})$ de K tous deux au-dessus de $\mathfrak{p}$ ont alors le même morphisme de Frobenius. Par hypothèse on a $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(b^{-1}(\mathfrak{P}))$, ce qui donne $b(\alpha_{\mathfrak{P}}) \equiv 1 \mod^*(\mathfrak{P})$. Ainsi $\zeta\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{P})$, mais puisque $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{P})$, on obtient finalement $\zeta \equiv 1 \mod^*(\mathfrak{P})$. Comme on désire avoir un résultat pour presque tout idéal premier de K', on peut considérer $\mathcal{P}'$ premier avec w_K, ce qui donne en particulier $\mathfrak{P}$ premier avec w_K et la condition de congruence sur ζ implique alors que ζ est égale à 1. Ainsi on a montré que $b(\alpha_{\mathfrak{P}}) = \alpha_{\mathfrak{P}}$ pour tout b dans $\mathrm{Gal}(K/K')$, l'élément $\alpha_{\mathfrak{P}}$ appartient donc à K'.

Pour presque tout idéal premier $\mathcal{P}'$ de K', il existe $\alpha_{\mathfrak{P}} \in K'^{\circ}$ tel que $\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'}-\mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K = \alpha_{\mathfrak{P}}\mathcal{O}_K$ et par conséquent $\mathfrak{a}'^{m_{G'}(\sigma_{\mathcal{P}'}-\mathcal{N}(\mathfrak{p}))\theta'} = \alpha_{\mathfrak{P}}\mathcal{O}_{K'}$. En outre, comme $\alpha_{\mathfrak{P}}$ est congru à $1 \mod^*(\mathfrak{P})$ et appartient à K', on a aussi $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathfrak{P} \cap \mathcal{O}_{K'})$, *i.e* $\alpha_{\mathfrak{P}} \equiv 1 \mod^*(\mathcal{P}')$.

Le choix de l'idéal premier $\mathfrak{P}$ de K au-dessus de $\mathcal{P}'$ n'a pas d'importance. Soient $\mathfrak{P}$ et $\mathfrak{P}'$ deux idéaux premiers de K au-dessus de $\mathcal{P}'$. Le raisonnement précédent nous donne l'égalité entre les idéaux $\alpha_{\mathfrak{P}}\mathcal{O}_{K'}$ et $\alpha_{\mathfrak{P}'}\mathcal{O}_{K'}$. Les éléments $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{P}'}$ diffèrent alors d'une racine de l'unité de K' et les deux relations de congruences modulo $\mathfrak{P}'$ dont on dispose permettent de conclure que cette racine de l'unité est triviale. De cette manière, $\alpha_{\mathfrak{P}}$ et $\alpha_{\mathfrak{P}'}$ sont égaux, ce qui permet de définir l'élément $\alpha_{\mathcal{P}'}$ comme $\alpha_{\mathfrak{P}}$ pour n'importe quel idéal premier $\mathfrak{P}$ de K au-dessus de $\mathcal{P}'$.

Pour obtenir la validité de la conjecture $BS_{\text{non ab}}(K'/k, S)$, il nous reste seulement à établir la condition de congruence sur $\alpha_{\mathcal{P}'}$. Soit $\mathcal{Q}'$ un idéal premier de K' au-dessus de $\mathfrak{p}$ vérifiant $\sigma_{\mathcal{Q}'} = \sigma_{\mathcal{P}'}$. Il existe $g' \in G'$ tel que $\mathcal{Q}' = g'(\mathcal{P}')$ et g' commute avec $\sigma_{\mathcal{P}'}$. La condition sur le groupe B implique que tous relèvements de $\sigma_{\mathcal{P}'}$ et de g' à K commutent entre eux. Ainsi, si l'on note g un relèvement de g' à K, on a $\sigma_{\mathfrak{P}}g = g\sigma_{\mathfrak{P}}$ et puisque l'on a supposé $BS_{\text{non ab}}(K/k, S)$ vraie, on obtient donc $\alpha_{\mathcal{P}'} \equiv 1 \mod^*(g(\mathfrak{P}))$, d'où $\alpha_{\mathcal{P}'} \equiv 1 \mod^*(g'(\mathcal{P}'))$, et $\alpha_{\mathcal{P}'} \equiv 1 \mod^*(\mathcal{Q}')$ ce qui termine la preuve. □

Corollaire 3.13. — *En particulier, lorsque le groupe G est lui-même abélien, la condition du théorème précédent est trivialement vérifiée pour tout sous-groupe B de G, et on obtient la propriété de changement d'extension dans le cas abélien.*

Ce résultat de changement d'extension impose entre autre que le corps intermédiaire K' doit être un sous-corps de K fixé par un sous-groupe du centre de G et limite ainsi les choix de K' possibles.

3.3.2. Cas où B est non abélien. — On peut obtenir un résultat de changement d'extension sous certaines conditions supplémentaires lorsque le groupe $B = \mathrm{Gal}(K/K')$ est non abélien, cependant ce résultat ne sera que partiel, à savoir qu'il ne sera vrai qu'au facteur $\frac{m_G}{m_{G'}}$ près. Avant de préciser ce que l'on entend par là, on commence par remarquer que le quotient $\frac{m_G}{m_{G'}}$ en question est entier.

Lemme 3.14. — *Le nombre $m_{G'}$ divise m_G.*

Démonstration. — On peut écrire tout élément g' de G' comme la restriction $\overline{g}$ d'un élément de G. Notons $C_{\overline{g}}$ la classe de conjugaison de $\overline{g}$ dans G' et C_g la classe de conjugaison de g dans G. D'après la formule des classes, on a l'égalité

$$|C_{\overline{g}}| = \frac{|G'|}{\mathrm{Stab}_{G'}(\overline{g})}.$$

où $\mathrm{Stab}_{G'}(\overline{g}) = \{\overline{\sigma} \in G' \mid \overline{\sigma} \cdot \overline{g} \cdot \overline{\sigma}^{-1} = \overline{g}\}$. Soit σ un élément de G tel que $\overline{\sigma}$ appartient au stabilisateur $\mathrm{Stab}_{G'}(\overline{g})$. Tout élément ν de G vérifiant $\overline{\nu} = \overline{\sigma}$ appartient aussi à $\mathrm{Stab}_{G'}(\overline{g})$, et il y a exactement $|B|$ éléments satisfaisant cette propriété. Si l'on note $A(g)$ l'ensemble $\{\sigma \in G \mid \overline{\sigma}\cdot\overline{g}\cdot\overline{\sigma}^{-1} = \overline{g}\}$, on peut alors écrire $|\mathrm{Stab}_{G'}(\overline{g})| = \dfrac{|A(g)|}{|B|}$. On remarque que le stabilisateur dans G de g, $\mathrm{Stab}_G(g)$ est un sous-groupe de $A(g)$, il existe donc un certain entier m vérifiant $|A(g)| = |\mathrm{Stab}_G(g)|m$. Le cardinal de $C_{\overline{g}}$ est alors égal à

$$|C_{\overline{g}}| = \frac{|G|/|B|}{|A(g)|/|B|} = \frac{|G|}{|\mathrm{Stab}_G(g)|m} = \frac{|C_g|}{m}.$$

Ainsi pour tout élément $\overline{g}$ de G', le cardinal de $C_{\overline{g}}$ divise celui de C_g, ce qui donne bien le résultat voulu. □

On observe alors pour un idéal fractionnaire $\mathfrak{a}'$ de K'

$$\mathfrak{a}^{m_G w_{K'} \theta_{K'/k,S}} = \left(\mathfrak{a}^{m_{G'} w_{K'} \theta_{K'/k,S}}\right)^{\frac{m_G}{m_{G'}}}$$

où $\frac{m_G}{m_{G'}}$ est un entier non nul. C'est pourquoi on dit que la conjecture $BS_{\text{non ab}}(K'/k, S)$ est vraie au facteur $\frac{m_G}{m_{G'}}$ près pour signifier que dans les assertions 1 à 3 du théorème 3.6, ce ne sera pas la puissance $m_{G'}$ qui interviendra mais m_G.

Théorème 3.15. — *Si le nombre de racines de l'unité de K est le même que celui de K' et si $|B|$ et w_K sont premiers entre eux, alors $BS_{non\ ab}(K/k, S)$ implique $BS_{non\ ab}(K'/k, S)$ au facteur $\frac{m_G}{m_{G'}}$ près.*

Démonstration. — Soit $\mathfrak{a}'$ un idéal fractionnaire non nul de K'. On montre comme dans la preuve du théorème 3.12 que pour presque tout idéal premier $\mathfrak{P}$ de K, il existe $\alpha_{\mathfrak{P}} \in K^\circ$ tel que $\mathfrak{a}'^{m_G(\sigma_{\mathcal{P}'} - \mathcal{N}(\mathfrak{p}))\theta'}\mathcal{O}_K = \alpha_{\mathfrak{P}}\mathcal{O}_K$ et $\alpha_{\mathfrak{P}}$ vérifie la propriété de congruence. De même, si l'on considère un élément b de $\mathrm{Gal}(K/K')$, il existe

$\zeta \in \mu(K)$ vérifiant $b(\alpha_{\mathfrak{P}}) = \zeta\alpha_{\mathfrak{P}}$. La preuve diffère à partir du moment où l'on veut démontrer que cette racine de l'unité est triviale. Si on calcule la norme relative de $b(\alpha_{\mathfrak{P}})$ associée à l'extension K/K', on trouve en utilisant la multiplicativité de la norme que $\mathcal{N}_{K/K'}(b(\alpha_{\mathfrak{P}})) = \mathcal{N}_{K/K'}(\zeta)\mathcal{N}_{K/K'}(\alpha_{\mathfrak{P}})$. Or on sait aussi que

$$\begin{aligned}\mathcal{N}_{K/K'}(b(\alpha_{\mathfrak{P}})) &= \prod_{\sigma\in\mathrm{Gal}(K/K')} \sigma(b(\alpha_{\mathfrak{P}})) \\ &= \prod_{\nu\in\mathrm{Gal}(K/K')} \nu(\alpha_{\mathfrak{P}}) \\ &= \mathcal{N}_{K/K'}(\alpha_{\mathfrak{P}}).\end{aligned}$$

Ainsi, $\mathcal{N}_{K/K'}(\alpha_{\mathfrak{P}}) = \mathcal{N}_{K/K'}(\zeta)\mathcal{N}_{K/K'}(\alpha_{\mathfrak{P}})$, et en simplifiant dans K' par $\mathcal{N}_{K/K'}(\alpha_{\mathfrak{P}})$, on obtient $\mathcal{N}_{K/K'}(\zeta) = 1$. Puisque l'on a supposé que les racines de K et celles de K' sont les mêmes, ζ appartient en réalité à K', c'est pourquoi sa norme relative est égale à $\zeta^{[K:K']} = \zeta^{|B|} = 1$, et l'ordre de ζ, qui est un diviseur de w_K, divise $|B|$. Les entiers $|B|$ et w_K étant premiers entre eux, ceci n'est possible que si ζ est égale à 1, ce qui prouve que l'élément $\alpha_{\mathfrak{P}}$ est dans K', et en particulier dans K'°.

Démontrer la condition de congruence sur $\alpha_{\mathfrak{P}}$ s'avère plus délicat. C'est pourquoi nous ne cherchons pas à démontrer la véracité de l'assertion 2 du théorème 3.6, mais utilisons les informations obtenues sur les éléments $\alpha_{\mathfrak{P}}$ afin de démontrer la validité de la condition 1 où intervient la puissance m_G à la place de m'_G pour l'extension K'/k. On sait que si l'on écrit w_K sous la forme

$$w_K = \sum_{\substack{\mathfrak{P}\\ \sigma_{\mathfrak{P}}=1}} \lambda_{\mathfrak{P}}(1 - \mathcal{N}(\mathfrak{p}))$$

où $(\lambda_{\mathfrak{P}})_{\mathfrak{P}}$ est une suite à support fini de $\mathbb{Z}$, l'élément $\alpha = \prod \alpha_{\mathfrak{P}}^{\lambda_{\mathfrak{P}}}$ est un élément qui convient pour la condition 3 de $BS_{\text{non ab}}(K/k, S)$, et ainsi pour la condition 1. Puisque chacun des $\alpha_{\mathfrak{P}}$ appartient à K'°, l'élément α est aussi dans K'°. De l'égalité $\mathfrak{a}'^{m_G w_{K'}\theta'}\mathcal{O}_K = \alpha\mathcal{O}_K$, on déduit en outre l'égalité $\mathfrak{a}'^{m_G w_{K'}\theta'} = \alpha\mathcal{O}_{K'}$. De plus si l'on note γ une racine w_K-ième de α, l'extension $L = K(\gamma)$ est galoisienne sur k et vérifie la propriété de centralité. Afin de prouver que l'extension $L' = K'(\gamma)$ est galoisienne sur k, on a besoin de propriétés supplémentaires sur γ.

Soit g un élément de G. Il existe un idéal premier $\mathfrak{P}_g$ de K dont g est le morphisme de Frobenius associé à l'extension K/k. Puisque $\langle g\rangle$ est un sous-groupe abélien de G, on peut alors démontrer comme dans la preuve de $(iii) \Rightarrow (iv)$ de la proposition 3.1 que l'on a l'égalité

$$\alpha_{\mathfrak{P}_g}^{\sigma_{\mathfrak{Q}} - \mathcal{N}(\mathfrak{q})} = \alpha_{\mathfrak{Q}}^{g - \mathcal{N}(\mathfrak{p}_g)}, \tag{3.3.1}$$

pour tout idéal premier $\mathfrak{Q}$ de K dont le Frobenius $\sigma_{\mathfrak{Q}}$ appartient au sous-groupe engendré par g. Notons pour simplifier $\alpha_g = \alpha_{\mathfrak{P}_g}$ et $n_g = \mathcal{N}(\mathfrak{p}_g)$.

On a alors

$$\alpha^{g-n_g} = \left(\prod_{\substack{\mathfrak{P} \\ \sigma_{\mathfrak{P}}=1}} \alpha_{\mathfrak{P}}^{\lambda_{\mathfrak{P}}} \right)^{g-n_g} = \prod_{\substack{\mathfrak{P} \\ \sigma_{\mathfrak{P}}=1}} \left(\alpha_{\mathfrak{P}}^{g-n_g} \right)^{\lambda_{\mathfrak{P}}}.$$

Puisque 1 appartient toujours au sous-groupe $\langle g \rangle$, les idéaux premiers $\mathfrak{P}$ intervenant dans l'expression précédente satisfont l'égalité (3.3.1), et on a de cette manière $\alpha_{\mathfrak{P}}^{g-n_g} = \alpha_g^{\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})} = \alpha_g^{1-\mathcal{N}(\mathfrak{p})}$. Ceci donne

$$\alpha^{g-n_g} = \prod_{\substack{\mathfrak{P} \\ \sigma_{\mathfrak{P}}=1}} \left(\alpha_g^{1-\mathcal{N}(\mathfrak{p})} \right)^{\lambda_{\mathfrak{P}}} = \alpha_g^{\sum_{\mathfrak{P}, \sigma_{\mathfrak{P}}=1} \lambda_{\mathfrak{P}} (1-\mathcal{N}(\mathfrak{p}))} = \alpha_g^{w_K}$$

avec $\alpha_g \in K'$. On peut désormais démontrer que $L' = K'(\gamma)$ est galoisienne sur k. Soit g' appartenant à G'. Notons ρ' un prolongement quelconque de g' à L', et ρ un prolongement de ρ' à $L = K(\gamma)$. La restriction de ρ à K est un élément de G que l'on appellera g. Alors

$$(\gamma^{\rho'})^{w_K} = (\gamma^{\rho})^{w_K} = \alpha^{\rho} = \alpha^{g} = \alpha^{g-n_g} \alpha^{n_g} = \alpha_g^{w_K} \alpha^{n_g} = (\alpha_g \gamma^{n_g})^{w_K}.$$

Ainsi, il existe ζ une racine w_K-ième de l'unité vérifiant $\rho'(\gamma) = \zeta \alpha_g \gamma^{n_g}$. Puisque ζ et α_g sont dans K', $\rho'(\gamma)$ appartient à $L' = K'(\gamma)$. L'image de L' par ρ' reste bien dans L', ce qui implique que L' est galoisienne sur k.

Notons alors Γ' le groupe de Galois de L'/k et C' celui de L'/K'. On désignera par B' le groupe de Galois de L/L'. On a le diagramme :

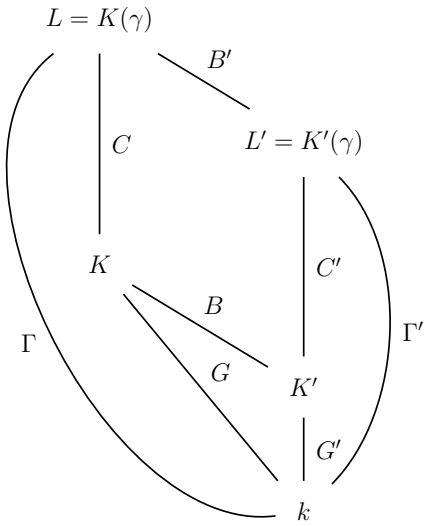


FIGURE 3.3. Diagramme des corps intervenant dans le changement d'extension, dans le cas où B est non abélien

L'élément γ est une racine w_K-ième de α et α appartient à K', donc l'ordre de $C' = \mathrm{Gal}(K'(\gamma)/K')$ est un diviseur de w_K. On en déduit que $|B|$ est premier avec $|C'|$. De plus, l'extension L est aussi le compositum de K et L'. L'intersection de K et L', $K \cap L'$, est un sous-corps de K et de L' qui contient K'. De plus le degré $[K \cap L' : K']$ divise $|B|$ ainsi que $|C'|$. Puisque $|B|$ et $|C'|$ sont premiers entre eux,

le degré de $K \cap L'$ sur K' est égal à 1, et l'intersection en question est donc K'. Par conséquent le groupe de Galois $\mathrm{Gal}(L/K')$ est isomorphe au produit direct de B par C' et on dispose aussi d'un isomorphisme entre C et C', donné par la restriction s' de L à L'. Soit alors $[\rho'_1, \rho'_2]$ un commutateur de Γ' qui appartient aussi à C'. L'image réciproque par s' de ce commutateur, $s'^{-1}([\rho'_1, \rho'_2])$, est donc dans C. Or $s'^{-1}([\rho'_1, \rho'_2]) = [s'^{-1}(\rho'_1), s'^{-1}(\rho'_2)]$ est un commutateur de Γ. D'après les propriétés de L, on en déduit que cet élément est trivial. En appliquant encore une fois s' à notre commutateur, on obtient finalement $[\rho'_1, \rho'_2] = \mathrm{Id}$, ainsi L' vérifie bien la propriété de centralité associée à l'extension K'/k. La conjecture $BS_{\text{non ab}}(K'/k, S)$ est donc vérifiée au facteur $\frac{m_G}{m_{G'}}$ près. □

3.4. Dépendance de la conjecture par rapport à l'ensemble S

Après avoir étudié le comportement de la conjecture de Brumer-Stark non abélienne suivant l'extension K que l'on considère, on s'interroge sur la dépendance de la conjecture relativement à l'ensemble de places S choisi. Dans le cas où le groupe G est abélien, la validité de la conjecture de Brumer-Stark pour un ensemble S donné implique la validité de la conjecture pour tout ensemble S' contenant S. Ce résultat repose sur l'expression de l'élément de Brumer-Stickelberger associé à S' en fonction de celui associé à S.

En ce qui concerne le cas général, la proposition 2.9 nous donne l'expression de $\theta_{K/k,S'}$ en fonction de $\theta_{K/k,S}$. Supposons que S' soit constitué de l'ensemble S auquel on a rajouté les premiers $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ de k. En appliquant plusieurs fois le résultat de la proposition 2.9, on obtient

$$\theta_{K/k,S'} = \prod_{i=1}^{n} \sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_i}))e_{\overline{\chi}} \cdot \theta_{K/k,S} \tag{3.4.1}$$

où pour tout $i \in \{1, \ldots, n\}$, $\mathfrak{P}_i$ est un idéal premier de K choisi arbitrairement au-dessus de $\mathfrak{p}_i$. Si $\theta_{K/k,S}$ est nul, alors pour tout ensemble S' contenant S, $\theta_{K/k,S'}$ est aussi nul et la conjecture de Brumer-Stark non abélienne est trivialement vérifiée. Si l'élément de Brumer associé à l'ensemble S n'est pas nul, le problème se pose alors de savoir si le produit précédent est ou non dans l'anneau de groupe $\mathbb{Z}[G]$. A priori, on ne sait même pas s'il est à coefficients rationnels.

Proposition 3.16. — *Soit S' l'ensemble $S \cup \{\mathfrak{p}_0, \ldots, \mathfrak{p}_n\}$ où les $\mathfrak{p}_i$ sont des idéaux premiers de k distincts deux à deux n'appartenant pas à S. Si le produit*

$$\prod_{i=1}^{n} \sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_i}))e_{\overline{\chi}}$$

appartient à $\mathbb{Z}[G]$, alors $BS_{non\ ab}(K/k, S)$ implique $BS_{non\ ab}(K/k, S')$.

Démonstration. — Appelons π le produit en question. Grâce aux propriétés d'orthogonalité des idempotents, on remarque que l'on peut aussi écrire π sous la

forme d'une somme,

$$\pi = \sum_{\chi \in \widehat{G}} \left(\prod_{i=1}^{n} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_i})) \right) e_{\overline{\chi}}.$$

On suppose la conjecture de Brumer-Stark non abélienne vraie pour l'ensemble S. Soit $\mathfrak{a}$ un idéal fractionnaire non nul de K. D'après l'identité (3.4.1), on a

$$\mathfrak{a}^{m_G w_K \theta_{K/k,S'}} = \mathfrak{a}^{m_G w_K \pi \theta_{K/k,S}} = \mathfrak{a}^{m_G w_K \theta_{K/k,S} \pi} = (\mathfrak{a}^\pi)^{m_G w_K \theta_{K/k,S}}.$$

D'autre part, $\mathfrak{a}^\pi$ est un idéal fractionnaire non nul de K, donc d'après $BS_{\text{non ab}}(K/k, S)$ que l'on a supposée vérifiée, il existe une anti-unité α de K telle que $(\mathfrak{a}^\pi)^{m_G w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$ et si l'on prend γ une racine w_K-ième de α, l'extension $K(\gamma)$ vérifie la propriété de centralité, ce qui prouve que $\mathfrak{a}$ vérifie $BS_{\text{non ab}}(K/k, S')$ et termine la preuve. □

Dans le cas abélien, on a vu que ce produit a une forme beaucoup plus simple et cette condition est toujours vérifiée. Malheureusement dans le cas non abélien, l'analyse de ce produit est plus délicate et de nombreux cas apparaîssent. On ne dispose donc pas pour l'instant d'un résultat général concernant la dépendance envers l'ensemble S qui soit similaire à celui du cas abélien.

Exemple : on considère le cas où G est isomorphe au groupe des quaternions Q_8 que l'on peut écrire sous la forme $\langle \tau, i, j, k \mid i^2 = j^2 = k^2 = ijk = \tau, \tau^2 = 1 \rangle$. Alors le centre de G est $\{1, \tau\}$, τ est l'unique conjugaison complexe de K, et G admet 5 classes de conjugaisons qui sont $C_1 = \{1\}$, $C_\tau = \{\tau\}$, et $C_l = \{l, l^{-1}\}$ pour l appartenant à $\{i, j, k\}$. La table des caractères de Q_8 est donnée par le tableau suivant :

	C_1	C_τ	C_i	C_j	C_k
1_G	1	1	1	1	1
$\chi_{i,j}$	1	1	−1	−1	1
$\chi_{i,k}$	1	1	−1	1	−1
$\chi_{j,k}$	1	1	1	−1	−1
ψ	2	−2	0	0	0

TABLE 3.1. Table des caractères du groupe des quaternions

Soit $\mathfrak{p}_0$ un idéal premier de k n'appartenant pas à l'ensemble S, et $\mathfrak{P}_0$ un premier quelconque de K au-dessus de $\mathfrak{p}_0$. On cherche à savoir si la somme

$$\sum_{\chi \in \widehat{G}} \det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0})) e_{\overline{\chi}}$$

est ou non dans $\mathbb{Z}[G]$. Pour les caractères χ de degré 1, le terme $\det(1 - \rho_\chi(\sigma_{\mathfrak{P}_0}))$ est égal à $1 - \chi(\sigma_{\mathfrak{P}_0})$. Afin de calculer le terme $\det(1 - \rho_\psi(\sigma_{\mathfrak{P}_0}))$, on a besoin d'expliciter la représentation ρ_ψ. Pour obtenir les valeurs de cette représentation, une façon de procéder est de se servir de l'ordre des éléments de G, ρ_ψ étant un morphisme de groupes, et d'utiliser la décomposition de la représentation régulière

de G. On obtient alors $\rho_\psi(1) = \mathrm{Id}$, $\rho_\psi(\tau) = -\mathrm{Id}$, et pour l appartenant à $\{i,j,k\}$, $\rho_\psi(l)$ est semblable à la matrice $\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$, où $\sqrt{-1}$ désigne une racine carrée de -1 fixée. Le calcul des idempotents centraux donne

$$e_{\overline{1_G}} = \frac{1}{8}\sum_{g\in G} g,$$

$$e_{\overline{\chi_{i,j}}} = \frac{1}{8}(1+\tau+C_k-C_i-C_j), \qquad e_{\overline{\chi_{i,k}}} = \frac{1}{8}(1+\tau+C_j-C_i-C_k),$$
$$e_{\overline{\chi_{j,k}}} = \frac{1}{8}(1+\tau+C_i-C_j-C_k), \qquad e_{\overline{\psi}} = \frac{2}{8}(2-2\tau) = \frac{1}{2}(1-\tau).$$

Si le morphisme de Frobenius $\sigma_{\mathfrak{P}_0}$ est trivial, le terme $\sum_{\chi\in\widehat{G}} \det(1-\rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}}$ est nul, et $BS_{\text{non ab}}(K/k, S\cup\mathfrak{p}_0)$ est trivialement vraie. Si $\sigma_{\mathfrak{P}_0}$ est égal à la conjugaison complexe τ, on a alors

$$\begin{aligned}\sum_{\chi\in\widehat{G}} \det(1-\rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}} &= \det(1-\rho_\psi(\tau))e_{\overline{\psi}} \\ &= \det\begin{pmatrix} 1-\sqrt{-1} & 0 \\ 0 & 1+\sqrt{-1}\end{pmatrix}\frac{1}{2}(1-\tau) \\ &= 2(1-\tau),\end{aligned}$$

qui appartient bien à $\mathbb{Z}[G]$. Dans ce cas, la validité de $BS_{\text{non ab}}(K/k,S)$ implique celle de $BS_{\text{non ab}}(K/k, S\cup\mathfrak{p}_0)$. Prenons l un élément de $\{i,j,k\}$ et supposons que $\sigma_{\mathfrak{P}_0}$ soit dans la classe C_l. On trouve après calculs

$$\sum_{\chi\in\widehat{G}} \det(1-\rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}} = \frac{1}{2}(3-2\tau-l-\tau l),$$

qui n'est pas dans $\mathbb{Z}[G]$, donc on ne peut pas conclure. On peut toutefois remarquer que lorsque l'on choisit deux idéaux premiers distincts de k non dans S, $\mathfrak{p}_0$ et $\mathfrak{p}_1$, si $\sigma_{\mathfrak{p}_0}$ est égale à τ et $\sigma_{\mathfrak{p}_1}$ est un élément de C_l, le produit

$$\sum_{\chi\in\widehat{G}} \det(1-\rho_\chi(\sigma_{\mathfrak{P}_0}))e_{\overline{\chi}} \cdot \sum_{\chi\in\widehat{G}} \det(1-\rho_\chi(\sigma_{\mathfrak{P}_1}))e_{\overline{\chi}}$$

est dans $\mathbb{Z}[G]$ et la proposition précédente donne l'implication de la conjecture $BS_{\text{non ab}}(K/k, S\cup\{\mathfrak{p}_0,\mathfrak{p}_1\})$ par $BS_{\text{non ab}}(K/k,S)$. Nous verrons plus tard (au corollaire 4.18) que dans ce cas particulier où G est isomorphe au groupe des quaternions, la conjecture de Brumer-Stark non abélienne est en fait vraie, ceci pour tout ensemble S considéré.

CHAPITRE 4

GROUPES POSSÉDANT UN SOUS-GROUPE ABÉLIEN DISTINGUÉ D'INDICE PREMIER

On garde les notations des chapitres précédents et on se place dans le cas où k est totalement réel et K totalement complexe. On suppose dans tout ce chapitre que G est un groupe fini non commutatif possédant un sous-groupe abélien distingué H d'indice p où p est un nombre premier. Nous allons voir que dans ce cas, la décomposition de Brauer des caractères irréductibles de G possède une forme simple qui nous permet d'exprimer l'élément de Brumer $\theta_{K/k,S}$ en fonction d'éléments de Brumer-Stickelberger abéliens.

Sous réserve que la conjecture de Brumer-Stark abélienne associée à certaines sous-extensions abéliennes de K/k soit vraie, nous en déduisons deux résultats suivant la parité du cardinal de H. Dans le cas impair, des simplifications surviennent et nous prouvons la conjecture non abélienne. Pour le cas pair, nous obtenons un résultat d'abélianité permettant, sous d'autres hypothèses, la démonstration de $BS_{\text{non ab}}(K/k, S)$.

4.1. Écriture de $\theta_{K/k,S}$ à l'aide d'éléments de Brumer-Stickelberger abéliens

On cherche à expliciter l'élément de Brumer associé à l'extension K/k et à l'ensemble S dans ce cas précis. Nous allons voir qu'il est possible de l'exprimer grâce aux éléments de Brumer-Stickelberger attachés à certaines sous-extensions abéliennes de K/k. Dans cette optique, on commence par étudier les caractères irréductibles de G.

4.1.1. Étude des caractères irréductibles de G. — Soit χ un caractère irréductible de G. On notera $\rho_\chi : G \longrightarrow V_\chi$ une représentation irréductible de G dont χ est le caractère associé. Le degré de χ est $\deg(\chi) = \dim_{\mathbb{C}}(V_\chi) = \chi(1)$. Puisque H est un sous-groupe abélien distingué de G, le degré de toute représentation irréductible de G divise l'indice $(G : H)$ de H dans G. L'indice p étant premier, on en déduit par conséquent que les caractères irréductibles de G sont de degré 1 ou p. On décompose alors $\widehat{G}$ sous la forme

$$\widehat{G} = \widehat{G}_1 \cup \widehat{G}_p \tag{4.1.1}$$

où $\widehat{G}_1$ désigne l'ensemble des caractères irréductibles de degré 1, et $\widehat{G}_p$ celui des caractères irréductibles de degré p. Ces deux ensembles sont non vides, le premier contenant toujours le caractère trivial de G, et le second ayant au moins un élément puisque l'on a supposé le groupe G non abélien.

Notons R_G la représentation régulière de G, on a alors

$$R_G = \bigoplus_{\chi \in \widehat{G}} V_\chi{}^{\chi(1)} = \bigoplus_{\chi \in \widehat{G}_1} V_\chi \oplus \bigoplus_{\chi \in \widehat{G}_p} V_\chi{}^p.$$

De même, si l'on adopte des notations similaires pour le sous-groupe H, on a

$$R_H = \bigoplus_{\varphi \in \widehat{H}} W_\varphi{}^{\varphi(1)} = \bigoplus_{\varphi \in \widehat{H}} W_\varphi,$$

la dernière égalité étant due au fait que les caractères irréductibles d'un groupe abélien sont tous de degré 1. D'un autre côté, la représentation induite dans G par la représentation régulière de H, $\mathrm{Ind}_H^G(R_H)$, n'est rien d'autre que la représentation régulière de G. On a donc l'égalité

$$\bigoplus_{\chi \in \widehat{G}_1} V_\chi \oplus \bigoplus_{\chi \in \widehat{G}_p} V_\chi{}^p = \bigoplus_{\varphi \in \widehat{H}} \mathrm{Ind}_H^G(W_\varphi) = \bigoplus_{\varphi \in \widehat{H}} V_{\mathrm{Ind}_H^G(\varphi)}. \tag{4.1.2}$$

En outre, notons R un système de représentants du quotient G/H. Pour un caractère φ de H, le caractère induit dans G par φ est donné par

$$\mathrm{Ind}_H^G(\varphi)(g) = \sum_{\substack{r \in R \\ r^{-1}gr \in H}} \varphi(r^{-1}gr),$$

pour tout élément g de G. En particulier, le caractère $\mathrm{Ind}_H^G(\varphi)$ est de degré $(G : H) = p$. Si l'on cherche à écrire sa décomposition en caractères irréductibles de G, on obtient donc soit un caractère irréductible de G de degré p, soit la somme de p caractères irréductibles de G de degré 1. On décompose alors $\widehat{H}$ en l'union disjointe $\widehat{H} = \widehat{H}_1 \sqcup \widehat{H}_p$, où $\widehat{H}_1$ désigne l'ensemble des caractères φ de H pour lesquels $\mathrm{Ind}_H^G(\varphi)$ est somme de p caractères irréductibles de degré 1 de G, et $\widehat{H}_p$ l'ensemble de ceux pour lesquels $\mathrm{Ind}_H^G(\varphi)$ est un caractère irréductible de degré p de G. Par construction, l'application induction restreinte à l'ensemble $\widehat{H}_p$

$$\begin{array}{rccc} \mathrm{Ind}_H^G : & \widehat{H}_p & \longrightarrow & \widehat{G}_p \\ & \varphi & \longmapsto & \mathrm{Ind}_H^G(\varphi) \end{array}$$

est à valeurs dans $\widehat{G}_p$. Grâce à la décomposition (4.1.2), on voit que l'image réciproque par cette application d'un caractère χ dans $\widehat{G}_p$, $(\mathrm{Ind}_H^G)^{-1}(\chi)$, contient exactement p caractères distincts de $\widehat{H}_p$, que l'on note $\varphi_{\chi,1}, \ldots, \varphi_{\chi,p}$. On peut alors partitionner $\widehat{H}_p$ de la manière suivante :

$$\widehat{H}_p = \bigsqcup_{\chi \in \widehat{G}_p} (\mathrm{Ind}_H^G)^{-1}(\chi) = \bigsqcup_{\chi \in \widehat{G}_p} \{\varphi_{\chi,1}, \ldots, \varphi_{\chi,p}\}. \tag{4.1.3}$$

De plus, l'application induction envoie un caractère φ de $\widehat{H}_1$ sur une somme de p caractères irréductibles de G, notés $\chi_{\varphi,1}, \ldots, \chi_{\varphi,p}$. En utilisant une nouvelle fois la décomposition (4.1.2), on en déduit que les caractères irréductibles $\chi_{\varphi,i}$

n'apparaissent dans aucune autre décomposition en irréductibles d'un caractère induit par un caractère de H. En d'autres termes, si χ appartient à $\widehat{G}_p$, il existe p caractères de $\widehat{H}_p$ qui l'induisent, et si χ est dans $\widehat{G}_1$, il existe un unique caractère de $\widehat{H}_1$ pour lequel la décomposition en irréductibles du caractère induit dans G contient χ.

D'autre part, la formule de réciprocité de Frobenius, rappelée à la proposition 0.1, implique que l'on a l'égalité, pour tout caractère φ de H, $\langle \chi_{|H}, \varphi\rangle_H = \langle \chi, \mathrm{Ind}_H^G(\varphi)\rangle_G$, où $\chi_{|H}$ désigne la restriction de χ à H. Autrement dit, le nombre de fois où φ apparaît dans la décomposition en irréductibles de $\chi_{|H}$ est égal au nombre de fois où le caractère χ apparaît dans la décomposition de $\mathrm{Ind}_H^G(\varphi)$. Considérons alors un caractère χ appartenant à $\widehat{G}_p$. D'après l'écriture (4.1.3), on sait que χ est égal à $\mathrm{Ind}_H^G(\varphi_{\chi,i})$ pour i appartenant à $\{1,\dots,p\}$ et que les caractères $\varphi_{\chi,i}$ sont les seuls caractères de H dont le caractère induit sur G contient χ. On en déduit les identités $\langle \chi_{|H}, \varphi_{\chi,i}\rangle_H = 1$ pour $i \in \{1,\dots,p\}$ et $\langle \chi_{|H}, \varphi\rangle_H = 0$ pour tout caractère φ de H différent des $\varphi_{\chi,i}$. En définitive, le caractère $\chi_{|H}$ de H est égal à la somme $\varphi_{\chi,1} + \cdots + \varphi_{\chi,p}$.

Si l'on considère à présent un caractère φ appartenant à $\widehat{H}_1$, $\mathrm{Ind}_H^G(\varphi)$ est somme des p caractères irréductibles de degré 1, $\chi_{\varphi,1},\dots,\chi_{\varphi,p}$, et il est le seul caractère induit dans lequel $\chi_{\varphi,i}$ apparaît dans la décomposition en irréductibles. Pour un entier i fixé dans $\{1,\dots,p\}$, le produit scalaire $\langle \varphi, \chi_{\varphi,i_{|H}}\rangle_H$ est donc égal à 1, mais si ψ est un caractère de H différent de φ, le produit scalaire $\langle \psi, \chi_{\varphi,i_{|H}}\rangle_H$ est nul. Ceci implique l'égalité entre la restriction de $\chi_{\varphi,i}$ à H et φ, pour tout i. L'application restriction à H, considérée seulement sur l'ensemble $\widehat{G}_1$,

$$\begin{array}{rccc} \mathrm{Res}_H : & \widehat{G}_1 & \longrightarrow & \widehat{H}_1 \\ & \chi & \longmapsto & \chi_{|H} \end{array}$$

est à valeurs dans $\widehat{H}_1$ par construction, et pour tout caractère φ de $\widehat{H}_1$, l'image réciproque de φ, $(\mathrm{Res}_H)^{-1}(\varphi)$ contient p caractères de $\widehat{G}_1$, à savoir $\chi_{\varphi,1},\dots,\chi_{\varphi,p}$.

On peut résumer cette étude des caractères irréductibles dans la proposition suivante.

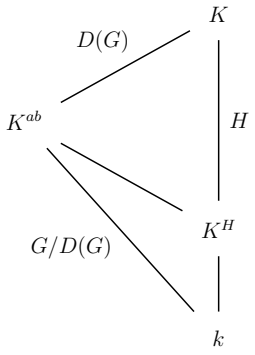
Proposition 4.1. — *Notons $\widehat{G}_1$ (resp. $\widehat{G}_p$) l'ensemble des caractères irréductibles de G de degré 1 (resp. p) de sorte que $\widehat{G} = \widehat{G}_1 \sqcup \widehat{G}_p$, et $\widehat{H}_1$ (resp. $\widehat{H}_p$) l'ensemble des caractères de H dont le caractère induit dans G est réductible (resp. irréductible de degré p) afin d'obtenir $\widehat{H} = \widehat{H}_1 \sqcup \widehat{H}_p$. On dispose des partitions suivantes :*

$$\widehat{H}_p = \bigsqcup_{\chi\in\widehat{G}_p} (\mathrm{Ind}_H^G)^{-1}(\chi),$$
$$\widehat{G}_1 = \bigsqcup_{\varphi\in\widehat{H}_1} (\mathrm{Res}_H)^{-1}(\varphi)$$

où l'on note $(\mathrm{Ind}_H^G)^{-1}(\chi) = \{\varphi_{\chi,1}, \ldots, \varphi_{\chi,p}\}$ *et* $(\mathrm{Res}_H)^{-1}(\varphi) = \{\chi_{\varphi,1}, \ldots, \chi_{\varphi,p}\}$. *De plus, on a aussi les identités*

$$\begin{aligned} \chi_{|_H} &= \varphi_{\chi,1} + \cdots + \varphi_{\chi,p}, \quad \forall \chi \in \widehat{G}_p, \\ \mathrm{Ind}_H^G(\varphi) &= \chi_{\varphi,1} + \cdots + \chi_{\varphi,p}, \quad \forall \varphi \in \widehat{H}_1. \end{aligned}$$

4.1.2. Expression explicite de $\theta_{K/k,S}$. — Cette étude préliminaire des caractères irréductibles de G effectuée, on peut décomposer l'élément de Brumer en une combinaison linéaire d'éléments de Brumer-Stickelberger abéliens. Notons $D(G)$ le groupe dérivé de G. On désignera par K^{ab} le sous-corps de K fixé par $D(G)$. Puisque H est un sous-groupe distingué d'indice premier, le quotient G/H est un groupe de cardinal premier, donc en particulier abélien. Par conséquent H contient le groupe dérivé $D(G)$. On résume ceci dans le diagramme suivant :



Si F est une sous-extension de K/k, on désignera par $N_{K/F} = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma$ la norme formelle de K sur F constituée de la somme des éléments du groupe de Galois $\mathrm{Gal}(K/F)$. On rappelle que S désigne un ensemble fini de places de k contenant les places infinies et les places finies qui se ramifient dans K, et possédant au moins deux éléments. On peut alors exprimer $\theta_{K/k,S}$ sous la forme suivante, les extensions intervenant étant toutes abéliennes.

Théorème 4.2. — *L'élément de Brumer associé à l'extension K/k et à l'ensemble S se décompose sous la forme*

$$\theta_{K/k,S} = \frac{1}{|D(G)|}\left(\theta_{K^{ab}/k,S} N_{K/K^{ab}} - \theta_{K^{ab}/K^H,S_H} N_{K/K^{ab}}\right) + \theta_{K/K^H,S_H}$$

où S_H désigne l'ensemble des places de K^H au-dessus des places de S.

Remarque. — Soit F une sous-extension de K/k galoisienne sur k. Si x est un élément de $\mathbb{Q}[G]$, l'élément $x \cdot N_{K/F}$ agit sur les éléments de K comme $x_{|_F} \cdot N_{K/F}$, c'est pourquoi on fera dans tout le chapitre l'abus de notation $x \cdot N_{K/F} = \overline{x} \cdot N_{K/F}$, où $\overline{x}$ désigne l'élément de $\mathrm{Gal}(F/k)$ dont x est un relèvement. Ceci explique la présence dans le théorème précédent des termes $\theta_{K^{ab}/k,S} N_{K/K^{ab}}$ et $\theta_{K^{ab}/K^H,S_H} N_{K/K^{ab}}$, considérés comme des éléments de $\mathbb{Q}[G]$.

Démonstration. — Pour commencer, l'écriture (4.1.1) nous permet de décomposer $\theta_{K/k,S}$ de la manière suivante :

$$\theta_{K/k,S} = \sum_{\chi\in\widehat{G}_1} L_{K/k,S}(0,\chi)e_{\overline{\chi}} + \sum_{\chi\in\widehat{G}_p} L_{K/k,S}(0,\chi)e_{\overline{\chi}}.$$

L'idée, pour obtenir une expression explicite de $\theta_{K/k,S}$, est d'utiliser la décomposition de Brauer des caractères irréductibles de G et de faire ensuite apparaître des éléments de Brumer associés à des sous-extensions abéliennes de K/k, grâce aux propriétés particulières vérifiées par les fonctions L d'Artin.

On commence par s'intéresser au premier terme, où seuls les caractères de degré 1 interviennent, puisque ceux-ci sont déjà décomposés. Soit χ un caractère appartenant à $\widehat{G}_1$. Puisque l'extension $K^{\ker(\chi)}/k$ est cyclique, donc en particulier abélienne, $\ker(\chi)$ contient le groupe dérivé de G. Comme ceci est valable pour tous les caractères de degré 1 de G, notre but est de relier le terme $\displaystyle\sum_{\chi\in\widehat{G}_1} L_{K/k,S}(0,\chi)e_{\overline{\chi}}$ à l'élément de Brumer associé à l'extension K^{ab}/k. Pour un caractère χ de degré 1, l'idempotent associé à $\overline{\chi}$ est $e_{\overline{\chi}} = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi(g)g$. Puisque $D(G)$ est distingué dans G, on peut décomposer G comme la somme disjointe $G = \displaystyle\bigsqcup_{i=1}^{(G:D(G))} g_iD(G)$ où les $g_i \in G$ sont des représentants de $G/D(G)$, ce qui nous permet de réorganiser la somme :

$$\begin{aligned} e_{\overline{\chi}} &= \frac{1}{|G|}\sum_{i=1}^{(G:D(G))}\sum_{g'\in D(G)}\chi(g_ig')g_ig' \\ &= \frac{1}{|G|}\sum_{i=1}^{(G:D(G))}\sum_{g'\in D(G)}\chi(g_i)\chi(g')g_ig' \end{aligned}$$

puisque χ est un morphisme de groupes de G dans $\mathbb{C}^\times$, car de degré 1. D'autre part, $D(G)$ est inclus dans le noyau $\ker(\chi)$ donc on a aussi l'égalité $\chi(g') = 1$, pour tout $g' \in D(G)$. En reportant ceci dans l'expression de $e_{\overline{\chi}}$, on trouve

$$\begin{aligned} e_{\overline{\chi}} &= \frac{1}{|G|}\sum_{i=1}^{(G:D(G))}\sum_{g'\in D(G)}\chi(g_i)g_ig' \\ &= \frac{1}{|G|}\sum_{i=1}^{(G:D(G))}\chi(g_i)g_i\sum_{g'\in D(G)}g' \\ &= \frac{1}{|G|}\sum_{i=1}^{(G:D(G))}\chi(g_i)g_iN_{K/K^{ab}}. \end{aligned}$$

De plus, toujours grâce à l'inclusion de $D(G)$ dans $\ker(\chi)$, le caractère χ passe au quotient par $D(G)$ pour donner le caractère

$$\begin{array}{rccc} \chi^{\curlyvee} : & G/D(G) & \longrightarrow & \mathbb{C}^{\times} \\ & \overline{g} & \longmapsto & \chi^{\curlyvee}(\overline{g}) = \chi(g). \end{array}$$

Le quotient $G/D(G)$ étant tout simplement l'ensemble $\{\overline{g_1}, \ldots, \overline{g_{(G:D(G))}}\}$, on obtient finalement

$$\begin{aligned} e_{\overline{\chi}} &= \frac{1}{|G|} \sum_{\overline{g} \in G/D(G)} \chi^{\curlyvee}(\overline{g}) \overline{g} N_{K/K^{ab}} \\ &= \frac{(G : D(G))}{|G|} e_{\overline{\chi^{\curlyvee}}} N_{K/K^{ab}} \\ &= \frac{1}{|D(G)|} e_{\overline{\chi^{\curlyvee}}} N_{K/K^{ab}}. \end{aligned}$$

Le caractère χ est en réalité le caractère relevé de $\chi^{\curlyvee}$ à G, $\mathrm{Infl}(\chi^{\curlyvee})$. D'après la propriété d'inflation (2.1.3) des fonctions L d'Artin, on sait de plus que $L_{K/k,S}(0, \chi)$ est égal à $L_{K^{ab}/k,S}(0, \chi^{\curlyvee})$. Il reste à voir si $\chi^{\curlyvee}$ parcourt tous les caractères de $G/D(G)$ lorsque χ parcourt les éléments de $\widehat{G}_1$.

Lemme 4.3. — *Pour un caractère $\chi \in \widehat{G}_1$, on note $\chi^{\curlyvee} : G/D(G) \longrightarrow \mathbb{C}^{\times}$ le caractère défini par $\chi^{\curlyvee}(\overline{g}) = \chi(g)$. L'application de $\widehat{G}_1$ dans $\widehat{G/D(G)}$ qui à χ associe $\chi^{\curlyvee}$ réalise une bijection de $\widehat{G}_1$ dans $\widehat{G/D(G)}$.*

Démonstration du lemme. — L'application définie précédemment a pour application réciproque l'application inflation

$$\begin{array}{ccc} \widehat{G/D(G)} & \longrightarrow & \widehat{G}_1 \\ \psi & \longmapsto & \mathrm{Infl}(\psi). \end{array}$$

En effet, on a l'égalité $\chi = \mathrm{Infl}(\chi^{\curlyvee})$. De plus, il est clair que pour tout $\psi \in \widehat{G/D(G)}$ et pour tout $\overline{g}$ dans $G/D(G)$, $\mathrm{Infl}(\psi)^{\curlyvee}(\overline{g}) = \mathrm{Infl}(\psi)(g) = \psi(\overline{g})$. On a bien une bijection entre les caractères de G de degré 1 et les caractères de $G/D(G)$. □

Ce lemme nous permet d'obtenir la forme finale concernant le premier terme de $\theta_{K/k,S}$,

$$\begin{aligned} \sum_{\chi \in \widehat{G}_1} L_{K/k,S}(0, \chi) e_{\overline{\chi}} &= \sum_{\chi \in \widehat{G}_1} L_{K^{ab}/k,S}(0, \chi^{\curlyvee}) \frac{1}{|D(G)|} e_{\overline{\chi^{\curlyvee}}} N_{K/K^{ab}} \\ &= \frac{1}{|D(G)|} \sum_{\chi^{\curlyvee} \in \widehat{G/D(G)}} L_{K^{ab}/k,S}(0, \chi^{\curlyvee}) e_{\overline{\chi^{\curlyvee}}} N_{K/K^{ab}} \\ &= \frac{1}{|D(G)|} \theta_{K^{ab}/k,S} N_{K/K^{ab}}, \end{aligned}$$

qui est le premier terme voulu.

On s'intéresse désormais à la partie de $\theta_{K/k,S}$ où interviennent uniquement les caractères de degré p de G. Pour cela, on va se servir de l'étude concernant les caractères de G réalisée précédemment. Soit χ appartenant à $\widehat{G}_p$. Puisque χ

est égal au caractère induit $\mathrm{Ind}_H^G(\varphi_{\chi,i})$ pour i compris entre 1 et p, d'après la proposition 4.1, on peut écrire pour tout g dans G

$$\chi(g) = \sum_{\substack{r\in R\\ r^{-1}gr\in H}} \varphi_{\chi,i}(r^{-1}gr). \tag{4.1.4}$$

Simplifions cette expression. Si g est un élément de H, puisque H est distingué dans G, on dispose de l'identité $t^{-1}Ht = H$ pour tout t de G. En particulier, pour tout représentant r dans R, l'élément $r^{-1}gr$ appartient à H. Sommer sur les éléments r de R vérifiant $r^{-1}gr \in H$ revient simplement à sommer sur les éléments de R. Au contraire, si g n'est pas dans H, quel que soit l'élément r de R choisi, la quantité $r^{-1}gr$ ne peut pas appartenir à H sinon l'élément g s'écrirait sous la forme rhr^{-1} pour un certain h dans H. Ainsi la somme intervenant en (4.1.4) est nulle. Pour résumer, le caractère χ est donc nul en dehors de H. L'idempotent associé à $\overline{\chi}$ se résume alors à

$$e_{\overline{\chi}} = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g)g = \frac{p}{|G|}\sum_{h\in H}\chi(h)h = \frac{1}{|H|}\sum_{h\in H}\chi_{|H}(h)h$$

où $\chi_{|H}$ désigne la restriction de χ à H. On utilise alors la décomposition de $\chi_{|H}$ en caractères irréductibles de H donnée par la proposition 4.1. Puisque χ appartient à $\widehat{G}_p$, elle s'écrit $\chi_{|H} = \varphi_{\chi,1} + \cdots + \varphi_{\chi,p}$. En réinjectant ceci dans l'expression de $e_{\overline{\chi}}$ on obtient

$$e_{\overline{\chi}} = \frac{1}{|H|}\sum_{h\in H}(\varphi_{\chi,1} + \cdots + \varphi_{\chi,p})(h)h = e_{\overline{\varphi_{\chi,1}}} + \cdots + e_{\overline{\varphi_{\chi,p}}}.$$

La propriété d'induction (2.1.2) des fonctions L d'Artin permet alors d'écrire le second terme intervenant dans l'élément de Brumer sous la forme

$$\begin{aligned}\sum_{\chi\in\widehat{G}_p} L_{K/k,S}(0,\chi)e_{\overline{\chi}} &= \sum_{\chi\in\widehat{G}_p} L_{K/k,S}(0,\chi)(e_{\overline{\varphi_{\chi,1}}} + \cdots + e_{\overline{\varphi_{\chi,p}}})\\ &= \sum_{\chi\in\widehat{G}_p}\sum_{i=1}^{p} L_{K/K^H,S_H}(0,\varphi_{\chi,i})e_{\overline{\varphi_{\chi,i}}}. \qquad (4.1.5)\end{aligned}$$

Or, la proposition 4.1 donne aussi une partition de $\widehat{H}_p$ sous la forme

$$\widehat{H}_p = \bigsqcup_{\chi\in\widehat{G}_p}\{\varphi_{\chi,1},\ldots,\varphi_{\chi,p}\} = \bigsqcup_{\chi\in\widehat{G}_p}(\mathrm{Ind}_H^G)^{-1}(\chi).$$

La somme (4.1.5) peut alors être réinterprétée de la manière suivante

$$\begin{aligned}\sum_{\chi\in\widehat{G}_p} L_{K/k,S}(0,\chi)e_{\overline{\chi}} &= \sum_{\chi\in\widehat{G}_p}\sum_{\varphi\in(\mathrm{Ind}_H^G)^{-1}(\chi)} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}}\\ &= \sum_{\varphi\in\widehat{H}_p} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}}.\end{aligned}$$

Afin d'obtenir l'élément de Brumer-Stickelberger associé à l'extension K/K^H, on fait apparaître tous les caractères de $\widehat{H}$ dans cette expression, ce qui donne

$$\begin{aligned}\sum_{\chi\in\widehat{G}_p} L_{K/k,S}(0,\chi)e_{\overline{\chi}} &= \sum_{\varphi\in\widehat{H}} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}} - \sum_{\varphi\in\widehat{H}_1} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}} \\ &= \theta_{K/K^H,S_H} - \sum_{\varphi\in\widehat{H}_1} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}}.\end{aligned}$$

On traite ensuite le dernier terme de manière similaire au terme qui ne faisait intervenir que des caractères appartenant à $\widehat{G}_1$. Pour cela, on utilise le fait que pour tout caractère φ appartenant à $\widehat{H}_1$, il existe p caractères dans $\widehat{G}_1$, $\chi_{\varphi,1},\ldots,\chi_{\varphi,p}$, dont la restriction à H est égale à φ. De plus, puisque $\chi_{\varphi,i}$ appartient à $\widehat{G}_1$, nous avons vu que le groupe dérivé $D(G)$ est inclus dans $\ker(\chi_{\varphi,i})$. D'autre part, l'indice $(G : H)$ étant premier, le quotient G/H est cyclique et ainsi H contient $D(G)$. Pour tout g' dans $D(G)$, l'élément $\varphi(g') = \chi_{\varphi,i|_H}(g')$ est donc égal à 1, et $D(G)$ est aussi inclus dans $\ker(\varphi)$. Pour tout φ appartenant à $\widehat{H}_1$, on peut alors comme précédemment passer au quotient par $D(G)$ pour définir un caractère

$$\begin{array}{rccc}\widetilde{\varphi}: & H/D(G) & \longrightarrow & \mathbb{C} \\ & \overline{h} & \longmapsto & \widetilde{\varphi}(\overline{h}) = \varphi(h).\end{array}$$

On démontre alors par le même calcul qu'auparavant l'égalité

$$e_{\overline{\varphi}} = \frac{1}{|D(G)|} e_{\overline{\widetilde{\varphi}}} N_{K/K^{ab}}.$$

Cependant, démontrer la bijection entre l'ensemble des caractères de $H/D(G)$ et $\widehat{H}_1$ dont on a besoin ne se fait pas de manière aussi directe qu'auparavant. On admet pour l'instant le lemme suivant.

Lemme 4.4. — *Pour un caractère $\varphi \in \widehat{H}_1$, on désigne par $\widetilde{\varphi} : H/D(G) \longrightarrow \mathbb{C}$ le caractère défini par $\widetilde{\varphi}(\overline{h}) = \varphi(h)$. L'application de $\widehat{H}_1$ dans $\widehat{H/D(G)}$ qui à φ associe $\widetilde{\varphi}$ réalise une bijection de $\widehat{H}_1$ dans $\widehat{H/D(G)}$.*

Le dernier terme non explicité de l'élément de Brumer devient alors

$$\begin{aligned}\sum_{\varphi\in\widehat{H}_1} L_{K/K^H,S_H}(0,\varphi)e_{\overline{\varphi}} &= \sum_{\varphi\in\widehat{H}_1} L_{K^{ab}/K^H,S_H}(0,\widetilde{\varphi})\frac{1}{|D(G)|}e_{\overline{\widetilde{\varphi}}}N_{K/K^{ab}} \\ &= \frac{1}{|D(G)|}\sum_{\widetilde{\varphi}\in\widehat{H/D(G)}} L_{K^{ab}/K^H,S_H}(0,\widetilde{\varphi})e_{\overline{\widetilde{\varphi}}}N_{K/K^{ab}} \\ &= \frac{1}{|D(G)|}\theta_{K^{ab}/K^H,S_H}N_{K/K^{ab}},\end{aligned}$$

ce qui en regroupant tous les termes donne bien le résultat voulu. □

Revenons à présent sur la démonstration du lemme 4.4.

Démonstration du lemme 4.4. — On considère l'application

$$\begin{array}{ccc}\widehat{H}_1 & \longrightarrow & \widehat{H/D(G)} \\ \varphi & \longmapsto & \widetilde{\varphi}\end{array}$$

qui est clairement injective. Pour la surjectivité, il suffit de vérifier que le caractère relevé à H d'un caractère ψ de $\widehat{H/D(G)}$, noté $\mathrm{Infl}_H(\psi)$, est bien dans $\widehat{H}_1$ et non dans $\widehat{H}_p$. Puisqu'il n'y a que deux choix possibles pour la décomposition en irréductibles de $\mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))$, on va en fait démontrer que $\mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))$ n'est pas un caractère irréductible de G. Pour cela, on calcule le produit scalaire de $\mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))$ par lui-même dans G, cette quantité étant égale à 1 si et seulement si le caractère $\mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))$ est irréductible :

$$\begin{aligned}
&\langle \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi)), \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))\rangle_G \\
&\qquad = \langle \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))_{|_H}, \mathrm{Infl}_H(\psi)\rangle_H \\
&\qquad = \frac{1}{|H|}\sum_{h\in H} \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))(h)\,\mathrm{Infl}_H(\psi)(h^{-1}) \\
&\qquad = \frac{1}{|H|}\sum_{h\in H}\left(\sum_{\substack{r\in R\\ r^{-1}hr\in H}} \mathrm{Infl}_H(\psi)(r^{-1}hr)\right)\mathrm{Infl}_H(\psi)(h^{-1}) \\
&\qquad = \frac{1}{|H|}\sum_{h\in H}\sum_{r\in R}\psi(\overline{r^{-1}hr})\psi(\overline{h^{-1}}) \\
&\qquad = \frac{1}{|H|}\sum_{h\in H}\sum_{r\in R}\psi(\overline{r^{-1}hr}\cdot\overline{h^{-1}})
\end{aligned}$$

puisque ψ est un caractère du groupe abélien $H/D(G)$ donc en particulier un morphisme de groupes. De plus, pour r dans R, le produit de classes $\overline{r^{-1}hr}\cdot\overline{h^{-1}}$ est égal à la classe $\overline{r^{-1}hrh^{-1}}$. L'élément $r^{-1}hrh^{-1}$ appartenant au groupe dérivé de G, on obtient donc $\psi(\overline{r^{-1}hrh^{-1}}) = 1$. Finalement le produit scalaire recherché vaut

$$\langle \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi)), \mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))\rangle_G = \frac{|H||R|}{|H|} = (G:H) \neq 1.$$

Par suite, le caractère $\mathrm{Ind}_H^G(\mathrm{Infl}_H(\psi))$ n'est pas irréductible mais est somme de p caractères irréductibles de G. Le caractère relevé $\mathrm{Infl}_H(\psi)$ est donc bien dans l'ensemble $\widehat{H}_1$ ce qui achève la preuve de la bijection entre les ensembles $\widehat{H}_1$ et $\widehat{H/D(G)}$. □

Cette écriture de $\theta_{K/k,S}$ à l'aide d'éléments de Brumer-Stickelberger associés à certaines sous-extensions abéliennes de K/k nous permet d'utiliser les résultats connus dans le cas abélien pour obtenir des informations dans ce cas.

4.2. Dénominateur de l'élément de Brumer

On s'intéresse à la vérification du postulat concernant le dénominateur de l'élément $\theta_{K/k,S}$. Commençons par donner une propriété de divisibilité vérifiée par l'élément m_G. On rappelle que m_G est le ppcm des cardinaux des classes de conjugaison de G.

4.2.1. Calcul de m_G. — Puisque $(G : H)$ est premier, G/H est cyclique, donc on peut écrire G/H sous la forme $G/H = \langle \overline{g_0} \rangle$, où g_0 est un élément de G dont la classe dans G/H est d'ordre p. On a en particulier que g_0^i n'appartient pas à H pour tout entier i compris entre 1 et $p-1$, et g_0^p appartient à H. On a $G = \bigsqcup_{i=0}^{p-1} g_0^i H$, où les unions sont toutes disjointes.

Avant de calculer explicitement les classes de conjugaison de G, on démontre un lemme concernant le centre de G.

Lemme 4.5. — *Le centre de G, noté $Z(G)$, est inclus dans H, et plus précisément, il est égal à l'ensemble $\{h \in H : hg_0 = g_0 h\}$.*

Démonstration. — Soit h un élément de H commutant avec g_0. Alors h commute avec toutes les puissances de g_0, donc il commute avec n'importe quel élément de la forme $g_0^i h$. Ainsi h est dans le centre de G.

Réciproquement, soit g un élément du centre de G. L'élément g commute bien évidemment avec g_0 mais montrons qu'il appartient en réalité à H. Il existe un certain entier i appartenant à $\{0, \ldots, p-1\}$ et un élément h de H tel que $g = g_0^i h$. Supposons i non nul, alors pour tout h' dans H, on a $g_0^i h h' = h' g_0^i h$, ce qui donne $g_0^i h' h = h' g_0^i h$ et en simplifiant par h, on trouve que les éléments h' et g_0^i commutent entre eux. Montrons que ceci implique en particulier que h' commute avec g_0. Puisque i est non nul, $\overline{g_0^i}$ est d'ordre p premier et les sous-groupes engendrés $\langle \overline{g_0^i} \rangle$ et $\langle \overline{g_0} \rangle$ sont égaux. Il existe donc l appartenant à $\{1, \ldots, p-1\}$ tel que $\overline{g_0} = \overline{g_0^i}^l$. On peut donc trouver un élément h'' de H vérifiant $g_0 = g_0^{li} h''$. Mais alors $g_0 h' = g_0^{li} h'' h' = h' g_0^{li} h'' = h' g_0$. Ainsi h' commute avec g_0 pour tout élément h' de H, ce qui implique que g_0 commute avec H tout entier ce qui n'est pas vrai puisque l'on a supposé G non abélien. Ainsi l'entier i est nul et g appartient bien à H, ce qui conclut la preuve. □

On peut alors calculer le cardinal de certaines classes de conjugaison de G.

Lemme 4.6. — *Soit h un élément de H. Le cardinal de la classe de conjugaison de h vaut 1 si h est dans le centre de G, et p sinon.*

Démonstration. — Prenons un élément h dans H, la classe de conjugaison de h dans G est $C_h = \{ghg^{-1} : g \in G\}$. En utilisant l'écriture $G = \bigsqcup_{i=0}^{p-1} g_0^i H$, cette classe s'écrit

$$\begin{aligned} C_h &= \bigcup_{i=0}^{p-1} \left\{ g_0^i k h (g_0^i k)^{-1} : k \in H \right\} \\ &= \bigcup_{i=0}^{p-1} \{ g_0^i h g_0^{-i} \}. \end{aligned}$$

Supposons qu'il existe $i \neq j$ dans $\{0, \ldots, p-1\}$ tel que $g_0^i h g_0^{-i} = g_0^j h g_0^{-j}$. Ceci est équivalent à l'égalité $g_0^{j-i} h = h g_0^{j-i}$. Puisque $j - i$ est non nul, d'après ce que

l'on a vu précédemment ceci implique que h est dans le centre de G. Finalement la classe de h est donc

$$C_h = \begin{cases} \{h\} \text{ si } h \in Z(G) \\ \{h, g_0 h g_0^{-1}, \ldots, g_0^{p-1} h g_0^{-(p-1)}\} \text{ sinon,} \end{cases}$$

ce qui donne le résultat voulu sur le cardinal de C_h. □

On cherche désormais le cardinal des classes de conjugaison des éléments de la forme $g_0^i h$, où i est un entier entre 1 et $p-1$ et h un élément de H. On ne pourra calculer explicitement ce cardinal en toute généralité que lorsque l'élément h appartient à $Z(G)$.

Lemme 4.7. — *Soit i un entier entre 1 et $p-1$. Si h appartient au centre de G, le cardinal de la classe de conjugaison de $g_0^i h$ vaut*

$$|C_{g_0^i h}| = \frac{|G|}{p|Z(G)|}.$$

Démonstration. — Soit h appartenant à $Z(G)$ et i dans $\{1, \ldots, p-1\}$. Puisque le cardinal de $C_{g_0^i h}$ est

$$|C_{g_0^i h}| = \frac{|G|}{|\mathrm{Stab}_G(g_0^i h)|}$$

où $\mathrm{Stab}_G(g_0^i h) = \{g \in G : g g_0^i h = g_0^i h g\}$ est le stabilisateur dans G de $g_0^i h$, on va calculer le cardinal du stabilisateur. On peut écrire $\mathrm{Stab}_G(g_0^i h)$ sous la forme

$$\mathrm{Stab}_G(g_0^i h) = \bigcup_{j=0}^{p-1} \{g_0^j k : k \in H \text{ et } g_0^j k g_0^i h = g_0^i h g_0^j k\}.$$

Or, pour un entier j entre 0 et $p-1$, l'ensemble qui apparaît peut se simplifier en utilisant l'appartenance de h à $Z(G)$:

$$\begin{aligned} \{g_0^j k : k \in H \text{ et } g_0^j k g_0^i h = g_0^i h g_0^j k\} &= \{g_0^j k : k \in H \text{ et } g_0^j k g_0^i h = g_0^{i+j} k h\} \\ &= \{g_0^j k : k \in H \text{ et } g_0^j k g_0^i = g_0^{i+j} k\} \\ &= \{g_0^j k : k \in H \text{ et } k g_0^i = g_0^i k\} \\ &= \{g_0^j k : k \in Z(G)\}. \end{aligned}$$

De cette façon, le stabilisateur est

$$\mathrm{Stab}_G(g_0^i h) = \bigcup_{j=0}^{p-1} \{g_0^j k : k \in Z(G)\}.$$

Les unions intervenant ci-dessus étant disjointes, ceci implique donc que lorsque h est dans le centre de G et i non nul, le cardinal de $C_{g_0^i h}$ est donné par la formule

$$|C_{g_0^i h}| = \frac{|G|}{p|Z(G)|}.$$

□

Remarque. — Lorsque l'élément h n'est pas dans le centre de G, le calcul semble plus difficile. Toutefois dans le cas particulier où l'indice p est égal à 2, l'appartenance de g_0^2 à H permet d'exprimer la classe de g_0h en fonction de celle de g_0. En effet, dans ce cas la classe de conjugaison de g_0h s'écrit $C_{g_0h} = \{kg_0hk^{-1} : k \in H\} \cup \{kg_0(g_0h)g_0^{-1}k^{-1} : k \in H\}$, or les deux ensembles intervenant sont tous deux égaux à $\{kg_0k^{-1} : k \in H\} \cdot h$. En effet, on a

$$\begin{aligned}
\{kg_0(g_0h)g_0^{-1}k^{-1} : k \in H\} &= \{kg_0^2hg_0^{-1}k^{-1} : k \in H\} \\
&= \{khg_0^2g_0^{-1}k^{-1} : k \in H\} \\
&= \{khg_0k^{-1} : k \in H\} \\
&= \{(kh)g_0(kh)^{-1} : k \in H\} \cdot h \\
&= \{h'g_0h'^{-1} : h' \in H\} \cdot h.
\end{aligned}$$

La classe de conjugaison de C_{g_0h} est donc égale à la classe de C_{g_0} multipliée à droite par h, ce qui nous permet d'obtenir dans ce cas le cardinal de toutes les classes de conjugaison de G et de calculer explicitement le nombre m_G.

Puisque l'on cherche à vérifier la validité du postulat concernant le dénominateur de $\theta_{K/k,S}$, on s'intéresse surtout à l'intégralité de $\dfrac{m_G}{|D(G)|}$. Pour ceci, la connaissance exacte de toutes les classes de conjugaison n'est pas nécessaire. En effet, le résultat obtenu au lemme 4.7 est suffisant pour démontrer que le quotient $\dfrac{m_G}{|D(G)|}$ est en réalité un nombre entier.

Lemme 4.8. — *Le nombre m_G est divisible par le cardinal du groupe dérivé de G.*

Démonstration. — La démonstration fait appel à un lemme que l'on peut trouver sous cette forme dans [**Isa08**, p.118] :

Lemme 4.9. — *Soit A un sous-groupe abélien distingué d'un groupe G tel que G/A est cyclique. Alors le groupe dérivé de G est $D(G) = [A, G]$ et*

$$D(G) \simeq A/(A \cap Z(G)).$$

Puisque H remplit les conditions du lemme, on a alors l'isomorphisme

$$D(G) \simeq H/(H \cap Z(G)) = H/Z(G).$$

Ainsi le cardinal du groupe dérivé de G vaut

$$|D(G)| = \frac{|H|}{|Z(G)|} = \frac{|G|}{p|Z(G)|} = |C_{g_0^ih}|$$

pour tout h appartenant à $Z(G)$ et pour tout i entier entre 1 et $p-1$. Ceci démontre que m_G est un multiple du cardinal du groupe dérivé de G et conclut la preuve. □

4.2.2. Vérification d'une partie du postulat. — En utilisant les propriétés d'intégralité des éléments de Brumer-Stickelberger abéliens, on obtient la vérification d'une partie du postulat sur le dénominateur de $\theta_{K/k,S}$, grâce à la forme de l'élément de Brumer donnée au théorème 4.2 ainsi qu'au lemme précédent.

Corollaire 4.10. — *Pour presque tout idéal premier $\mathfrak{P}$ de K dont le morphisme de Frobenius $\sigma_{\mathfrak{P}}$ associé à l'extension K/k est dans H, l'élément $m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$, où $\mathfrak{p}$ désigne toujours l'idéal premier de k en-dessous de $\mathfrak{P}$.*
De plus, l'élément $m_G w_K \theta_{K/k,S}$ est à coefficients entiers.

Remarque. — Avant de démontrer ce résultat, on peut observer l'égalité entre les groupes $\mu(K)$ et $\mu(K^{ab})$. En effet, puisque l'extension $k(\mu(K))$, définie comme $k(\zeta : \zeta \in \mu(K))$, est une extension abélienne de k, elle est forcément contenue dans l'extension K^{ab}. En particulier, son groupe des racines de l'unité, qui n'est rien d'autre que $\mu(K)$, est inclus dans $\mu(K^{ab})$. L'inclusion inverse étant immédiate, les groupes des racines de l'unité de K et K^{ab} sont les mêmes.

Démonstration du corollaire. — On part de l'écriture de $\theta_{K/k,S}$ du théorème 4.2 :

$$\theta_{K/k,S} = \frac{1}{|D(G)|}\left(\theta_{K^{ab}/k,S} N_{K/K^{ab}} - \theta_{K^{ab}/K^H,S_H} N_{K/K^{ab}}\right) + \theta_{K/K^H,S_H}.$$

On considère un ensemble d'idéaux premiers $\mathcal{T}$ de K vérifiant les hypothèses du lemme 2.16. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{T}$ dont le Frobenius $\sigma_{\mathfrak{P}}$ appartient à H. La quantité $\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p})$ est dans l'anneau de groupe $\mathbb{Z}[H]$ et annule le groupe des racines de l'unité $\mu(K)$. C'est pourquoi, d'après les propriétés de l'élément de Stickelberger associé à l'extension abélienne K/K^H, la quantité $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K/K^H,S_H}$ appartient à $\mathbb{Z}[H]$, donc en particulier à $\mathbb{Z}[G]$. Par conséquent, la multiplier par l'entier m_G donne un élément de $\mathbb{Z}[G]$.

Pour les termes restants, on écrit $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S} N_{K/K^{ab}}$ sous la forme $(\sigma_{\mathfrak{P}|_{K^{ab}}} - \mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S} N_{K/K^{ab}}$. Puisque $\sigma_{\mathfrak{P}|_{K^{ab}}}$ appartient au groupe de Galois $\mathrm{Gal}(K^{ab}/K^H)$, lui-même inclus dans $\mathrm{Gal}(K^{ab}/k)$, $\sigma_{\mathfrak{P}|_{K^{ab}}} - \mathcal{N}(\mathfrak{p})$ est dans $\mathbb{Z}[\mathrm{Gal}(K^{ab}/k)]$ et annule $\mu(K) = \mu(K^{ab})$. De cette manière, l'élément $(\sigma_{\mathfrak{P}|_{K^{ab}}} - \mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S}$ est à coefficients entiers, et il en va de même de $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S} N_{K/K^{ab}}$. Le dernier terme $(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/K^H,S_H} N_{K/K^{ab}}$ se traite exactement de la même manière. Comme $\dfrac{m_G}{|D(G)|}$ est entier d'après le lemme 4.8, on en déduit ainsi l'intégralité de l'élément de Brumer $\theta_{K/k,S}$. □

Remarque. — Dans le cas où l'on a égalité entre m_G et $|D(G)|$, le postulat sur le dénominateur est optimal, au sens où l'on obtient exactement le dénominateur des éléments de Brumer-Stickelberger associés à l'extension K^{ab} ; ceci bien entendu à condition que les termes associés à K^{ab} soient non nuls, faute de quoi le facteur m_G est superflu.

En particulier, dans le cas où l'indice premier p est égal à 2, les calculs précédents démontrent que m_G est égal à $|D(G)|$ si ce cardinal est pair, et $2|D(G)|$ sinon, et le dénominateur conjecturé est ainsi presque optimal.

Étant donné la forme particulière de l'élément de Brumer, une tentation naturelle serait de vouloir prendre comme dénominateur de $\theta_{K/k,S}$ le cardinal de $D(G)$, qui vaut bien 1 lorsque le groupe G est abélien. Cependant, nous verrons au chapitre suivant des exemples de groupe de Galois isomorphe à $SL_2(\mathbb{F}_3)$, pour lesquels le groupe dérivé est isomorphe au groupe des quaternions, donc d'ordre 8, alors que le dénominateur de $\theta_{K/k,S}$ est 3. Ceci laisse à penser que certains facteurs de m_G ne provenant pas de $|D(G)|$ jouent un rôle important.

Nous allons voir dans la section suivante que des simplifications se produisent lorsque le sous-groupe H est de cardinal impair.

4.3. Cas particulier où H est de cardinal impair

Dans le cas où le cardinal de H est impair, le corps fixé par H, K^H, ne peut pas être totalement réel (chaque plongement réel de K^H dans $\mathbb{C}$ donnant lieu à $\frac{[K:K^H]}{2}$ couples de plongements complexes conjugués). D'après les propriétés 1.3 de l'élément de Brumer-Stickelberger, ceci implique que les éléments $\theta_{K/K^H,S_H}$ et $\theta_{K^{ab}/K^H,S_H}$ sont nuls. L'élément de Brumer s'écrit alors simplement

$$\theta_{K/k,S} = \frac{1}{|D(G)|}\theta_{K^{ab}/k,S}N_{K/K^{ab}}.$$

Les difficultés rencontrées précédemment pour démontrer la validité complète du postulat concernant le dénominateur de l'élément de Brumer proviennent du terme $\theta_{K/K^H,S_H}$. Ce terme ayant disparu dans le cas $|H|$ impair, nous obtenons naturellement le résultat suivant.

Corollaire 4.11. — *Dans le cas où $|H|$ est impair, le postulat concernant l'élément de Brumer est vérifié.*

Démonstration. — La preuve est immédiate en reprenant la démonstration du corollaire 4.10 et en considérant cette fois tous les idéaux premiers $\mathfrak{P}$ de $\mathcal{T}$ sans restriction sur leur morphisme de Frobénius. L'élément $(\sigma_{\mathfrak{P}|_{K^{ab}}} - \mathcal{N}(\mathfrak{p}))$ appartient encore à $\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K^{ab}/k)]}(\mu(K^{ab}))$ et la proposition 1.2 permet de nouveau de conclure que $m_G(\sigma_{\mathfrak{P}} - \mathcal{N}(\mathfrak{p}))\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$. □

On peut à présent démontrer la conjecture de Brumer-Stark non abélienne, sous la condition que la conjecture abélienne associée à l'extension K^{ab}/k soit vraie.

Proposition 4.12. — *Si $BS(K^{ab}/k, S)$ est vraie, alors la conjecture non abélienne $BS_{non\ ab}(K/k, S)$ est aussi vraie.*

Démonstration. — On suppose la conjecture $BS(K^{ab}/k,S)$ vraie. Soit $\mathcal{T}_{ab}$ l'ensemble des idéaux premiers de K^{ab} vérifiant l'assertion (iii) de la proposition 1.5. Soit $\mathfrak{P}$ un idéal premier de K au-dessus d'un élément de $\mathcal{T}_{ab}$. On considère un idéal fractionnaire non nul $\mathfrak{a}$ de K. On a

$$\begin{aligned}\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta_{K/k,S}} &= \mathfrak{a}^{\frac{m_G}{|D(G)|}(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S}N_{K/K^{ab}}}\\ &= \left(\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{\frac{m_G}{|D(G)|}}\right)^{(\sigma_{\mathcal{P}_{ab}}-\mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S}}\mathcal{O}_K,\end{aligned}$$

où $\mathcal{P}_{ab}$ désigne l'idéal premier de K^{ab} au-dessous de $\mathfrak{P}$. Puisque l'idéal $\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{\frac{m_G}{|D(G)|}}$ est un idéal fractionnaire de K^{ab}, il existe alors une anti-unité $\alpha_{\mathcal{P}_{ab}}$ de K^{ab} vérifiant $\left(\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{\frac{m_G}{|D(G)|}}\right)^{(\sigma_{\mathcal{P}_{ab}}-\mathcal{N}(\mathfrak{p}))\theta_{K^{ab}/k,S}} = \alpha_{\mathcal{P}_{ab}}\mathcal{O}_{K^{ab}}$, et $\alpha_{\mathcal{P}_{ab}} \equiv 1 \mod^*(\mathfrak{p}\mathcal{O}_{K^{ab}})$. Par suite, on obtient

$$\mathfrak{a}^{m_G(\sigma_{\mathfrak{P}}-\mathcal{N}(\mathfrak{p}))\theta_{K/k,S}} = \alpha_{\mathcal{P}_{ab}}\mathcal{O}_K.$$

Soit $\mathfrak{Q}$ un idéal premier de K au-dessus de $\mathfrak{p}$ tel que $\sigma_{\mathfrak{Q}} = \sigma_{\mathfrak{P}}$. La condition de congruence s'obtient en remarquant que

$$v_{\mathfrak{Q}}(\alpha_{\mathcal{P}_{ab}}-1) = v_{\mathcal{Q}_{ab}}(\alpha_{\mathcal{P}_{ab}}-1)e(\mathfrak{Q}/\mathcal{Q}_{ab}) = v_{\mathcal{Q}_{ab}}(\alpha_{\mathcal{P}_{ab}}-1) \geq v_{\mathcal{Q}_{ab}}(\mathfrak{p}\mathcal{O}_{K^{ab}}) = 1,$$

où $\mathcal{Q}_{ab} = \mathfrak{Q}\cap\mathcal{O}_{K^{ab}}$. Par conséquent $\alpha_{\mathcal{P}_{ab}} \equiv 1 \mod^*(\mathfrak{Q})$ et $BS_{\text{non ab}}(K/k,S)$ est vraie. □

Corollaire 4.13. — *Si le cardinal du groupe dérivé de G est premier avec w_K, la validité de $BS_{non\ ab}(K/k,S)$ équivaut à celle de $BS(K^{ab}/k,S)$.*

Démonstration. — Puisque les groupes $\mu(K)$ et $\mu(K^{ab})$ sont égaux, la condition $|D(G)|$ et w_K sont premiers entre eux entraîne la véracité du changement d'extension appliqué à K^{ab}. Ainsi la conjecture $BS_{\text{non ab}}(K/k,S)$ implique $BS(K^{ab}/k,S)$. La réciproque étant donnée par la proposition 4.12, ceci conclut la preuve. □

Corollaire 4.14. — *Si* $\mathrm{Gal}(K/k)$ *est isomorphe au groupe diédral à $2n$ éléments, avec n impair, la conjecture $BS_{non\ ab}(K/k,S)$ est vraie quel que soit l'ensemble S considéré.*

Démonstration. — C'est une application directe de la proposition 4.12 en remarquant que le groupe dérivé du groupe diédral est le sous-groupe engendré par un élément d'ordre n. Il est donc abélien, d'indice 2, et par conséquent distingué. De plus, l'extension K^{ab}/k est quadratique donc la conjecture de Brumer-Stark est vraie pour cette extension. □

4.4. Un résultat d'abélianité dans le cas où H est de cardinal pair

Sous la condition que la conjecture de Brumer-Stark abélienne associée à des sous-extensions convenables de K/k soit vraie, la forme de l'élément de Brumer donnée par le théorème 4.2 permet de démontrer la partie "Brumer" de la conjecture non abélienne concernant l'annulation du groupe des classes de K. Elle implique aussi un certain résultat d'abélianité, qui correspond à une partie de la condition de centralité stipulée dans $BS_{\text{non ab}}(K/k,S)$. Nous allons voir que sous

d'autres hypothèses, cela entraîne la véracité de la conjecture de Brumer-Stark non abélienne en totalité.

4.4.1. Énoncé et démonstration du résultat. — On rappelle que l'on suppose que k est un corps totalement réel, K totalement complexe, et que le groupe de Galois $G = \mathrm{Gal}(K/k)$ contient un sous-groupe abélien distingué H d'indice premier. Le cas impair ayant été traité précédemment, on considère de plus dans cette partie que le cardinal de H est pair.

Théorème 4.15. — *Supposons les conjectures abéliennes $BS(K^{ab}/k, S)$ ainsi que $BS(K/K^H, S_H)$ vraies. Pour tout idéal fractionnaire non nul $\mathfrak{a}$ de K, il existe $\alpha \in K^\circ$ vérifiant $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} = \alpha \mathcal{O}_K$, et si l'on prend γ une racine w_K-ième de α, l'extension $K(\gamma)$ est abélienne sur K^H.*

Démonstration. — On suppose donc la validité des conjectures $BS(K^{ab}/k, S)$ et $BS(K/K^H, S_H)$. L'extension K^{ab}/K^H étant une sous-extension de K/K^H, les propriétés de changement d'extension de la conjecture de Brumer-Stark abélienne impliquent en particulier que la conjecture $BS(K^{ab}/K^H, S_H)$ est vraie. On note w_{ab} le nombre de racines de l'unité de K^{ab}. On rappelle que w_{ab} est égal à w_K, cependant dans l'optique d'utiliser les résultats abéliens associés au corps K^{ab}, on garde à certains endroits la notation w_{ab}. On considère un idéal fractionnaire non nul $\mathfrak{a}$ de K. On ne cherche pas à démontrer directement le résultat par une propriété équivalente donnée par la proposition 3.1 mais plutôt à exploiter les données des conjectures abéliennes, ce qui fournit aussi des informations sur le générateur de l'idéal principal obtenu. On utilise la forme de $\theta_{K/k,S}$ donnée par le théorème 4.2 :

$$\begin{aligned}
\mathfrak{a}^{m_G w_K \theta_{K/k,S}} &= \mathfrak{a}^{\frac{m_G}{|D(G)|} w_K \left(\theta_{K^{ab}/k,S} N_{K/K^{ab}} - \theta_{K^{ab}/K^H,S_H} N_{K/K^{ab}}\right) + m_G w_K \theta_{K/K^H,S_H}} \\
&= \mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{\frac{m_G}{|D(G)|} w_K \theta_{K^{ab}/k,S}} \cdot \mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{-\frac{m_G}{|D(G)|} w_K \theta_{K^{ab}/K^H,S_H}} \\
&\quad \cdot \mathfrak{a}^{m_G w_K \theta_{K/K^H,S_H}} \\
&= \left(\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{w_{ab}\theta_{K^{ab}/k,S}}\right)^{\frac{m_G}{|D(G)|}} \\
&\quad \cdot \left(\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{w_{ab}\theta_{K^{ab}/K^H,S_H}}\right)^{-\frac{m_G}{|D(G)|}} \left(\mathfrak{a}^{w_K \theta_{K/K^H,S_H}}\right)^{m_G}
\end{aligned}$$

où $\mathcal{N}_{K/K^{ab}}$ désigne la norme relative associée à l'extension K/K^{ab}. L'idéal $\mathcal{N}_{K/K^{ab}}(\mathfrak{a})$ est en particulier un idéal fractionnaire non nul de K^{ab}. Puisque la conjecture de Brumer-Stark abélienne est supposée vraie pour les différentes extensions intervenant, il existe alors des anti-unités α_{ab}, β_{ab} de K^{ab}, et une anti-unité α_H de K vérifiant

$$\begin{aligned}
\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{w_{ab}\theta_{K^{ab}/k,S}} &= \alpha_{ab}\mathcal{O}_{K^{ab}}, \\
\mathcal{N}_{K/K^{ab}}(\mathfrak{a})^{w_{ab}\theta_{K^{ab}/K^H,S_H}} &= \beta_{ab}\mathcal{O}_{K^{ab}}, \\
\text{et enfin} \qquad \mathfrak{a}^{w_K\theta_{K/K^H,S_H}} &= \alpha_H \mathcal{O}_K.
\end{aligned}$$

De plus, si l'on note γ_{ab} (respectivement δ_{ab}) une racine w_{ab}-ième de α_{ab} (resp. β_{ab}), et γ_H une racine w_K-ième de α_H, les extensions $K^{ab}(\gamma_{ab})/k$, $K^{ab}(\delta_{ab})/K^H$ et

$K(\gamma_H)/K^H$ sont abéliennes. En réinjectant ceci dans l'expression de $\mathfrak{a}^{m_G w_K \theta_{K/k,S}}$, on trouve

$$\begin{aligned}\mathfrak{a}^{m_G w_K \theta_{K/k,S}} &= {\alpha_{ab}}^{\frac{m_G}{|D(G)|}} {\beta_{ab}}^{-\frac{m_G}{|D(G)|}} {\alpha_H}^{m_G} \mathcal{O}_K \\ &= \left(\alpha_{ab}\beta_{ab}^{-1}\right)^{\frac{m_G}{|D(G)|}} {\alpha_H}^{m_G} \mathcal{O}_K,\end{aligned}$$

ce qui démontre que $m_G w_K \theta_{K/k,S}$ annule le groupe des classes de K. Posons alors $\alpha = \left(\alpha_{ab}\beta_{ab}^{-1}\right)^{\frac{m_G}{|D(G)|}} {\alpha_H}^{m_G}$ de sorte que l'idéal principal $\mathfrak{a}^{m_G w_K \theta_{K/k,S}}$ de K soit engendré par α. Les éléments α_{ab} et β_{ab} étant des anti-unités de K^{ab}, ce sont aussi des anti-unités de K, tout comme α_H, ce qui entraîne l'appartenance de α à K°.

Soit γ une racine w_K-ième de α. Démontrons que l'extension $K(\gamma)$ est abélienne sur K^H. Pour cela, nous utilisons le critère d'abélianité de Tate, rappelé à la proposition 3.11. Soient $\{h_1, \ldots, h_t\}$ un ensemble de générateurs de H. Il existe un système d'entier $\{n_1, \ldots, n_t\}$ vérifiant pour toute racine de l'unité ζ de K, $\zeta^{h_i - n_i} = 1$, ceci quel que soit i entre 1 et t. L'extension $K(\gamma)$ est abélienne sur K^H si et seulement s'il existe des élements $\alpha_1, \ldots, \alpha_t$ de $K^\times$ vérifiant

$$\alpha^{h_i - n_i} = \alpha_i^{w_K} \text{ et } \alpha_i^{h_j - n_j} = \alpha_j^{h_i - n_i}, \text{ pour tous } 1 \leq i, j \leq t.$$

Puisque l'extension $K^{ab}(\gamma_{ab})$ est abélienne sur k, elle l'est en particulier sur K^H. De plus, le groupe de Galois de K^{ab}/K^H est un groupe abélien engendré par les restrictions des éléments $h_1, \ldots, h_t$, que l'on note $\overline{h_1}, \ldots, \overline{h_t}$. Nous allons chercher à utiliser le critère d'abélianité puisque γ_{ab} est une racine w_{ab}-ième d'un élément de K^{ab}. Il reste à expliquer comment choisir les entiers m_i vérifiant $\xi^{\overline{h_i} - m_i} = 1$ pour toute racine de l'unité ξ appartenant à K^{ab}. Puisque le groupe des racines de l'unité de K^{ab} est égal au groupe des racines de l'unité de K, on a l'égalité $\xi^{\overline{h_i} - n_i} = \xi^{h_i - n_i} = 1$ pour toute racine ξ dans $\mu(K^{ab})$. On peut donc choisir les entiers m_i égaux aux n_i définis précédemment. Le critère de Tate implique alors l'existence d'un système $\{\alpha_{ab,1}, \ldots, \alpha_{ab,t}\}$ d'éléments non nuls de K^{ab} tels que ${\alpha_{ab}}^{\overline{h_i} - n_i} = {\alpha_{ab,i}}^{w_{ab}}$ et ${\alpha_{ab,i}}^{\overline{h_j} - n_j} = {\alpha_{ab,j}}^{\overline{h_i} - n_i}$ pour tous $1 \leq i, j \leq t$. En adaptant les notations, on obtient un système similaire $\{\beta_{ab,1}, \ldots, \beta_{ab,t}\}$ en remplaçant l'élément α_{ab} par β_{ab}. Enfin, puisque l'extension $K(\gamma_H)$ est abélienne sur K^H, il existe aussi des éléments non nuls de K, notés $\alpha_{H,1}, \ldots, \alpha_{H,t}$ vérifiant les propriétés ${\alpha_H}^{h_i - n_i} = {\alpha_{H,i}}^{w_K}$ et ${\alpha_{H,i}}^{h_j - n_j} = {\alpha_{H,j}}^{h_i - n_i}$ pour tous $1 \leq i, j \leq t$. En regroupant ces différentes informations ensemble, on obtient finalement pour tout entier i compris entre 1 et t

$$\begin{aligned}\alpha^{h_i - n_i} &= \left(\left(\alpha_{ab}\beta_{ab}^{-1}\right)^{\frac{m_G}{|D(G)|}} {\alpha_H}^{m_G}\right)^{h_i - n_i} \\ &= \left({\alpha_{ab}}^{h_i - n_i} ({\beta_{ab}}^{h_i - n_i})^{-1}\right)^{\frac{m_G}{|D(G)|}} \left({\alpha_H}^{h_i - n_i}\right)^{m_G} \\ &= \left({\alpha_{ab}}^{\overline{h_i} - n_i} ({\beta_{ab}}^{\overline{h_i} - n_i})^{-1}\right)^{\frac{m_G}{|D(G)|}} \left({\alpha_H}^{h_i - n_i}\right)^{m_G} \\ &= \left({\alpha_{ab,i}}^{w_{ab}} {\beta_{ab,i}}^{-w_{ab}}\right)^{\frac{m_G}{|D(G)|}} \left({\alpha_{H,i}}^{w_K}\right)^{m_G} \\ &= \left(\left(\alpha_{ab,i}\beta_{ab,i}^{-1}\right)^{\frac{m_G}{D(G)}} {\alpha_{H,i}}^{m_G}\right)^{w_K}.\end{aligned}$$

Poser $\alpha_i = (\alpha_{ab,i}\beta_{ab,i}^{-1})^{\frac{m_G}{D(G)}}{\alpha_{H,i}}^{m_G}$ donne alors des éléments α_i vérifiant la première partie des propriétés voulues. Le reste s'obtient facilement grâce aux propriétés vérifiées par les éléments intervenant. Soient i, j deux entiers compris entre 1 et t. On a les identités

$$\begin{aligned}
{\alpha_i}^{h_j-n_j} &= \left((\alpha_{ab,i}\beta_{ab,i}^{-1})^{\frac{m_G}{D(G)}}{\alpha_{H,i}}^{m_G}\right)^{h_j-n_j} \\
&= \left({\alpha_{ab,i}}^{\overline{h_j}-n_j}(\beta_{ab,i}^{\overline{h_j}-n_j})^{-1}\right)^{\frac{m_G}{D(G)}}({\alpha_{H,i}}^{h_j-n_j})^{m_G} \\
&= \left({\alpha_{ab,j}}^{\overline{h_i}-n_i}(\beta_{ab,j}^{\overline{h_i}-n_i})^{-1}\right)^{\frac{m_G}{D(G)}}({\alpha_{H,j}}^{h_i-n_i})^{m_G} \\
&= \left({\alpha_{ab,j}}^{h_i-n_i}({\beta_{ab,j}}^{h_i-n_i})^{-1}\right)^{\frac{m_G}{D(G)}}({\alpha_{H,j}}^{h_i-n_i})^{m_G} \\
&= {\alpha_j}^{h_i-n_i}
\end{aligned}$$

ce qui achève la démonstration. □

Remarque. — Le critère d'abélianité de Tate nous permet de voir que la condition d'abélianité de l'extension $K(\gamma)$ sur la sous-extension abélienne K^H de K/k ne dépend pas du choix du générateur α. En effet, si β est une autre anti-unité de K engendrant le même idéal principal sur K que α, alors α et β diffèrent d'une racine de l'unité de K près. Il existe donc ζ dans $\mu(K)$ vérifiant l'égalité $\beta = \zeta\alpha$. On suppose que α vérifie la condition d'abélianité. On a, en gardant les notations de la démonstration précédente, $\beta^{h_i-n_i} = (\zeta\alpha)^{h_i-n_i} = \zeta^{h_i-n_i}\alpha^{h_i-n_i} = \alpha_i^{w_K}$ puisque $h_i - n_i$ annule $\mu(K)$. En définitive, l'élément β vérifie lui aussi le critère d'abélianité.

4.4.2. Cas impliquant la validité de $BS_{\text{non ab}}(K/k, S)$. — Le théorème 4.15 fournit la démonstration d'une partie de la condition de centralité de $BS_{\text{non ab}}(K/k, S)$, à savoir la condition d'abélianité concernant le sous-groupe H d'indice premier. Il permet dans des cas particuliers d'obtenir la véracité de $BS_{\text{non ab}}(K/k, S)$.

Tout d'abord, on peut remarquer que sous l'hypothèse que tout sous-groupe abélien de G est inclus dans un sous-groupe abélien distingué d'indice premier, le corollaire 4.10 appliqué à chacun de ces sous-groupes distingués implique directement la vérification complète du postulat concernant l'élément de Brumer. En fait, sous cette hypothèse on peut même obtenir la validité de $BS_{\text{non ab}}(K/k, S)$, à condition que la conjecture de Brumer-Stark abélienne soit vraie pour certaines sous-extensions de K/k.

Corollaire 4.16. — *On suppose que les sous-groupes abéliens maximaux de G, que l'on notera $H_1, \ldots, H_n$, sont distingués et d'indice premier. Si les conjectures abéliennes $BS(K/K^{H_i}, S_{H_i})$ pour i dans $\{1, \ldots, n\}$ ainsi que $BS(K^{ab}/k, S)$ sont vraies, alors la conjecture non abélienne $BS_{non\ ab}(K/k, S)$ est vérifiée.*

Démonstration. — C'est une application du théorème 4.15 et de la remarque qui le suit. Soit $\mathfrak{a}$ un idéal fractionnaire non nul de K. Soit i appartenant à $\{1, \ldots, n\}$.

Il existe donc $\alpha_i \in K^\circ$ tel que $\mathfrak{a}^{m_G w_K \theta_{K/k,S}} = \alpha_i \mathcal{O}_K$, et si γ_i est un élément qui élevé à la puissance w_K donne α_i, l'extension $K(\gamma_i)$ est abélienne sur K^{H_i}. Puisque les éléments α_i engendrent tous le même idéal sur K, si la condition d'abélianité sur l'un des K^{H_j} est vérifiée pour l'un d'entre eux, elle est vérifiée pour tous ces éléments. En particulier, on obtient par exemple que $K(\gamma_1)$ est abélienne sur K^{H_j} pour tout j dans $\{1, \ldots, n\}$. Si l'on prend alors un sous-groupe abélien H' de G, il existe un sous-groupe H_j le contenant. Puisque $K(\gamma_1)/K^{H'}$ est une sous-extension de $K(\gamma_1)/K^{H_j}$, elle est bien abélienne, ce qui démontre l'assertion (2) du théorème 3.6 et démontre la validité de $BS_{\text{non ab}}(K/k, S)$ dans ce cas. □

Remarque. — Les propriétés de changement d'extension permettent de s'apercevoir que la condition sur la validité de la conjecture de Brumer-Stark abélienne des sous-extensions associées aux sous-groupes abéliens maximaux H_i est équivalente à la véracité de la conjecture abélienne associée à toute sous-extension abélienne de K/k.

Une question naturelle est de se demander s'il existe beaucoup de groupes vérifiant la condition du corollaire 4.16. Le lemme suivant répond en partie à cette interrogation.

Lemme 4.17. — *Soit G_1 un groupe fini dont les sous-groupes abéliens maximaux sont distingués d'indice premier. Soit G_2 un groupe abélien fini. Alors les sous-groupes abéliens maximaux du produit direct $G = G_1 \times G_2$ sont aussi distingués et d'indice premier.*

Démonstration. — Notons $H_1, \ldots, H_n$ les sous-groupes abéliens maximaux de G_1. Soit H' un sous-groupe abélien de $G = G_1 \times G_2$. Notons H'_1 la projection de H' sur G_1. La projection sur G_1 étant un morphisme de groupes, l'image de tout sous-groupe abélien de G par cette projection est un sous-groupe abélien de G_1. L'ensemble H'_1 est donc un sous-groupe abélien de G_1.

Par suite, il existe un entier $i \in \{1, \ldots, n\}$ tel que H'_1 est inclus dans H_i. Or, H' s'injecte de manière naturelle dans $H'_1 \times G_2$, ce qui implique que l'on dispose de l'inclusion $H' \subset H_i \times G_2$. Ainsi, tout sous-groupe abélien de G est inclus dans l'un des $H_1 \times G_2, \ldots, H_n \times G_2$. Ces groupes étant par définition des sous-groupes abéliens de G, on en déduit que ce sont les sous-groupes abéliens maximaux de G.

Soit i appartenant à $\{1, \ldots, n\}$. Comme H_i est distingué dans G_1, le groupe $H_i \times G_2$ est distingué dans G. En effet, on a pour tout $(g_1, g_2) \in G$

$$(g_1, g_2) \cdot (H_i \times G_2) \cdot (g_1, g_2)^{-1} = (g_1 H_i g_1^{-1}) \times (g_2 G_2 g_2^{-1}) = H_i \times G_2.$$

L'indice de $H_i \times G_2$ dans $G_1 \times G_2$ est égal à $\dfrac{|G_1 \times G_2|}{|H_i \times G_2|} = (G_1 : H_i)$ et est donc premier, ce qui termine la démonstration. □

Remarque. — À partir d'un groupe non abélien vérifiant la condition du corollaire 4.16, il est donc possible de créer une famille infinie de groupes vérifiant

cette condition en prenant le produit cartésien de ce groupe avec n'importe quel groupe abélien fini.

Application aux groupes non abéliens d'ordre 8 : on s'intéresse au cas où G est non commutatif d'ordre 8. Puisqu'il n'y a que deux tels groupes à isomorphisme près, G est isomorphe soit au groupe des quaternions, soit au groupe diédral à 8 éléments. On considère tout d'abord le cas où G est isomorphe au groupe des quaternions Q_8, que l'on peut présenter sous la forme $Q_8 = \langle \tau, i, j, k \mid i^2 = j^2 = k^2 = ijk = \tau \text{ et } \tau^2 = 1 \rangle$. Hormis le sous-groupe trivial, Q_8 possède un unique sous-groupe d'ordre 2, le groupe engendré par l'unique conjugaison complexe τ, et trois sous-groupes abéliens d'ordre 4, que l'on notera $H_1 = \langle i \rangle, H_2 = \langle j \rangle$ et $H_3 = \langle k \rangle$. Les sous-groupes H_1, H_2 et H_3 sont d'indice 2, donc distingués dans G. De plus, l'extension K/K^{H_l} pour l entre 1 et 3 est une extension abélienne de degré 4, qui est sous-extension de l'extension galoisienne mais non abélienne K/k de degré 8. D'après [**Tat81**], la conjecture de Brumer-Stark abélienne a été démontrée dans ce cas, et $BS(K/K^{H_l}, S)$ est donc vérifiée pour tout l. Il reste à savoir si $BS(K^{ab}/k, S)$ est aussi vraie dans ce cas. Le groupe dérivé de Q_8 est égal au sous-groupe engendré par τ, ainsi K^{ab} est égal au sous-corps totalement réel maximal de K, et $BS(K^{ab}/k, S)$ est trivialement vérifiée. Le corollaire précédent entraîne donc la validité de $BS_{\text{non ab}}(K/k, S)$ quand G est isomorphe à Q_8, ceci quel que soit l'ensemble de places S considéré.

Le même type de phénomène se produit lorsque le groupe G est isomorphe au groupe diédral à 8 éléments, D_4, dont une présentation est $D_4 = \langle \sigma, \tau \mid \sigma^2 = \tau^4 = 1, \sigma\tau\sigma = \tau^{-1} \rangle$. L'unique élément non trivial du centre de G est τ^2 qui engendre le groupe dérivé de D_4. Le groupe de Galois de l'extension K^{ab}/k est alors isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et $BS(K^{ab}/k, S)$ est vraie d'après le théorème 1.8. Les cinq sous-groupes d'ordre 2 sont inclus dans les sous-groupes abéliens d'ordre 4, $H = \langle \tau \rangle$, $H_\sigma = \langle \sigma, \tau^2 \rangle$ et $H_{\sigma\tau} = \langle \sigma\tau, \tau^2 \rangle$. Les extensions intervenant sont alors, comme pour les quaternions, des sous-extensions de degré 4 d'une extension galoisienne non abélienne de degré 8, ce qui entraîne la validité des conjectures abéliennes de Brumer-Stark nécessaires à l'application du corollaire 4.16 et démontre la conjecture non abélienne associée à G.

En conclusion, on obtient le résultat suivant.

Corollaire 4.18. — *Si K/k est une extension galoisienne de corps de nombres, vérifiant k totalement réel et K totalement complexe, de groupe de Galois non abélien d'ordre* 8*, la conjecture non abélienne $BS_{non\ ab}(K/k, S)$ est vraie quel que soit l'ensemble S choisi.*

Dans le cas des p-groupes d'ordre p^n, où p est un nombre premier, tout sous-groupe maximal est d'ordre p^{n-1} et est distingué. Ainsi si les sous-groupes maximaux sont abéliens, on est donc dans le cadre du corollaire 4.16. Puisque l'on a supposé K totalement complexe et k totalement réel, le cardinal de G est pair et les seuls p-groupes qui nous intéresseront sont les 2-groupes. Le cas $n = 3$ ayant

été traité, on peut se demander ce qu'il se passe dans le cas $n = 4$. Contrairement au cas $n = 3$, les groupes qui interviennent ne vérifient pas tous les hypothèses du corollaire 4.16. Si l'on prend par exemple le cas où G est isomorphe au groupe diédral à 16 éléments, $D_8 = \langle \sigma, \tau \mid \sigma^2 = \tau^8 = 1, \sigma\tau\sigma = \tau^{-1} \rangle$, l'étude des sous-groupes de G montre que les sous groupes maximaux, qui sont donc d'ordre 8, sont $\langle \tau \rangle$, $\langle \sigma, \tau^2 \rangle$, $\langle \sigma\tau, \tau^2 \rangle$ et $\langle \sigma\tau^2, \tau^2 \rangle$, dont seul le premier est abélien. Au contraire, dans le cas où G est isomorphe au groupe d'ordre 16, de présentation $\langle s, t \mid s^8 = t^2 = 1, st = ts^5 \rangle$, tous les éléments sont de la forme $s^l t^m$ avec $l \in \{0, \ldots, 7\}$ et $m \in \{0, 1\}$, et le centre est $\{1, s^2, s^4, s^6\}$. Le diagramme des sous-groupes est le suivant.

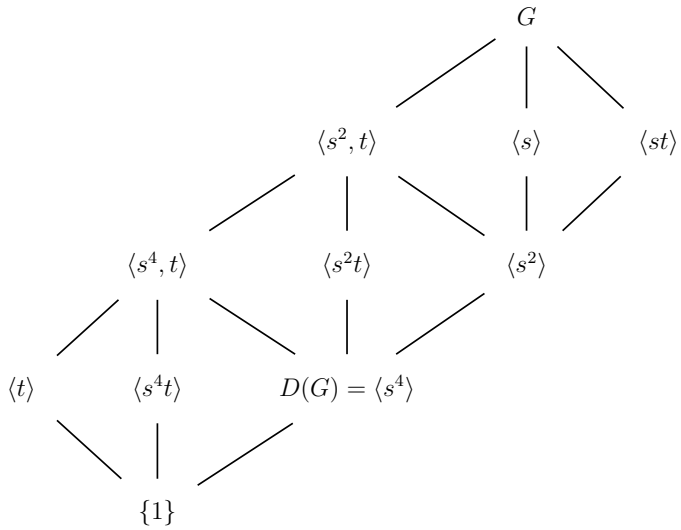


FIGURE 4.1. Diagramme des sous-groupes du groupe d'ordre 16 de présentation $\langle s, t \mid s^8 = t^2 = 1, st = ts^5 \rangle$

Les sous-groupes maximaux de G sont tous abéliens. Notons $H_1 = \langle s^2, t \rangle$, $H_2 = \langle s \rangle$ et $H_3 = \langle st \rangle$ les sous-groupes maximaux de G, $K^i = K^{H_i}$ les sous-corps fixés respectifs et S_i l'ensemble des places de K^i au-dessus des places de S.

Corollaire 4.19. — *Avec les notations précédentes, si les conjectures abéliennes $BS(K/K^i, S_i)$ pour i entre 1 et 3 ainsi que $BS(K^{ab}/k, S)$ sont vraies, alors $BS_{non\ ab}(K/k, S)$ est vérifiée.*

CHAPITRE 5

QUELQUES VÉRIFICATIONS NUMÉRIQUES

À l'aide du logiciel PARI-GP ([**The08**]), nous testons notre conjecture de Brumer-Stark non abélienne pour quelques extensions de groupe de Galois particulier. Tous les calculs ont été réalisés en prenant pour S l'ensemble minimal, *i.e* en considérant exactement l'ensemble des places infinies de k et des places finies qui se ramifient dans K.

5.1. Décomposition rationnelle de $Z(\mathbb{Q}[G])$

Soit χ un caractère irréductible de G. Pour un élément g de G, le nombre complexe $\chi(g)$ est un entier algébrique. Si l'on note $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$, le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur $\widehat{G}$ par

$$\sigma \cdot \chi(g) = \sigma(\chi(g)) \text{ pour } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Notons $\mathfrak{X}$ l'ensemble des classes de $\widehat{G}/\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Pour une classe X dans $\mathfrak{X}$, on définit l'élément e_X comme la somme des idempotents associés aux caractères χ dans X. On a alors

$$\begin{aligned} e_X &= \sum_{\chi\in X} e_\chi = \sum_{\chi\in X} \frac{\chi(1)}{|G|} \sum_{g\in G} \chi(g)g^{-1} = \frac{\chi(1)}{|G|} \sum_{g\in G}\sum_{\psi\in X} \psi(g)g^{-1} \\ &= \frac{\chi(1)}{|G|} \sum_{g\in G} \mathrm{Tr}_{\mathbb{Q}(\chi)/\mathbb{Q}}(\chi(g))g^{-1}, \end{aligned}$$

pour un caractère χ quelconque dans X. En particulier, e_X est dans le centre de $\mathbb{Q}[G]$. Grâce aux relations d'orthogonalité vérifiées par les idempotents e_χ, on démontre les identités suivantes :

$$e_X \cdot e_Y = \delta_{X,Y} e_X \quad \text{et} \quad \sum_{X\in\mathfrak{X}} e_X = 1,$$

où $\delta_{X,Y}$ désigne le symbole de Kronecker de X et Y. Ceci nous permet ce décomposer $\mathbb{Q}[G]$ sous la forme

$$\mathbb{Q}[G] = \bigoplus_{X\in\mathfrak{X}} \mathbb{Q}[G]\cdot e_X.$$

On appelle X-composante de $\theta_{K/k,S}$ l'élément $\theta_{K/k,S} \cdot e_X$ aussi égal à

$$\theta_{K/k,S} \cdot e_X = \frac{\chi(1)}{|G|} \sum_{g \in G} \mathrm{Tr}_{\mathbb{Q}(\chi)/\mathbb{Q}}(L_{K/k,S}(0,\chi)\chi(g))g$$

pour un caractère χ fixé dans X. Si l'élément $m_G w_K \theta_{K/k,S} \cdot e_X$ appartient à $\mathbb{Z}[G]$ pour toute classe X, on peut parler de X-composante de la conjecture $BS_{\text{non ab}}(K/k,S)$, obtenue en remplaçant l'élément de Brumer par sa X-composante. La véracité des X-composantes de la conjecture de Brumer-Stark non abélienne entraîne alors la validité de $BS_{\text{non ab}}(K/k,S)$, ce qui nous permet de tester la conjecture composante par composante. Toutefois il n'y a pas d'indications évidentes qu'il puisse y avoir équivalence.

5.2. Cas où Gal(K/k) est isomorphe à $SL_2(\mathbb{F}_3)$

On considère une extension galoisienne finie de corps de nombres K/k, de groupe de Galois G isomorphe à $SL_2(\mathbb{F}_3)$. On remarque que ce groupe n'appartient pas à la famille des groupes considérés dans le chapitre précédent. On suppose de plus que k est totalement réel et K est un corps CM.

Pour ce groupe de Galois, la décomposition de Brauer des caractères irréductibles n'a pas une forme aussi simple que dans le cas où le groupe possède un sous-groupe abélien distingué d'indice premier. L'écriture de l'élément de Brumer associé à de telles extensions fait apparaître des quotients de fonctions L de Hecke qui empêchent une approche similaire de la conjecture non abélienne. Nous ne disposons pas pour l'instant de résultats théoriques pour ces extensions, d'où l'importance d'effectuer dans ce cas des tests numériques.

5.2.1. Étude théorique de l'élément de Brumer. — Le groupe $SL_2(\mathbb{F}_3)$ est composé des matrices de taille 2 à coefficients dans $\mathbb{F}_3$ de déterminant 1. Notons $\sigma = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ d'ordre 6 et $\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ d'ordre 4. Le groupe $SL_2(\mathbb{F}_3)$ est engendré par σ et ρ. L'unique conjugaison complexe est donnée par le seul élément d'ordre 2 de $SL_2(\mathbb{F}_3)$, noté τ, vérifiant $\tau = \sigma^3 = \rho^2$, et le centre de $SL_2(\mathbb{F}_3)$ est réduit à $\langle\tau\rangle$. Le groupe G possède sept classes de conjugaison, à savoir deux classes possédant un seul élément , C_{Id} et C_τ, quatre classes de cardinal 4,

$$\begin{aligned} C_\sigma &= \left\{\sigma, \sigma^2\rho\sigma^2, \rho^{-1}\sigma, \sigma\rho^{-1}\right\}, \\ C_{\sigma^{-1}} &= \left\{\sigma^{-1}, \sigma^{-1}\rho, \rho\sigma^{-1}, \sigma\rho^{-1}\sigma\right\}, \\ C_{\sigma^2} &= \tau \cdot C_{\sigma^{-1}}, \\ C_{\sigma^{-2}} &= \tau \cdot C_\sigma, \end{aligned}$$

et une classe de cardinal 6 contenant tous les éléments d'ordre 4,

$$C_\rho = \left\{\rho, \rho^{-1}, \sigma^{-1}\rho\sigma, \sigma^{-1}\rho^{-1}\sigma, \sigma^{-2}\rho\sigma^2, \sigma^{-2}\rho^{-1}\sigma^2\right\}.$$

On remarque au passage que le ppcm des classes de conjugaison, m_G, est égal à 12. Par suite, le groupe G possède sept caractères irréductibles, trois de degré 1, que l'on note χ_0, χ_1, χ_2 (le caractère χ_0 désignant le caractère trivial de G),

trois de degré 2, notés ψ_1, ψ_2, ψ_3, et un de degré 3 désigné par φ. La table des caractères de G est donnée par le tableau 5.1, où ω est égal à $e^{\frac{2\sqrt{-1}\pi}{3}}$ (on désigne par $\sqrt{-1}$ une racine carrée fixée de -1, afin de rester cohérent avec les notations du chapitre précédent).

	C_{Id}	C_τ	C_σ	C_{σ^2}	$C_{\sigma^{-2}}$	$C_{\sigma^{-1}}$	C_ρ
χ_0	1	1	1	1	1	1	1
χ_1	1	1	ω	ω^2	ω	ω^2	1
χ_2	1	1	ω^2	ω	ω^2	ω	1
ψ_1	2	-2	1	-1	-1	1	0
ψ_2	2	-2	ω	$-\omega^2$	$-\omega$	ω^2	0
ψ_3	2	-2	ω^2	$-\omega$	$-\omega^2$	ω	0
φ	3	3	0	0	0	0	-1

TABLE 5.1. Table des caractères de $SL_2(\mathbb{F}_3)$

Notre but est d'expliciter l'élément de Brumer. Puisque le cardinal de S est supérieur ou égal à 2, la fonction L associée au caractère trivial en $s = 0$, $L_{K/k,S}(0, \chi_0)$, est nulle. De plus, les caractères χ_1, χ_2 et φ sont triviaux sur la conjugaison complexe τ. En utilisant la proposition 2.2 et le fait que pour toute place infinie v dans S, le groupe de décomposition D_w d'une place w au-dessus de v est égal à $\langle\tau\rangle$, on obtient pour chacun de ces trois caractères

$$r(\chi) = \sum_{v\in S} \dim V^{D_w} - \dim V^G = \sum_{v\in S} \dim V^{D_w} \geq 1$$

où l'on a noté V le sous-espace vectoriel de la représentation dont χ est le caractère. Ainsi l'élément de Brumer s'écrit simplement

$$\theta_{K/k,S} = \sum_{i=1}^{3} L_{K/k,S}(0, \psi_i) e_{\overline{\psi_i}}. \tag{5.2.1}$$

On s'intéresse à l'ordre d'annulation des fonctions L d'Artin associées aux caractères ψ_i. Notons ρ_i la représentation dont ψ_i est le caractère. Pour cela, on a besoin de l'expression des représentations ρ_i, détaillée dans la table suivante. On ne donne pas la valeur explicite de $\rho_i(g)$ mais seulement ses valeurs propres, ce qui est suffisant pour obtenir l'ordre d'annulation de la fonction L associée en $s = 0$. Le nombre ξ désigne le complexe $e^{\frac{2\sqrt{-1}\pi}{6}}$.

	C_{Id}	C_τ	C_σ	C_{σ^2}	$C_{\sigma^{-2}}$	$C_{\sigma^{-1}}$	C_ρ
ρ_1	$(1,1)$	$(-1,-1)$	(ξ, ξ^{-1})	(ω, ω^{-1})	(ω^{-1}, ω)	(ξ^{-1}, ξ)	$(\sqrt{-1}, -\sqrt{-1})$
ρ_2	$(1,1)$	$(-1,-1)$	$(-1, \xi)$	$(1, \omega)$	$(1, \omega^{-1})$	$(-1, \xi^{-1})$	$(\sqrt{-1}, -\sqrt{-1})$

TABLE 5.2. Valeurs propres des matrices des représentations ρ_i pour $i \in \{1, 2\}$

On remarque que $\psi_3 = \overline{\psi_2}$, ce qui entraîne l'égalité $L_{K/k,S}(0, \psi_3) = \overline{L_{K/k,S}(0, \psi_2)}$, et les ordres d'annulations de ψ_2 et ψ_3 sont égaux. De plus, $r(\psi_1)$ est égal à

$2|\{v \in S \mid D_w = \{I_2\}\}|$, et on constate que l'ordre $r(\psi_2)$ est supérieur ou égal à $r(\psi_1)$.

Trois cas se présentent alors :

Cas 1 : $r(\psi_1) \geq 1$ alors $\theta_{K/k,S} = 0$.

Cas 2 : $r(\psi_1) = 0$ et $r(\psi_2) \geq 1$, alors $\theta_{K/k,S} = L_{K/k,S}(0, \psi_1)e_{\overline{\psi_1}}$.

Cas 3 : $r(\psi_2) = 0$, alors $\theta_{K/k,S}$ est donné par la formule (5.2.1) où tous les termes sont non nuls.

Il nous reste à trouver la décomposition de Brauer des caractères ψ_i afin de ne faire apparaître que des fonctions L de Hecke dans l'expression de $\theta_{K/k,S}$. Cette décomposition n'étant pas unique, nous privilégions la forme la plus "simple" que l'on puisse obtenir. Notons H_4 le sous-groupe engendré par ρ et H_6 celui engendré par σ. En cherchant les caractères induits dans G par les caractères de ces deux sous-groupes, on trouve la décomposition

$$\begin{aligned}
\psi_1 &= \mathrm{Ind}_{H_4}^G(\Upsilon_1) - \mathrm{Ind}_{H_6}^G(\eta_3),\\
\psi_2 &= \mathrm{Ind}_{H_4}^G(\Upsilon_1) - \mathrm{Ind}_{H_6}^G(\eta_1),\\
\psi_3 &= \mathrm{Ind}_{H_4}^G(\Upsilon_1) - \mathrm{Ind}_{H_6}^G(\eta_5),
\end{aligned}$$

où pour $j \in \{0, \ldots, 3\}$, Υ_j est le caractère du groupe abélien H_4 défini par $\Upsilon_j(\rho) = \sqrt{-1}^j$, et pour $i \in \{0, \ldots, 5\}$, η_i est le caractère de H_6 défini par $\eta_i(\sigma) = \xi^i$, avec $\xi = e^{\frac{2\sqrt{-1}\pi}{6}}$. En remplaçant ceci dans l'expression (5.2.1) et en utilisant les propriétés (2.1.1) et (2.1.2) des fonctions L d'Artin, on obtient finalement le résultat suivant :

Proposition 5.1. — *Sous les notations précédentes, l'élément de Brumer s'écrit*

$$\theta_{K/k,S} = \frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_3)}e_{\overline{\psi_1}} + \frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_1)}e_{\overline{\psi_2}} + \frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_5)}e_{\overline{\psi_3}}$$

où K_i désigne le sous-corps de K fixé par H_i et S_i l'ensemble des places de K_i au-dessus de S.

Dans le cas où $r(\psi_1) = 0$, on peut obtenir l'expression explicite (au signe près) du terme $\dfrac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_3)}$. Pour cela, on utilise le fait que

$$\begin{aligned}
\zeta_{K,S}(s) &= \prod_{i=0}^{3} L_{K/K_4,S_4}(s,\Upsilon_i)\\
&= \zeta_{K_4,S_4}(s)L_{K/K_4,S_4}(s,\Upsilon_1)^2 L_{K/K_4,S_4}(s,\Upsilon_2)
\end{aligned}$$

puisque l'étude des caractères induits de H_4 dans G nous donne l'égalité $\mathrm{Ind}_{H_4}^G(\Upsilon_1) = \mathrm{Ind}_{H_4}^G(\Upsilon_3)$ et ainsi $L_{K/K_4,S_4}(s,\Upsilon_1) = L_{K/K_4,S_4}(s,\Upsilon_3)$. Le caractère Υ_2 passe au quotient par son noyau pour définir l'unique caractère non trivial $\widetilde{\Upsilon_2}$ de $\mathrm{Gal}(K_2/K_4) \simeq \mathbb{Z}/2\mathbb{Z}$, où $K_2 = K^{\langle\tau\rangle}$. On en déduit l'égalité

$$\zeta_{K_2,S_2}(s) = \zeta_{K_4,S_4}(s)L_{K_2/K_4,S_4}(0,\widetilde{\Upsilon_2}) = \zeta_{K_4,S_4}(s)L_{K/K_4,S_4}(0,\Upsilon_2),$$

ce qui donne finalement

$$\zeta_{K,S}(s) = \zeta_{K_2,S_2}(s) L_{K/K_4,S_4}(s, \Upsilon_1)^2.$$

De manière similaire, on démontre que $\zeta_{K_3,S_3}(s) = \zeta_{K_6,S_6}(s) L_{K/K_6,S_6}(s, \eta_3)$. Les identités suivantes (que l'on peut trouver dans [**Tat84**, chap. I]), données pour un corps de nombres F de nombre de classes h_F, de régulateur R_F et possédant $r_{1,F}$ plongements réels et $r_{2,F}$ plongements complexes, permettent alors d'obtenir la valeur recherchée :

$$\zeta_F(s) \sim -\frac{h_F R_F}{w_F} s^{r_{1,F}+r_{2,F}-1}$$
$$\text{et} \quad \zeta_{F,S\cup\{\mathfrak{p}\}} \sim \ln(\mathcal{N}(\mathfrak{p})) \cdot s \cdot \zeta_{F,S}$$

au voisinage de $s = 0$. On obtient au final

$$\frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_3)} = \pm \sqrt{\frac{h_K r_K w_{K_2}}{h_{K_2} R_{K_2} w_K} \prod_{\mathcal{P}\in S_2} \frac{\prod_{\mathfrak{P}/\mathcal{P}} \ln(\mathcal{N}(\mathfrak{P}))}{\ln(\mathcal{N}(\mathcal{P}))}} \cdot \frac{h_{K_6} R_{K_6} w_{K_3}}{h_{K_3} R_{K_3} w_{K_6}} \prod_{Q\in S_6} \frac{\ln(\mathcal{N}(Q))}{\prod_{\mathcal{Q}/Q} \ln(\mathcal{N}(\mathcal{Q}))}. \tag{5.2.2}$$

où $\mathfrak{P}$ parcourt l'ensemble des idéaux premiers de K au-dessus de $\mathcal{P}$, et $\mathcal{Q}$ l'ensemble des idéaux premiers de K_3 au-dessus de Q. Bien que cette formule ne soit valable qu'au signe près, les termes (regroupés) qui apparaissent peuvent tous être calculés de manière exacte.

5.2.2. Un exemple détaillé. — Nous détaillons ici sur un exemple la démarche utilisée en PARI-GP pour tester notre conjecture de Brumer-Stark non abélienne. On considère le cas où le corps de base k est le corps des nombres rationnels. Afin d'obtenir un corps K dont le groupe de Galois sur $\mathbb{Q}$ est isomorphe à $SL_2(\mathbb{F}_3)$, on utilise la base de donnée de Kluners (cf. [**Klu**]). Cette table nous donne un polynôme de degré 8, $P(x) = x^8 - 2x^7 + x^6 + x^5 - x^4 + 2x^3 + 4x^2 - 16x + 16$ dont le groupe de Galois est $SL_2(\mathbb{F}_3)$, à partir duquel nous construisons une extension K de degré 24 de groupe de Galois voulu. Le corps K considéré est le corps engendré sur $\mathbb{Q}$ par un entier algébrique α vérifiant

$$\alpha^{24} - 6\alpha^{23} - 13\alpha^{22} + 161\alpha^{21} + 138\alpha^{20} - 2648\alpha^{19} - 2160\alpha^{18} + 30177\alpha^{17} + 46614\alpha^{16}$$
$$- 297509\alpha^{15} - 685236\alpha^{14} + 2432267\alpha^{13} + 7184278\alpha^{12} - 14624097\alpha^{11} - 59413217\alpha^{10}$$
$$+ 70646068\alpha^9 + 429160067\alpha^8 - 439020766\alpha^7 - 1953797513\alpha^6 + 2406133100\alpha^5$$
$$+ 5506444854\alpha^4 - 6155768132\alpha^3 - 9169793005\alpha^2 + 7728723643\alpha + 11013503383 = 0.$$

Le discriminant absolu de K est $D_K = 853^{16}$ et 853 est donc le seul premier de $\mathbb{Q}$ qui se ramifie dans K. L'ensemble de places S minimal est ainsi $\{\infty, 853\}$, où ∞ désigne l'unique place infinie de $\mathbb{Q}$. Le groupe des classes de K est isomorphe à $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. La figure 5.1 donne la décomposition de 853 ainsi que celle des idéaux premiers au-dessus de lui dans les extensions définies dans la partie précédente.

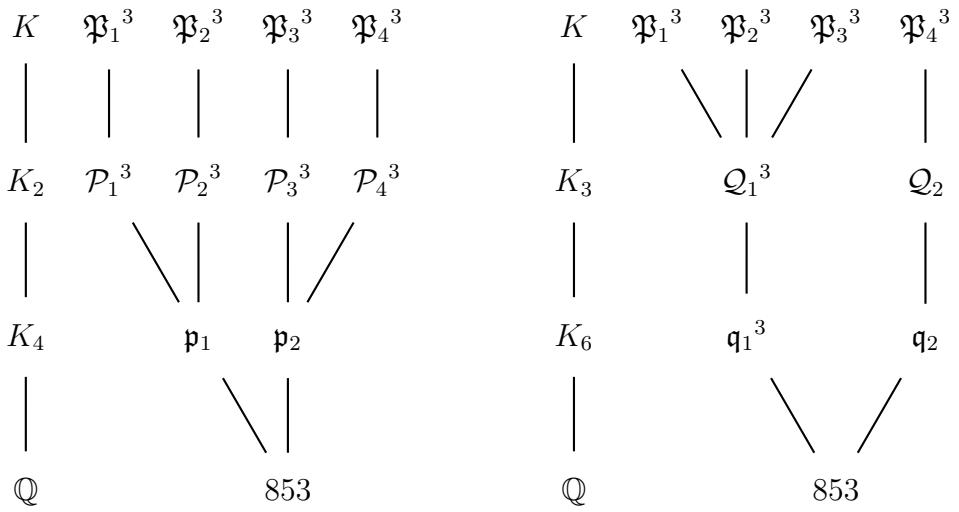


FIGURE 5.1. Décomposition du nombre premier 853 dans $K = \mathbb{Q}(\alpha)$

Puisqu'aucun idéal premier de S_4 n'est totalement décomposé dans K/K_4, la fonction $L_{K/K_4,S_4}(\cdot, \Upsilon_1)$ ne s'annule pas en $s = 0$. Il en est de même pour la fonction $L_{K/K_6,S_6}(\cdot, \eta_1)$ (resp. $L_{K/K_6,S_6}(\cdot, \eta_3)$), dont l'ordre en 0 est égal au nombre de premiers dans S_6 ne se décomposant pas dans K/K_6 (resp. K_3/K_6). L'extension de corps considérée $K/\mathbb{Q}$ correspond ainsi au cas 3 et l'élément de Brumer est donné par la proposition 5.1, où tous les termes sont non nuls.

On décompose cette expression en différentes composantes rationnelles : les classes de $\mathfrak{X}$ qui apparaissent sont celle de ψ_1, possédant uniquement le caractère ψ_1, et celle de ψ_2, composée des caractères ψ_2 et ψ_3.

Le calcul du premier terme peut être effectué au signe près par la formule (5.2.2) ou grâce à la fonction `bnrL1` de PARI-GP, permettant de calculer l'ordre d'annulation en $s = 0$ ainsi que le premier terme non nul de fonctions L abéliennes relatives :

$$\frac{L_{K/K_4,S_4}(0, \Upsilon_1)}{L_{K/K_6,S_6}(0, \eta_3)} e_{\overline{\psi_1}} = -\frac{22}{3}(1-\tau)(2I_2 + C_\sigma + C_{\sigma^{-1}}).$$

Le calcul de cette quantité par la fonction `bnrL1` pouvant prendre du temps, pour tester uniquement la composante de la conjecture correspondant à la classe du caractère ψ_1, on préfère utiliser la formule (5.2.2). On remarque ici que

$$m_G \frac{L_{K/K_4,S_4}(0, \Upsilon_1)}{L_{K/K_6,S_6}(0, \eta_3)} e_{\overline{\psi_1}} = -2^3 \cdot 11(1-\tau)(2I_2 + C_\sigma + C_{\sigma^{-1}}),$$

et l'exposant du groupe des classes de K est égal à 11. En particulier, pour tout idéal fractionnaire $\mathfrak{a}$ non nul de K, l'idéal $\mathfrak{a}^{11(2I_2+C_\sigma+C_{\sigma^{-1}})}$ est principal, engendré par β, et $\beta^{w_K(1-\tau)}$ est une anti-unité de K. Par conséquent, toute racine w_K-ième de $\beta^{w_K(1-\tau)}$ appartient à K et la propriété de centralité est trivialement vérifiée pour cette composante.

L'autre composante de l'élément de Brumer vaut

$$\frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_1)}e_{\overline{\psi_2}}+\frac{L_{K/K_4,S_4}(0,\Upsilon_1)}{L_{K/K_6,S_6}(0,\eta_5)}e_{\overline{\psi_3}}=\frac{1}{3}(1-\tau)(2I_2+2C_{\sigma^{-2}}+C_{\sigma^{-1}}),$$

et on obtient en définitive

$$\theta_{K/k,S}=\frac{1}{3}(1-\tau)(-42I_2-21C_{\sigma^{-1}}+2C_{\sigma^{-2}}-22C_\sigma).$$

Dans cet exemple, K ne possède que deux racines de l'unité ce qui permet d'observer que $w_K\theta_{K/k,S}$ n'est pas à coefficients entiers. En revanche, l'élément $m_G\theta_{K/k,S}=12\theta_{K/k,S}$ appartient à $\mathbb{Z}[G]$, et par suite le postulat concernant le dénominateur de l'élément de Brumer est vérifié.

On constate encore une fois dans les calculs que seule la partie $\frac{m_G}{4}(-42I_2-21C_{\sigma^{-1}}+2C_{\sigma^{-2}}-22C_\sigma)$ est nécessaire pour obtenir l'annulation du groupe des classes de K. Il s'ensuit que le générateur de l'idéal principal obtenu en appliquant $m_Gw_K\theta_{K/k,S}$ est une anti-unité de K qui est une puissance w_K-ième et la condition de centralité est trivialement vérifiée.

Proposition 5.2. — *La conjecture de Brumer-Stark non abélienne est vraie pour cette extension, elle est même vraie si on remplace $\theta_{K/k,S}$ par $\dfrac{\theta_{K/k,S}}{4}$.*

5.2.3. Résultats obtenus. — Tous les calculs ont été obtenus dans le cas où k est le corps des rationnels. Pour les 26 corps testés, l'élément de Brumer n'est jamais nul, 20 corps correspondent au cas 2 où l'écriture de $\theta_{K/k,S}$ ne fait apparaître qu'un seul terme non nul. Ces corps sont décrits dans la table 5.4. Les 6 corps restant correspondent au cas 3, où aucun des termes intervenant en 5.1 ne s'annule, et sont donnés par la table 5.3.

Les polynômes définissant les extensions K possèdent de grands coefficients. Dans le but d'améliorer la lisibilité des tables ci-dessous, on donne uniquement le polynôme P de degré 8 qui nous permet de trouver un polynôme générateur en prenant le polynôme réduit du premier polynôme de degré 24 donné par `polcompositum(P,P)`. On précise en outre le discriminant absolu du corps de nombres, et son groupe des classes.

Proposition 5.3. — *Pour les extensions intervenant dans les tables 5.3 et 5.4, le postulat concernant l'élément de Brumer ainsi que la conjecture de Brumer-Stark non abélienne sont vrais.*

Il est à noter que pour tous ces corps sauf pour l'avant dernier de la table 5.3, la généralisation de la partie "Stark" de la conjecture s'obtient trivialement. En effet, le facteur w_K n'est pas nécessaire pour avoir l'appartenance de $m_Gw_K\theta_{K/k,S}$ à $\mathbb{Z}[G]$ et l'annulation du groupe des classes par cet élément, ce qui entraîne la vérification de la condition de centralité. De plus, dans ces exemples, on constate que l'on peut factoriser $\theta_{K/k,S}$ par $(1-\tau)$ et obtenir tout de même l'annulation du groupe des classes par l'élément $m_Gw_K\theta_{K/k,S}$ privé de ce facteur. Les générateurs obtenus sont ainsi des anti-unités. Pour le corps problématique, seul le fait que les

générateurs soient des anti-unités de K ne se vérifie pas directement. On utilise alors le critère donné au lemme 3.9 pour vérifier cette partie.

On remarque aussi que le nombre des racines de l'unité des corps traités est toujours égal à 2. Enfin, dans de nombreux cas on constate l'existence de puissances superflues de 2 pour la démonstration de la conjecture de Brumer-Stark non abélienne.

Deux corps de la table 5.3 ont un comportement sensiblement différent des autres extensions testées. Pour le corps de discriminant $13^{16}199^{16}$, la vérification de la conjecture sans le facteur $w_K(1-\tau)$ ne peut pas se faire composante par composante contrairement à toutes les autres extensions considérées, mais elle est vraie pour l'élément de Brumer en entier.

Le dernier corps de la table donne un renseignement significatif sur le rôle de notre élément m_G. En effet, dans ce cas l'élément de Brumer associé est dans l'anneau de groupe $\mathbb{Z}[G]$ mais nécessite tout de même le facteur 3 provenant du nombre m_G pour annuler le groupe des classes, facteur ne pouvant apparaître grâce au terme w_K. On s'aperçoit ainsi que même si m_G peut ne pas être optimal en ce qui concerne l'intégralité de $\theta_{K/k,S}$, une partie au moins de cet élément est nécessaire pour obtenir la conjecture de Brumer-Stark non abélienne. Ceci semble indiquer que certains facteurs du dénominateur conjecturé sont essentiels pour la validité de la conjecture.

D_K	polynôme de degré 8	h_K	Cl_K
853^{16}	$x^8 - x^7 - 6x^6 + 26x^5 + 61x^4$ $-63x^3 + 185x^2 - 62x + 92$	121	$(\mathbb{Z}/11\mathbb{Z})^2$
$2^{36}277^{16}$	$x^8 + 26x^6 + 208x^4 + 520x^2 + 144$	1254400	$(\mathbb{Z}/140\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^3$
2311^{16}	$x^8 - 4x^7 + 32x^6 - 82x^5 + 176x^4$ $-220x^3 + 192x^2 - 95x + 26$	9025	$(\mathbb{Z}/95\mathbb{Z})^2$
$13^{16}199^{16}$	$x^8 + 30x^6 + 143x^4 + 205x^2 + 49$	8427	$\mathbb{Z}/199\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$
$2^{24}19^{16}37^{16}$	$x^8 + 22x^6 + 47x^4 + 23x^2 + 1$	2276736	$\mathbb{Z}/924\mathbb{Z} \times \mathbb{Z}/154\mathbb{Z}$ $\times(\mathbb{Z}/2\mathbb{Z})^4$
2803^{16}	$x^8 + 4x^7 + 36x^6 + 94x^5 + 270x^4$ $+388x^3 + 524x^2 + 345x + 151$	13689	$(\mathbb{Z}/117\mathbb{Z})^2$

TABLE 5.3. Table des extensions testées appartenant au cas 3

D_K	polynôme de degré 8	h_K	Cl_K
349^{16}	$x^8 - 4x^7 + 5x^6 - 3x^5 + 4x^4$ $-9x^3 + 45x^2 - 108x + 81$	9	$(\mathbb{Z}/3\mathbb{Z})^2$
547^{16}	$x^8 - 2x^7 - 3x^6 - 4x^5 + 50x^4$ $-30x^3 + 55x^2 - 34x + 32$	81	$(\mathbb{Z}/3\mathbb{Z})^4$
$7^{16}97^{16}$	$x^8 + 15x^6 + 60x^4 + 35x^2 + 1$	243	$(\mathbb{Z}/3\mathbb{Z})^5$
709^{16}	$x^8 - 4x^7 + 26x^6 - 64x^5 + 122x^4$ $-142x^3 + 114x^2 - 53x + 14$	441	$(\mathbb{Z}/21\mathbb{Z})^2$
$5^{12}163^{16}$	$x^8 - 2x^7 + 15x^6 - 22x^5 + 68x^4$ $-37x^3 + 188x^2 - 269x + 599$	2592	$(\mathbb{Z}/18\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^3$
$3^{12}277^{16}$	$x^8 - 3x^7 + 7x^6 - 5x^5 + 16x^4$ $-31x^3 + 289x^2 - 180x + 69$	1296	$\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ $\times\mathbb{Z}/2\mathbb{Z}$
$2^{24}277^{16}$	$x^8 + 13x^6 + 52x^4 + 65x^2 + 9$	28224	$(\mathbb{Z}/42\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^4$
$31^{16}37^{16}$	$x^8 + 17x^6 + 59x^4 + 46x^2 + 1$	1323	$(\mathbb{Z}/21\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$
$3^{32}7^{16}19^{16}$	$x^8 + 4x^7 + 36x^6 + 94x^5 + 244x^4$ $+336x^3 + 297x^2 + 144x + 27$	35721	$(\mathbb{Z}/21\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^4$
$2^{36}163^{16}$	$x^8 + 18x^6 + 92x^4 + 112x^2 + 16$	56448	$(\mathbb{Z}/84\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ $\times\mathbb{Z}/2\mathbb{Z}$
$2^{66}31^{16}$	$x^8 + 20x^6 + 42x^4 + 24x^2 + 4$	5832	$(\mathbb{Z}/18\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$ $\times\mathbb{Z}/3\mathbb{Z}$
$2^{66}31^{16}$	$x^8 + 12x^6 + 42x^4 + 40x^2 + 4$	12168	$(\mathbb{Z}/78\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$
1879^{16}	$x^8 - 4x^7 + 36x^6 - 94x^5$ $+396x^4 - 640x^3 + 1546x^2$ $-1241x + 1712$	13689	$(\mathbb{Z}/117\mathbb{Z})^2$
$7^{12}277^{16}$	$x^8 - 3x^7 + 16x^6 - 35x^5 + 153x^4$ $-325x^3 + 1148x^2 + 841x + 571$	176400	$\mathbb{Z}/420\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}$ $\times\mathbb{Z}/2\mathbb{Z}$
$2^{24}3^{12}163^{16}$	$x^8 + 27x^6 + 207x^4 + 378x^2 + 81$	903168	$\mathbb{Z}/168\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ $\times\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^4$
$3^{36}127^{16}$	$x^8 - 4x^7 + 4x^6 + 51x^5 - 51x^4$ $-207x^3 + 582x^2 + 984x + 600$	190512	$\mathbb{Z}/252\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}$ $\mathbb{Z}/6\mathbb{Z}$
$3^{12}19^{16}37^{16}$	$x^8 - 2x^7 + 8x^6 + 6x^5 - 106x^4$ $-6x^3 + 260x^2 + 325x + 502$	761048	$\mathbb{Z}/252\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}$ $\times\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$
$13^{12}163^{16}$	$x^8 + 2x^7 + 40x^6 - 19x^5 + 81x^4$ $+516x^3 + 1283x^2 + 1000x + 693$	1143072	$(\mathbb{Z}/126\mathbb{Z})^2 \times (\mathbb{Z}/6\mathbb{Z})^2$ $\times\mathbb{Z}/2\mathbb{Z}$
$2^{24}607^{16}$	$x^8 + 15x^6 + 47x^4 + 38x^2 + 9$	608400	$(\mathbb{Z}/390\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2$
$2^{72}4316$	$x^8 + 12x^6 + 44x^4 + 52x^2 + 9$	63504	$(\mathbb{Z}/126\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2$

TABLE 5.4. Table des extensions testées appartenant au cas 2

BIBLIOGRAPHIE

[Bar78] D. Barsky – « Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels », Groupe d'Etude d'Analyse Ultramétrique (5e année : 1977/78), Secrétariat Math., Paris, 1978, p. Exp. No. 16, 23.

[BBB+97] C. Batut, K. Belabas, D. Bernardi, H. Cohen & M. Olivier – « User's Guide to PARI-GP », 1997, http ://pari.math.u-bordeaux.fr.

[BJ11] D. Burns & H. Jonhston – « A non-abelian stickelberger theorem », *Compositio Math.* **147** (2011), p. 35–55.

[CN79] P. Cassou-Noguès – « Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques », *Invent. Math.* **51** (1979), no. 1, p. 29–59.

[Coh00] H. Cohen – *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[CR06] C. W. Curtis & I. Reiner – *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006, Reprint of the 1962 original.

[DR80] P. Deligne & K. A. Ribet – « Values of abelian L-functions at negative integers over totally real fields », *Invent. Math.* **59** (1980), no. 3, p. 227–286.

[GP11] C. Greither & C. D. Popescu – « An equivariant main conjecture in Iwasawa theory and applications », (à paraître), 2011.

[Gre00] C. Greither – « Some cases of Brumer's conjecture for abelian CM extensions of totally real fields », *Math. Z.* **233** (2000), no. 3, p. 515–534.

[GRT04] C. Greither, X.-F. Roblot & B. A. Tangedal – « The Brumer-Stark conjecture in some families of extensions of specified degree », *Math. Comp.* **73** (2004), no. 245, p. 297–315 (electronic).

[Hay98] D. R. Hayes – « Base change for the conjecture of Brumer-Stark », *J. Reine Angew. Math.* **497** (1998), p. 83–89.

[Hay04] ———, « Stickelberger functions for non-abelian Galois extensions of global fields », Stark's conjectures : recent work and new directions, Contemp. Math., vol. 358, Amer. Math. Soc., Providence, RI, 2004, p. 193–206.

[Isa08] I. M. Isaacs – *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008.

[Jau08] J.-F. Jaulent – « Plongements l-adiques et l-nombres de Weil », *J. Théor. Nombres Bordeaux* **20** (2008), no. 2, p. 335–351.

[Kli62] H. Klingen – « Über die Werte der Dedekindschen Zetafunktion », *Math. Ann.* **145** (1961/1962), p. 265–272.

[Klu] J. Kluners – `www.math.uni-duesseldorf.de/∼klueners/`.

[Mar77] J. Martinet – « Character theory and Artin L-functions », Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, p. 1–87.

[Mil11] J. S. Milne – « Fields and Galois theory », 2011, Disponible sur `www.jmilne.org/math/`.

[Neu99] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pop11] C. D. Popescu – « Integral and p-adic refinements of the abelian stark conjecture », The Arithmetic of L-Functions, The IAS-Park City Mathematics Series, vol. 18, AMS, 2011, (à paraître).

[RT00] X.-F. Roblot & B. A. Tangedal – « Numerical verification of the Brumer-Stark conjecture », Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, p. 491–503.

[Sam67] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[San84a] J. W. Sands – « Abelian fields and the Brumer-Stark conjecture », *Compositio Math.* **53** (1984), no. 3, p. 337–346.

[San84b] ———, « Galois groups of exponent two and the Brumer-Stark conjecture », *J. Reine Angew. Math.* **349** (1984), p. 129–135.

[Ser78] J.-P. Serre – *Représentations linéaires des groupes finis*, deuxième éd., Hermann, Paris, 1978.

[Sie70] C. L. Siegel – « Über die Fourierschen Koeffizienten von Modulformen », *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* **1970** (1970), p. 15–56.

[Tat81] J. Tate – « Brumer-Stark-Stickelberger », Seminar on Number Theory, 1980–1981 (Talence, 1980–1981), Univ. Bordeaux I, Talence, 1981, p. Exp. No. 24, 16.

[Tat84] ———, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Mathematics, vol. 47, Birkhäuser Boston Inc., Boston, MA, 1984, Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[The08] The PARI Group – Bordeaux, *PARI/GP, version* `2.3.4`, 2008, available from `http://pari.math.u-bordeaux.fr/`.

[Was97] L. C. Washington – *Introduction to cyclotomic fields*, deuxième éd., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[Wil90] A. Wiles – « On a conjecture of Brumer », *Ann. of Math. (2)* **131** (1990), no. 3, p. 555–565.