Dossier de troisième année

Yichao HUANG
encadré par Rémi RHODES et Vincent VARGAS

Octobre 2013

Table des matières

I Curriculum Vitæ **1**

II Introduction au domaine de recherche **4**

III Mémoire de M2 **12**

IV Mémoire de M1 **79**

Première partie

Curriculum Vitæ

Curriculum Vitæ

HUANG Yichao
Portable : 07 86 52 27 21
Email : `yichao.huang@ens.fr`
Nationalité chinoise
Né le 3 avril 1991

Études passées

2012-2013 : M2 à l'École Normale Supérieure de Paris et à l'Université Paris VI.

2011-2012 : M1 à l'École Normale Supérieure de Paris.

2010-2011 : L3 à l'École Normale Supérieure de Paris.

2008-2010 : Classes préparatoires à Paris au Lycée Janson de Sailly.

Travaux

Septembre 2013 : « Chaos multiplicatif gaussien critique : construction de la martingale dérivée, cas du champ libre gaussien massif sur le plan », mémoire de master sous la direction de Rémi Rhodes et Vincent Vargas.

Juin 2011 : « Sur le problème de Noether abélien », exposé de maîtrise réalisé avec Diego Izquierdo sous la direction d'Olivier Wittenberg.

Expériences pédagogiques

2011-2012 : Interrogateur en Sup 2 au lycée Janson de Sailly.

2010-2011 : Tuteur de six élèves du lycée dans le cadre de l'association TalENS.

Langues pratiquées

– **Chinois**, langue maternelle

– **Anglais**, courant

– **Français**, courant

Miscellanées

– **Piano** : “Niveau 10” obtenu en 2003, diplôme délivré par “The Music Examination Committee of the Chinese Musicians’ Association”.

Liste des cours de M2 suivis

Cours figurant dans le diplôme : Processus de Markov ; Mouvement brownien et calcul stochastique ; Processus ponctuels, graphes aléatoires et géométrie aléatoire ; Dimères et pavages aléatoires

Autres cours suivis : Théorie des nombres algébrique ; Matrices aléatoires ; Théorèmes limites et grandes déviations ; Processus stochastiques, quelques compléments ; Mécanique statistique et graphes aléatoires

Deuxième partie

Introduction au domaine de recherche

Introduction au domaine de recherche : Chaos multiplicatif gaussien

Yichao HUANG
sous la direction de Rémi RHODES et Vincent VARGAS

Octobre 2013

Résumé

La théorie du chaos multiplicatif gaussien a été introduite rigoureusement par J.P. Kahane en 1985. Après son succès pour la modélisation stochastique de la turbulence en 3d, elle s'est avérée importante aujourd'hui dans beaucoup de domaines variés tels que la gravité quantique de Liouville ou encore la finance. Dans cette courte introduction, nous essayons de donner un point de vue intuitif à la construction du chaos multiplicatif gaussien, en passant par le modèle discret dit des cascades de Mandelbrot qui est à l'origine de cette théorie.

Organisation du manuscript :
– Section 1 : Introduction : modèle des cascades de Mandelbrot
– Section 2 : Chaos multiplicatif gaussien : construction
– Section 3 : Chaos multiplicatif gaussien : théorème principaux
– Section 4 : Chaos multiplicatif gaussien : cas critique
– Section 5 : Chaos multiplicatif gaussien : la suite

1 Introduction : modèle des cascades de Mandelbrot

Dans cette section, une "nouvelle" variable aléatoire désigne une variable aléatoire indépendante de toutes les autres variables aléatoires qui sont déjà présentes. Cette section est rédigée de façon libre et informelle, le but étant de donner quelques intuitions et motivations pour la construction du chaos multiplicatif gaussien.

Rappelons la construction de Lévy du mouvement brownien (en dimension 1) en suivant [1].
L'image que donne cette construction est celle d'un segment élastique, que l'on déforme sous l'action additive d'une famille de variables aléatoires gaussiennes d'espérance 0 indépendantes.
• On part du segment (0,0)–(1,0).

FIGURE 1 – Un segment

•∗ On change le segment (0,0)–(1,0) en (0,0)–(1,ξ) avec ξ une variable gaussienne standard [1].
• On regarde les demi-segments (0,0)–(1/2,ξ/2) et (1/2,ξ/2)–(1,ξ).
• Pour chaque segment, on prend une nouvelle variable gaussienne standard ξ_0 (resp. ξ_1) et on le change en (0,0)–(1/2^2,$\xi_0/2^2 + \xi/2^2$)–(1/2,ξ/2) (resp. (1/2,ξ/2)–(3/2^2,$\xi_1/2^2 + 3\xi/2^2$)–(1,ξ)).
• Et ainsi de suite. La régle à la n-ième étape de la construction : on voit un segment affine de longueur $1/2^n$, on va tirer son point au milieu à une distance verticale $\xi_*/2^{n+1}$ par rapport à sa position initiale, avec ξ_* une nouvelle variable gaussienne standard.

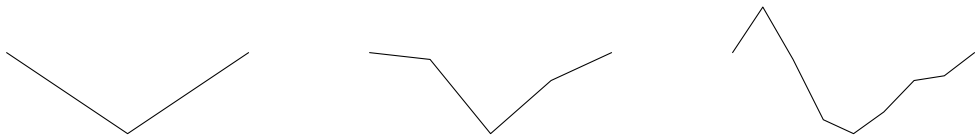

FIGURE 2 – Les trois premières étapes (pour un pont brownien)

L'objet que l'on obtient à la limite quand n tend vers l'infini est le mouvement brownien standard sur l'intervalle $[0, 1]$.
Rappelons une définition propre du mouvement brownien standard :

Définition 1.1 (Mouvement brownien standard)**.** *Un mouvement brownien standard* $(B_t)_{t\geq 0}$ *est un processus gaussien centré de covariance* $K(s, t) = \min(s, t)$.

En particulier, il s'agit d'un processus gaussien.

Rappelons maintenant la construction de Mandelbrot du modèle des cascades multiplicatives (en dimension 1) en suivant l'article [2].
L'image que donne cette construction est celle d'un pavé (divisible) élastique, que l'on déforme sous l'action multiplicative d'une famille de variables aléatoires d'espérance 1 indépendantes.
Fixons W une variable aléatoire d'espérance 1.
• On part du segment (0,1)–(1,1) et on regarde le pavé en-dessous de lui.
• On regarde les demi-segments (0,1)–(1/2,1) et (1/2,1)–(1,1).
• Pour chaque segment, on prend une nouvelle variable W_0 (resp. W_1) ayant la même loi que W

1. Si en revanche on impose $\xi = 0$, alors on obtiendra un pont brownien de (0,0) à (1,0).

FIGURE 3 – Un pavé

et on le change en $(0,W_0)$–$(1/2,W_0)$ (resp. $(1/2,W_1)$–$(1,W_1)$).
• Et ainsi de suite. La règle à la n-ième étape de la construction : on voit un segment horizontal de longueur $1/2^n$, on va le diviser en deux segment horizontaux de longueur $1/2^{n+1}$, et pour chaque segment, on choisit une nouvelle variable aléatoire ayant la même loi que W et on multiplie la hauteur du segment par cette nouvelle variable aléatoire.

FIGURE 4 – Les trois premières divisions (simulation avec $\mathcal{U}([\frac{1}{2},\frac{3}{2}])$)

On note Y_n la masse totale (i.e. le volume) après la n-ième étape et Y_∞ la masse totale à l'infini. Remarquons que Y_n forme une martingale et Y_∞ est la limite faible des Y_n. Cette martingale n'étant pas uniformément intégrable, il se peut que la limite Y_∞ soit dégénérée.
Bien sûr, dans la construction précédente, on peut diviser chaque intervalle en c parties égales au lieu de 2.
Concernant ce modèle des cascades, on a le théorème suivant (voir [2] pour une preuve) :

Théorème 1.1 (Critères de dégénérescence)**.** *Les assertions suivantes sont équivalentes :*
a) $\mathbb{E}[Y_\infty] = 1$ *;*
b) $\mathbb{E}[Y_\infty] > 0$ *;*
c) $\mathbb{E}[W \ln W] < \ln c$.

Ce modèle devient particulièrement intéressant quand la variable multiplicatrice W est gaussienne, i.e. de la forme $\exp(\xi - \mathbb{E}[\xi^2]/2)$, avec ξ une variable gaussienne centrée réduite. On verra dans la suite la construction du chaos multiplicatif gaussien, qui en est un modèle analogue dans le continu.

2 Chaos multiplicatif gaussien : construction

Cette section ainsi que celle qui suit sont basées sur l'article [3].
On introduit maintenant le chaos multiplicatif gaussien, qui est la version continue d'un cas particulier du modèle précédent. On se place dans $\mathbb{R}^d$ avec $d \in \mathbb{N}^*$.

> [Un peu de fausses intuitions...
> S'inspirant de la construction des cascades multiplicatives avec W gaussienne, le chaos multiplicatif gaussien en un point x sera alors "défini" comme
>
> $$Q(x) = \prod_{n=1}^{+\infty} e^{\xi_n - \frac{\mathbb{E}[\xi_n^2]}{2}} = e^{\sum_{n=1}^{+\infty} \xi_n - \frac{\mathbb{E}[\xi_n^2]}{2}}$$
>
> avec $(\xi_n)_{n\in\mathbb{N}^*}$ une suite de variables gaussiennes centrées indépendantes.
> Donc si l'on définit $X = \sum_{n=1}^{+\infty} \xi_n$, on a envie de définir Q par
>
> $$Q(x) = e^{X - \frac{\mathbb{E}[X^2]}{2}}$$
>
> Malheureusement cette définition n'est pas rigoureuse. Par exemple si l'on prend pour chaque ξ_n une gaussienne centrées réduites, X sera de variance infinie...
> Il va falloir en effet définir une distribution (au sens de Schwartz) plutôt qu'une fonction.]

Cette fois-ci on fait une construction plus directe et plus générale sans passer par la division des pavés. Tout comme le mouvement brownien est défini comme un processus gaussien, on va regarder un processus gaussien indexé par l'espace $\mathbb{R}^d$. Dans la littérature on l'appelle plutôt champ gaussien, car la géométrie de l'espace sous-jacent (ici $\mathbb{R}^d$) joue souvent un rôle dans l'étude de notre processus. Le but maintenant est de construire un objet qui est l'exponentielle (renormalisée) de ce champ gaussien, comme annoncé antérieurement.
Prenons donc un champ gaussien X défini sur $\mathbb{R}^d$. Le but est de donner un sens à l'objet suivant :

$$A \mapsto \int_A e^{X(x) - \frac{\mathbb{E}[X(x)^2]}{2}} dx$$

pour tout borélien A borné de $\mathbb{R}^d$. Si l'on arrive à construire proprement un tel objet, on dispose alors d'une mesure de Radon positive sur $\mathbb{R}^d$. Bien sûr si l'on remplace dx par une mesure de Radon quelconque, alors on définit une action sur l'espace des mesures de Radon positives sur $\mathbb{R}^d$.
Dans la suite de cette section, on suppose que le noyau de covariance q de X (rappelons que q est définie par $q(x,y) = \mathbb{E}[X(x)X(y)]$, et qu'il est symétrique positif) s'écrit comme la somme d'une suite de noyaux gaussiens positifs continus $q = \sum_{n=1}^{+\infty} p_n$.
On prend alors une suite de champs gaussiens X_i indépendants, chaque X_i ayant p_i comme noyau de covariance. En vue d'étudier $\sum_{n=1}^{+\infty} X_i$, on introduit la somme partielle $Y_k = \sum_{n=1}^{k} X_k$ et on regarde, pour chaque borélien A borné,

$$Q_k(A) = \int_A e^{Y_k(x) - \frac{\mathbb{E}[Y_k(x)^2]}{2}} dx = \int_A \prod_{n=1}^{k} e^{X_n(x) - \frac{\mathbb{E}[X_n(x)^2]}{2}} dx$$

Par indépendance des X_n, ceci est une martingale ! En plus elle est positive, donc elle converge p.s. vers une limite que l'on note $Q(A)$. On appelle Q l'opérateur chaos multiplicatif gaussien (qui agit sur l'espace des mesures de Radon positives sur $\mathbb{R}^d$, les calculs précédents se généralisent facilement à une mesure de Radon positive quelconque).
On laisse aux lecteurs le soin de vérifier que ceci nous définit bien une mesure de Radon aléatoire.
Résumons :

Définition 2.1 (Opérateur du chaos multiplicatif gaussien)**.** *Soit σ une mesure de Radon positive sur $\mathbb{R}^d$. X un champ gaussien de noyau de covariance q, et X_n une suite de champs gaussiens de noyau de covariance p_n respectif (positif, continu) telle que $q = \sum_{n=1}^{+\infty} p_n$.*
Alors l'opérateur du chaos multiplicatif gaussien Q agit sur σ par

$$Q\sigma(A) = \lim_{k\to+\infty} \int_A \prod_{n=1}^{k} e^{X_n(x) - \frac{\mathbb{E}[X_n(x)^2]}{2}} d\sigma(x)$$

avec A borélien borné quelconque.

Attention toutefois que pour l'instant, cette définition du chaos multiplicatif gaussien dépend de la suite de décomposition p_n choisie. On verra dans la suite un théorème d'unicité qui enlèvera cette malheureuse liaison.

3 Chaos multiplicatif gaussien : théorèmes principaux

Le premier théorème justifie la construction du chaos multiplicatif gaussien : sa définition ne dépend pas de la décomposition choisie. Le second théorème important est un phénomène de transition de phases pour une certaine classe intéressante du chaos multiplicatif gaussien, tout comme dans le cas discret.

Théorème 3.1 (Unicité)**.** *L'opérateur du chaos multiplicatif gaussien Q ne dépend pas du choix de la suite de noyaux p_n. Plus précisément, si Q est l'opérateur associé à la décomposition p_n et Q' celui associé à la décomposition p'_n avec $\sum_{n=1}^{+\infty} p_n = \sum_{n=1}^{+\infty} p'_n = q$, alors Q et Q' sont égaux en loi.*

Voici quelques idées clés de la démonstration de ce théorème.
Rappelons d'abord le théorème de De la Vallée Poussin qui permet de détecter l'uniforme intégrabilité d'une martingale par le biais d'une fonction convexe F :

Lemme 3.2 (Théorème de De la Vallée Poussin)**.** *Soit $(M_n)_n$ une martingale. Elle est uniformément intégrable ssi il existe une fonction convexe $F : \mathbb{R}_+ \to \mathbb{R}_+$ et un α fixé positif tels que*
1) $\frac{F(x)}{x} \to +\infty$ quand $x \to +\infty$;
2) $F(\lambda x) \leq \lambda^\alpha F(x)$ pour tout $\lambda > 0$;
3) $\sup_n \mathbb{E}[F|M_n|] < +\infty$.

On dispose ensuite de l'inégalité de convexité de Kahane pour les processus gaussiens, qui nous permet de comparer (via une fonction convexe F) deux chaos multiplicatifs gaussiens dont les champs gaussiens sous-jacents ont des noyaux de covariance uniformément proches.

Lemme 3.3 (Inégalité de convexité de Kahane)**.** *Soient $(X_i)_{i\in I}$ et $(Y_i)_{i\in I}$ deux familles finies de variables aléatoires réelles gaussiennes. On suppose que $\forall i, j \in I$, $\mathbb{E}[X_iX_j] \leq \mathbb{E}[Y_iY_j]$. Soit $F : \mathbb{R}_+ \to \mathbb{R}$ une fonction convexe avec croissance au plus polynomiale à l'infini. Alors*

$$\forall p_i \geq 0, \mathbb{E}[F(\sum_{i\in I} p_i \exp(X_i - \frac{1}{2}\mathbb{E}[X_i^2]))] \leq \mathbb{E}[F(\sum_{i\in I} p_i \exp(Y_i - \frac{1}{2}\mathbb{E}[Y_i^2]))]$$

Les sommes partielles de p_n et de p'_n sont très proche uniformément à l'infini : c'est assuré par le théorème de Dini. Alors on peut comparer les chaos associés à l'aide de l'inégalité de Kahane, via une fonction convexe F. Les chaos sont en effet comparables à un facteur multiplicatif près

(toujours via la fonction convexe F). Mais alors par le théorème de De la Vallée Poussin, si l'un est uniformément intégrable, l'autre le sera aussi par la 3) du théorème. Les détails et le reste de la preuve sont laissés aux lecteurs (ils sont dans les références).
Dans la suite de cette section on se place dans le cas où le champ X est stationnaire défini sur $\mathbb{R}^d$, de fonction de covariance $q(x) = -\gamma^2 \log|x| + O(1)$, où x désigne la distance entre deux points (par stationnarité). On observe alors un phénomène de transition de phases lorsque le paramètre γ se rapproche de $\sqrt{2d}$.

Théorème 3.4 (Transition de phases)**.** *σ désigne la mesure de Lebesgue sur $\mathbb{R}^d$.*
Soit Q le chaos multiplicatif gaussien associé à q.
– *Si $\gamma^2 < 2d$, alors σ est fortement non-dégénérée pour Q : $\mathbb{E}[Q\sigma(A)] = A$ pour tout borélien A ;*
– *Si $\gamma^2 \geq 2d$, alors σ est dégénérée pour Q : $\mathbb{E}[Q\sigma(A)] = 0$ pour tout borélien A.*

Ce théorème se démontre à partir du théorème dans le cas discret (théorème 1.1) en utilisant des techniques d'approximation (l'idée étant d'approximer un intervalle par un ensemble auto-similaire construit à la Cantor, puis d'utiliser le théorème dans le cas discret sur l'arbre naturellement associé à cette construction). Les détails se trouvent dans l'article [3].

4 Chaos multiplicatif gaussien : cas critique

On dit un mot sur le comportement au voisinage du point critique du chaos multiplicatif gaussien. Cette section est basée sur l'article [4].
On se place toujours dans le cas où l'espace ambient est $\mathbb{R}^d$ (ou un sous-domaine de $\mathbb{R}^d$), avec X un champ de noyau de covariance $K(s,t) = -\log|s-t| + O(1)$. Le noyau de covariance pour γX sera alors $K^\gamma(s,t) = -\gamma^2 \log|s-t| + O(1)$.
On compte parmi les exemples du champ gaussien log-corrélé le très étudié champ libre gaussien (*gaussian free field* en anglais) ou encore le champ libre gaussien massif (*massive gaussian free field* en anglais).
Remarquons tout de suite que le cas sur-critique est facile à étudier car on sait d'après le théorème de Kahane (théorème 3.4) que la mesure limite est dégénérée dans ce cas.
Pour étudier le chaos multiplicatif gaussien dans le cas sous-critique, on introduit la martingale dérivée, obtenue en dérivant formellement par rapport au paramètre γ :

$$M_t'(A) = -\frac{\partial}{\partial\gamma}[M_t^\gamma(A)]_{\gamma=\sqrt{2d}} = [\int_A (\gamma\mathbb{E}[X_t(x)^2] - X_t(x))e^{\gamma X_t(x) - \frac{\gamma^2}{2}\mathbb{E}[X_t(x)^2]}dx]_{\gamma=\sqrt{2d}}$$

où X_t est un champ gaussien stationnaire de noyau

$$K_t(x) = \int_1^{e^t} \frac{k(ux)}{u} du$$

(avec k un noyau gaussien, $k(0) = 1$) de sorte que $\lim_{t\to+\infty} K_t(x) = K(x)$.

[Par exemple, pour le champ libre gaussien massif de masse m,

$$K(x) = G_m(x) = \int_0^{+\infty} \frac{1}{2u} e^{-mu - \frac{|x|^2}{2u}} du = \int_1^{+\infty} \frac{k_m(ux)}{u} du$$

avec $k_m(z) = \frac{1}{2}\int_0^{+\infty} e^{-\frac{m|z|^2}{v} - \frac{v}{2}} dv$.]

Concernant M_t', on a le théorème suivant :

Théorème 4.1 (Théorème DRSV)**.** *Supposons que k est à support compact. Alors quand t tend vers l'infini, M'_t converge p.s. vers une limite non triviale que l'on note M'. En plus, M' est à support plein et sans atome.*

Les hypothèses telles que la stationnarité sur X et la compacité du support sur k peut-être relaxées, à conditions d'avoir une décroissance rapide du noyau de covariance K.
Différentes preuves sont proposées, basées sur la méthode dite du cut-off : on exploite le caractère log-corrélé du champ et on distingue le phénomène de courte corrélation avec celui à longue portée. La preuve étant technique, les lecteurs intéressés par les détails techniques sont invités à consulter les références.

5 Chaos multiplicatif gaussien : la suite

On en trouve déjà dans la littérature beaucoup de généralisations et d'applications de la théorie du chaos multiplicatif gaussien. Les lecteurs intéressés peuvent consulter [5].
Le chaos multiplicatif gaussien est aussi parmi les candidats pour la limite continue de surfaces aléatoires discrètes [2].
À vous d'écrire la suite des aventures dans le monde du chaos multiplicatif gaussien !

Références

[1] P. Lévy, « Le mouvement brownien », 1954.

[2] J.-P. Kahane et J. Peyrière, « Sur certaines martingales de benoit mandelbrot », *Advances in Mathematics*, vol. 22, no. 2, p. 131–145, 1976.

[3] J.-P. Kahane, « Sur le chaos multiplicatif », *Ann. Sci. Math. Québec*, 1985.

[4] B. Duplantier, R. Rhodes, S. Sheffield et V. Vargas, « Critical gaussian multiplicative chaos : convergence of the derivative martingale », *arXiv preprint arXiv :1206.1671*, 2012.

[5] R. Rhodes et V. Vargas, « Gaussian multiplicative chaos and applications : a review », *arXiv preprint arXiv :1305.6221*, 2013.

2. On rappelle que le mouvement brownien est limite continue d'une marche aléatoire simple symétrique.

Troisième partie

Mémoire de M2

Chaos multiplicatif gaussien critique : Construction de la martingale dérivée, cas du champ libre gaussien massif sur le plan

Mémoire de M2 de Yichao HUANG
sous la direction de Rémi RHODES et Vincent VARGAS

Septembre 2013

Table des matières

1 Introduction **1**
1.1 Un très bref historique du chaos multiplicatif gaussien 1
1.2 Un petit aperçu du chaos multiplicatif gaussien 2
1.3 Organisation du manuscript 4
1.4 Remerciements 4

2 La théorie de Kahane **5**
2.1 Construction de l'opérateur du chaos multiplicatif 5
2.1.1 Définitions 5
2.1.2 Fonction de type sigma-positif 6
2.1.3 Martingale des poids partiels 7
2.2 Théorèmes principaux 8
2.2.1 Unicité de la construction 8
2.2.2 Critère de non-dégénéréscence 10
2.3 Quelques propriétés 11
2.3.1 Existence des moments positifs 11
2.3.2 Non-linéarité du spectre puissance 19

3 Étude du cas critique **20**
3.1 Construction de la martingale dérivée 20
3.2 Preuve du théorème 3.2 22
3.3 Sur le supremum d'un champ gaussien log-corrélé 30

4 Un petit résultat **37**
4.1 Énoncé du théorème dans le cas du champ libre gaussien massif . . 37
4.2 Discussion sur le cut-off 38
4.3 Preuve du théorème 4.1 40

5 Quelques rappels de probabilités **48**
5.1 Quelques théorèmes sur les martingales et les mouvements browniens 48
5.2 Quelques inégalités gaussiennes 49
5.3 Rappels sur les champs gaussiens 56
5.3.1 Définition du champ gaussien 56
5.3.2 Fonction de Green 57
5.3.3 Champ libre gaussien (GFF) 58
5.3.4 Champ libre gaussien massif (MGFF) 59
5.4 Un lemme sur le processus du branchement 60

1 Introduction

1.1 Un très bref historique du chaos multiplicatif gaussien

La théorie du chaos multiplicatif gaussien a été introduite par J.P. Kahane dans les années 80 dans [11], motivée par la modélisation statistique de l'énergie de dissipation dans l'étude de la turbulence [17]. Cette théorie a été révisée et étudiée récemment et s'est avérée aujourd'hui importante dans beaucoup de domaines variés, par exemple en finance ou encore en physique (gravité quantique de Liouville et formule de KPZ, [8], [7], voir [6] pour plus de discussions), turbulence en dimension 3 (voir [24] pour plus de références). L'article [22] fournit une liste impressionnante d'applications directes de la théorie, y compris une collection de généralisations de cette théorie qui est en plein développement.
Comme fil conducteur de cette présentation, nous avons choisi de présenter brièvement son intervention (dans un contexte historique) dans l'étude de la turbulence. On veut comprendre le transfert d'énergie dans un écoulement turbulent, par une voie statistique. Une propriété classique est le processus dit cascade d'énergie : un grand tourbillon peut être divisé en tourbillons plus petits, permettant un transfert d'énergie des grandes échelles vers les petites échelles.
Un objet important dans la compréhension du transfert d'énergie est la dissipation locale que l'on note ϵ (qui à chaque région A associe une énergie $\epsilon(A)$). En 1941, Kolmogorov proposa une étude statistique de cette quantité, appelée théorie K41. Sous quelques hypothèses convenables (par exemple si le nombre de Reynolds est suffisamment grand), il postula que la dissipation locale d'énergie devrait être :
1) spatialement homogène : la loi de ϵ est invariante par translations spatiale ;
2) statistiquement isotrope : la loi de ϵ est invariante par rotations ;
3) autosimilaire : il existe $\alpha > 0$ tel que pour tout $\lambda > 0$, on a $\epsilon(\lambda A) = \lambda^\alpha \epsilon(A)$ en loi.
Une conséquence de ces critères est la linéarité du spectre de loi puissance :

$$\mathbb{E}[\epsilon(B(0,r))^q] = Cr^{\xi(q)}$$

où ξ est une fonction linéaire en q.
Cette théorie féconde d'un point de vue mathématique fut toutefois contestée par Landau, en raison de la non-linéarité du spectre de loi puissance observée dans les études expérimentales relevant un phénomène plus général dit d'intermittence. En 1962, Kolmogorov et Obukhov révisèrent la théorie et formulèrent la théorie KO62, dans laquelle la troisième hypothèse fut remplacée par :
3) log-normalité : la variable $\epsilon(A)$ est log-normale, i.e. "$\ln \epsilon(A)$ suit une loi normale" ;
4) non-linéarité du spectre de loi puissance.
L'objet de la construction du chaos multiplicatif gaussien a été, entre autres, de donner un objet (probabiliste) satisfaisant les critères de la théorie KO62.

Mais depuis, de bonnes propriétés manifestées par le chaos multiplicatif gaussien (multifractalité, autosimilarité etc.) ont fait de lui un modèle important dans des domaines très variés.

1.2 Un petit aperçu du chaos multiplicatif gaussien

L'objet principal dans la théorie du chaos multiplicatif gaussien est le suivant :

$$A \mapsto \int_A \exp(X(x) - \frac{1}{2}\mathbb{E}[X(x)^2])dx$$

où A est un borélien (dans $\mathbb{R}^d$ par exemple) et X un champ gaussien centré (défini sur $\mathbb{R}^d$ par exemple).
Nous essayons d'expliquer maintenant de façon informelle, sans trop entrer dans les détails, pourquoi cette définition est intéressante.
C'est une "exponentielle renormalisée" d'un champ gaussien (i.e. en chaque point c'est l'exponentielle renormalisée d'une variable aléatoire gaussienne, avec une certaine structure de covariance entre les gaussiennes). Pourquoi est-il naturel d'étudier cet objet pour la modélisation de l'énergie de dissipation ?
Pour cela, réfléchissons un peu comment on peut modéliser de façon agréable le "transfert d'énergie des grandes échelles vers les petites échelles". Une solution élégante a été proposée par Mandelbrot dans [17], où l'on a étudié un modèle dit des cascades. Pour une présentation heuristique, on se place maintenant dans le demi-plan supérieur.

– Prenons le segment $(0,1)-(1,1)$ et regardons l'aire de la région en-dessous de ce segment. Méditons un peu et imaginons pendant quelques minutes que ça représente un bloc d'énergie dans une grande échelle ;

FIGURE 1 – Un pavé

– Divisons le segment en deux parties, $(0,1)-(\frac{1}{2},1)$ et $(\frac{1}{2},1)-(1,1)$. Numérotons-les en binaire, disons la partie 0 et la partie 1. Nous voudrions maintenant changer un peu l'aire sous chaque petit segment : on multiplie indépendamment la hauteur de chaque partie par une variable aléatoire normalisée, i.e. d'espérance 1 (pour des

raisons de conservation d'énergie). Notons alors W_0, W_1 deux variables aléatoires indépendantes et identiquement distribuées (selon la loi d'un W disons), et changeons les petits segments en $(0, W_0) - (\frac{1}{2}, W_0)$ et $(\frac{1}{2}, W_1) - (1, W_1)$. Contentons de dire pendant quelques minutes que ça représente le transfert d'énergie d'une grande échelle vers une petite échelle ;

– Et comme il n'y a visiblement aucune difficulté à continuer cette démarche, on la fait une fois de plus. Regardons les quatre petits segments $(0, W_0) - (\frac{1}{2^2}, W_0)$, $(\frac{1}{2^2}, W_0) - (\frac{1}{2^1}, W_0)$, $(\frac{1}{2^1}, W_1) - (\frac{1}{2^1} + \frac{1}{2^2}, W_1)$, $(\frac{1}{2^1} + \frac{1}{2^2}, W_1) - (1, W_1)$, numérotés respectivement 00, 01, 10, 11. Prenons quatre variables aléatoires W_{00}, W_{01}, W_{10}, W_{11} ayant la même loi que W, indépendantes entre elles et indépendantes de W_0, W_1. Multiplions la hauteur de chaque partie par la variable aléatoire associée de façon évidente, et on obtient quatre rectangles, chacun ayant pour base $\frac{1}{2^2}$ et pour hauteur $W_* W_{**}$;

FIGURE 2 – Les trois premières divisions (simulation avec $\mathcal{U}([\frac{1}{2}, \frac{3}{2}])$)

– Et on continue, mais dans la tête. Et ce jusqu'à l'infini. À la fin, il n'y aura probablement plus de rectangle, mais des segments (un peu comme le mouvement brownien selon la construction de Lévy, à la fin on ne voit plus de segments en zigzag). Intuitivement, si l'on choisit un point x uniformément au hasard dans l'intervalle $[0, 1[$, presque sûrement [1], la hauteur au-dessus de x devrait être sous la forme d'un produit infini de copies indépendantes de W. Mais alors le théorème central limite classique nous dit que, en prenant le logarithme, c'est une gaussienne (quoique de variance infinie, on en discutera proprement dans la suite).

Maintenant si l'on prend un borélien A et on s'intéresse à l'énergie de A, on fait une intégrale, qui nous donne la forme de l'expression au début de la discussion. Il s'avère que c'est une bonne définition en passant par une intégrale, car on a du mal à manipuler une gaussienne de variance infinie comme une fonction classique, mais comme distribution (donc on s'intéresse à sa valeur moyenne), il n'y a plus de

1. Il va falloir avoir beaucoup de chance pour que l'on tombe sur un nombre dont le développement en base 2 est fini, car c'est un ensemble dénombrable donc de mesure de Lebesgue nulle.

souci au niveau théorique.
Reste, par exemple, à imposer des conditions sur la loi de W. Ceci revient, si nous oublions un instant l'intuition au-dessus et gardons juste en esprit le formalisme "l'exponentielle d'un champ gaussien", à imposer des structures de covariances sur le champ gaussien X sous-jacent. Un bon choix de la fonction de covariance nous mènera à un objet qui répond à la théorie KO62, on verra cela rigoureusement dans la section qui suit.

1.3 Organisation du manuscript

• Section 2 : nous rappelons la théorie de Kahane en 1985, en particulier la construction du chaos multiplicatif gaussien comme la limite d'une martingale ;
• Section 3 : nous suivons de près l'article de Duplantier, Rhodes, Scheffield et Vargas [6] sur la construction de la martinagle dérivée dans le cas critique ;
• Section 4 : nous fournissons les calculs pour la construction de la martingale dérivée dans le cas d'un champ libre gaussien massif dans le cas critique ;
• Section 5 : nous rassemblons quelques résultats en probabilités qui nous sont utiles.

1.4 Remerciements

J'aimerais remercier chaleureusement M. Rémi Rhodes et M. Vincent Vargas d'avoir accepté de me proposer ce sujet de mémoire stimulant, de leur disponibilité, leurs conseils précieux et leur enthousiasme dont je suis très reconnaissant tout au long de ce travail.
J'aimerais aussi remercier M. Wendelin Werner pour m'avoir orienté vers ce domaine fort intéressant.

2 La théorie de Kahane

Dans un premier temps, nous rappelons la construction du chaos multiplicatif gaussien, en nous appuyant sur le texte original de Kahane [11] ainsi que les surveys [24], [22]. Ce qui suit dans cette section est très largement inspiré de [21].

Remarque 2.1. ***Avertissement***
Dans la suite, certaines conditions que l'on exige sur le noyau pour construire le chaos multiplicatif gaussien pour être affaiblies (et en pratique c'est important de pouvoir les relaxer), voir [24].

2.1 Construction de l'opérateur du chaos multiplicatif

Dans cette section on va donner la construction d'un modèle qui répond aux critères de la théorie KO62. Le but est de construire une sorte de "l'exponentielle d'un champ gaussien" vu l'hypothèse de log-normalité imposée par la théorie KO62. Informellement, l'objet mathématique que l'on veut construire devrait ressembler à

$$A \mapsto \int_A \exp(X_x - \frac{1}{2}\mathbb{E}[X_x^2])dx$$

où A désigne un borélien de $\mathbb{R}^d$ et X un processus gaussien réel centré (stationnaire) sur $\mathbb{R}^d$. Ceci est une "mesure aléatoire" sur l'ensemble des boréliens de $\mathbb{R}^d$.
On se refère à la section 5 pour les définitions et les terminologies sur le champ gaussien. Souvent dans la pratique, le champ X possède en plus le caractère log-corrélé, à savoir que son noyau de covariance $f_X(s,t)$ se comporte comme $\ln \frac{1}{|s-t|} + O(1)$ quand $|s-t| \to 0$. Un exemple célèbre du champ gaussien log-corrélé est le champ libre gaussien (massif) que l'on traite dans la section 4. Dans ce cas, on manipule plutôt les distributions (au sens de Schwartz) que les fonctions au sens classique.

2.1.1 Définitions

On se place dans $\mathbb{R}^d$ avec $d \geq 1$. M_+ désignera l'espace des mesures de Radon positives sur $\mathbb{R}^d$.

Définition 2.1. ***Poids aléatoire***
Soit p une fonction réelle de type positif continue sur $\mathbb{R}^d$ et X un processus gaussien réel centré stationnaire associé à p.
Le poids aléatoire P associé au processus X est défini par

$$P(x) = \exp(X_x - \frac{1}{2}\mathbb{E}[X_x^2]) = \exp(X_x - \frac{1}{2}p(0))$$

et l'action de P sur M_+ est définie par

$$\forall \sigma \in M_+, P\sigma(dx) = P(x)\sigma(dx)$$

2.1.2 Fonction de type sigma-positif

On se donne une suite $(p_n)_{n\in\mathbb{N}}$ de fonctions réelles **positives**[2] de type positif et **continues** sur $\mathbb{R}^d$. On se donne ensuite une suite de processus gaussiens stationnaires indépendants $(X^n)_{n\in\mathbb{N}}$ associés à $(p_n)_{n\in\mathbb{N}}$. On pose

$$q_n(x) = \sum_{i=1}^{n} p_i(x)$$

comme la somme partielle des p_n, et

$$Y^n(x) = \sum_{i=1}^{n} X^i(x)$$

la somme partielle des X^n.
Remarquons que q_n et Y^n sont associés. Le poids Q^n associé à Y^n n'est autre que le produit partiel des poids $P^1 \times \cdots \times P^n$.
On pose

$$q = \sum_{n=1}^{\infty} p_n$$

Définition 2.2. ***Fonction de type sigma-positif***
Une telle fonction q est dite de type sigma-positif. On dira également que q est un noyau de type sigma-positif.

Remarque 2.2. ***Sur le spectre puissance de l'opérateur***
On explique maintenant pourquoi l'on a voulu prendre une suite de fonctions de type-positif au lieu d'une seule.
Prenons une fonction p de type positif continu et un processus gaussien stationnaire associé X. On définit l'opérateur P qui agit sur l'espace $\mathcal{M}_+$ des mesures de Radon positives sur $\mathbb{R}^d$:

$$\forall \sigma \in \mathcal{M}_+, \forall A \in \mathcal{B}(\mathbb{R}^d), P\sigma(dx) = P(x) \cdot \sigma(dx)$$

Ceci nous définit bien une sorte d'exponentielle du mouvement brownien dans $\mathbb{R}^2$. Mais pour appliquer cela à notre problème de modélisation de l'énergie de dissipation locale, cette méthode n'est pas assez élaborée : on va se retrouver devant un spectre

2. Ceci n'est pas nécessaire, mais simplifiera les calculs de cette section, voir [22].

de loi puissance linéaire.
Voici un calcul du spectre puissance dans un cas simple. Pour $d = 1$, $\alpha > 0$ et t tendant vers 0 :

$$\mathbb{E}[(P\sigma[0,t])^\alpha] \to t^\alpha \exp(\frac{1}{2}(\alpha^2 - \alpha)p(0))$$

car pour tout $\alpha > 0$, $\mathbb{E}[(P(x))^\alpha] = \exp(\frac{1}{2}(\alpha^2 - \alpha)p(0))$. On constate que le spectre de loi puissance est linéaire dans ce cas.

2.1.3 Martingale des poids partiels

Maintenant on va définir un opérateur limite associé à q.
Remarquons que pour tout borélien A de $\mathbb{R}^d$, la suite $(Q^n\sigma(A))_n$ est une martingale positive par rapport à la filtration $\mathcal{F}_n$ engendrée par les variables $\{X_u^k; k \leq n, u \in \mathbb{R}^d\}$:

$$\mathbb{E}[Q^n\sigma(A)|\mathcal{F}_{n-1}] = \int_A Q^{n-1}(x)\mathbb{E}[P^n(x)]\sigma(dx) = Q^{n-1}\sigma(A)$$

par indépendance des X^k et le fait que le poids est normalisé.
En se rappelant qu'une martingale positive converge p.s., on peut alors définir un opérateur limite.

Définition 2.3. ***Opérateur du chaos multiplicatif gaussien***
L'opérateur limite Q, qui à chaque $\sigma \in \mathcal{M}_+$ associe la limite de la suite $Q^n\sigma$ notée $Q\sigma$, est appelé l'opérateur du chaos multiplicatif associé au noyau q.

Remarque 2.3. ***Unicité de la constuction***
On verra dans la suite que cette définition ne dépend pas de la décomposition choisie. La définition est donc bien posée.

En récapulatif, l'opérateur du chaos multiplicatif gaussien est donc construit comme la limite d'une martingale positve. Naturellement, on veut savoir un peu plus sur la dégénérescence de cette limite. Ceci est l'un des objets d'étude du reste de cette section.
On donne tout de suite quelques conséquences élémentaires de cette construction.

Proposition 2.1. ***Propriétés élémentaires***
Voici quelques conséquences immédiates de la construction de l'opérateur du chaos multiplicatif gaussien :
1) - $\mathbb{E}[Q\sigma(A)] \leq \sigma(A)$. Ceci résulte du lemme de Fatou.
2) - La probabilité que la mesure $Q\sigma(A)$ soit nulle vaut 0 ou 1. Ceci est une conséquence de la loi du $0-1$ de Kolmogorov : on constate que pour A borélien quelconque, l'évènement $Q(A) = 0$ est un évènement dans la tribu à l'infini.
3) - Si σ est la mesure de Lebesgue, la mesure aléatoire $Q\sigma$ associée est soit identiquement nulle, soit à support plein, i.e. $\mathbb{R}^d$ tout entier. C'est une conséquence de l'invariance par translation du champ X.

2.2 Théorèmes principaux

2.2.1 Unicité de la construction

Théorème 2.2. ***Unicité de la construction***
L'opérateur limite Q ne dépend pas de la décomposition (i.e. la suite p_n) choisie. Autrement dit, si l'on a deux décompositions d'un même noyau :

$$q(x) = \sum_{i=1}^{+\infty} p_i(x) = \sum_{i=1}^{+\infty} p'_i(x)$$

et l'on note Q (resp. Q') l'opérateur du chaos multiplicatif associé à la décomposition p (resp. p'), alors Q et Q' sont égaux en loi.

Démonstration. On montre ce théorème en plusieurs étapes :
– Chaque mesure σ se décompose en deux mesures de Radon, l'une est dégénérée et l'autre fortement non dégénérée.
– En utilisant le fait que les suites sont "proches" à la limite, on contrôle la différence des opérateurs limites à l'aide de l'inégalité de convexité de Kahane (voir théorème 5.4) et le théorème de De la Vallée Poussin (voir théorème 5.1), on montre que les mesures ont les mêmes mesures dégénérées (resp. fortement non-dégénérées).
– Enfin, encore en utilisant l'inégalité de convexité de Kahane, on montre que pour tout borélien A, $Q\sigma(A)$ et $Q'\sigma(A)$ ont la même loi. Ceci s'étend facilement à une famille de boréliens.
Voici la preuve.

• Étape 1) : Décomposition de la mesure σ.
Étant donnée une mesure de Radon σ positive, on définit

$$\sigma_0(A) = \mathbb{E}[Q\sigma(A)], \sigma_1(A) = \sigma(A) - \sigma_0(A)$$

de sorte que $(Q^n\sigma_0(A))_n$ soit une martingale qui converge dans $\mathcal{L}^1$ (car $\sigma_0(A) = \mathbb{E}[Q\sigma_0(A)]$).
Énonçons ceci sous forme de lemme pour fixer les notations.

Lemme 2.3. *Étant donné un opérateur du chaos multiplicatif gaussien Q, toute mesure $\sigma \in M_+$ peut-être décomposée en une somme de deux mesure $\sigma_0, \sigma_1 \in M_+$ telles que pour tout A borélien de $\mathbb{R}^d$:*
– $\mathbb{E}[Q\sigma_0(A)] = \sigma_0(A)$;
– $\mathbb{E}[Q\sigma_1(A)] = 0$.
Autrement dit,
– $(Q^n\sigma_0(A))_{n\in\mathbb{N}}$ *est une martingale régulière ;*
– Q *est dégénérée en* σ_1.

On dit aussi que σ_0 (resp. σ_1) est la partie fortement non-dégénérée (resp. dégénérée) de σ.

• Étape 2) : Q et Q' ont les mêmes mesures fortement non-dégénérées (resp. dégénérées).
Montrons d'abord que Q et Q' ont les mêmes mesures fortement non-dégénérées : Remarquons que par positivité des suites p_n et p'_n, les sommes partielles sont proches uniformément à l'infini sur tout compact. Ceci est une conséquence du théorème de Dini : si K est un compact de $\mathbb{R}^d$ et $N \in \mathbb{N}$, alors la partie négative $((q_n - q'_N)_-)_n$ décroît et converge vers 0 car la suite $(q_n - q'_N)_n$ converge en décroissant vers $q - q'_N$, et d'après le théorème de Dini, cette convergence est uniforme sur K.
On a donc pour $\epsilon > 0$ fixé,

$$q'_N(x) \leq q_n(x) + \epsilon \tag{1}$$

sur K pour n assez grand.
On a alors, grâce à l'inégalité de convexité de Kahane (théorème 5.4) et (1), pour toute fonction F convexe avec croissance au plus polynomiale à l'infini, tout $A \subset K$ borélien et toute Y variable aléatoire gaussienne centrée réduite indépendante de Q_n :

$$\mathbb{E}[F(Q'_N\sigma(A))] \leq \mathbb{E}[F(Q_n\sigma(A)e^{\sqrt{\epsilon}Y - \frac{\epsilon}{2})}] = \mathbb{E}[F(Q_n\sigma(A))]e^{\frac{(a^2-a)\epsilon}{2}} \tag{2}$$

Supposons maintenant que $Q_n\sigma(A)$ soit uniformément intégrable et montrons que $Q'_n\sigma(A)$ l'est aussi. D'après le théorème de De la Vallée Poussin (théorème 5.1), il existe une fonction F qui est en particulier convexe et une constante positive α telle que $F(\lambda x) \leq \lambda^\alpha F(x)$. Combinant cela avec (2), on obtient

$$\sup_n \mathbb{E}[F|Q'_n|] \leq \sup_n \mathbb{E}[F|Q_n|]e^{\frac{(a^2-a)\epsilon}{2}} < +\infty$$

Et d'après le théorème de De la Vallée Poussin, la martingale $(Q'_n\sigma(A))_n$ est aussi uniformément intégrable.
On vient de montrer :

Lemme 2.4. *Q et Q' ont les mêmes mesures fortement non-dégénérées.*

Montrons maintenant que Q et Q' ont les mêmes mesures dégénérées.
Supposons par l'absurde qu'il existe une mesure σ dégénérée pour Q et non dégénérée pour Q'. D'après le lemme de décomposition de mesure 2.3 appliqué à Q', on peut décomposer σ en somme de deux mesure σ_0 et σ_1 avec σ_0 fortement non-dégénérée pour Q' et σ_1 dégénérée pour Q'. Alors d'après le lemme précédent, σ_0 est aussi fortement non-dégénérée pour Q, mais $Q\sigma_0 \leq Q\sigma = 0$, contradiction.
On vient de montrer :

Lemme 2.5. *Q et Q' ont les mêmes mesures dégénérées.*

• Étape 3) : $Q\sigma$ et $Q'\sigma$ sont égaux en loi.
On revient sur l'équation (2). De façon heuristique, il s'agit de faire tendre ϵ vers 0 pour que la première inégalité dans (2) devienne une égalité, puis se débarrasser de la fonction convexe F pour conclure. Voici maintenant les détails pour un borélien A par souci de simplicité, mais cette preuve se généralise facilement.
En vue de se débarrasser de la fonction convexe F, on va prendre une fonction F qui est en plus **lipschizienne**. D'après une version de l'inégalité de convexité de Kahane (théorème 5.7), on a :

$$\mathbb{E}[F(Q\sigma(A))] = \lim_{n\to+\infty} \uparrow \mathbb{E}[F(Q_n\sigma(A))]$$

Combinant ceci avec (2) donne

$$\forall N, \mathbb{E}[F(Q'_N\sigma(A)] \leq \mathbb{E}[F(Q\sigma(A))]e^{\frac{a^2-a}{2}\epsilon}$$

En passant à la limite lorsque N tend vers ∞ et ϵ vers 0, on a :

$$\mathbb{E}[F(Q'\sigma(A))] \leq \mathbb{E}[F(Q\sigma(A))]$$

En inversant les rôles de Q et Q' on obtient une inégalité dans l'autre sens. Comme les combinaisons linéaires de toutes les fonctions convexes et lipschiziennes engendrent toutes les fonctions régulières à support compact, on vient de montrer :

Lemme 2.6. ***Égalité en loi***
Pour tout borélien A, $Q\sigma(A)$ et $Q'\sigma(A)$ sont égaux en loi.

La preuve s'étend facilement à une famille de boréliens, on conclut que $Q\sigma$ et $Q'\sigma$ ont la même loi. □

2.2.2 Critère de non-dégénéréscence

On se limitera dans la suite au cas où σ est la mesure de Lebesgue sur $\mathbb{R}^d$, et on suppose que q est de la forme $\gamma^2 \log_+ \frac{1}{|x|} + g(x)$ où g est une fonction continue bornée sur $\mathbb{R}^d$.
Ce théorème suivant dû à Kahane [11] est l'un des premiers théorèmes importants de la théorie. Une façon de comprendre l'énoncé est de le voir comme un phénomène de transition de phase.

Théorème 2.7. ***Sur la dégénérescence du chaos multiplicatif gaussien***
On constate l'existence d'un point critique pour la dégénérescence du chaos multiplicatif gaussien :
– Si $\gamma \geq \sqrt{2d}$, le chaos multiplicatif est dégénéré ;
– Si $\gamma < \sqrt{2d}$, le chaos multiplicatif est fortement non-dégénéré sur la mesure de Lebesgue.

Remarque 2.4. *La preuve originale de Kahane en 1985 suppose que q est un noyau de type sigma-positif. Dans la pratique, l'hypothèse de sigma-positivité est délicate à vérifier à chaque fois. Cette généralisation a été traitée par Robert et Vargas dans [24].*

On démontera ce théorème dans la section qui suit.

2.3 Quelques propriétés

2.3.1 Existence des moments positifs

Théorème 2.8. ***Existence des moments positifs***
Dans le cas $\gamma^2 < 2d$, on a $\mathbb{E}[Q(K)^p] < \infty$ ssi $\gamma^2 < \frac{2d}{p}$.

On montre maintenant les théorèmes 2.7 et 2.8 en suivant l'article [11]. On montrera d'abord les résultats analogues dans un cas "discret" selon [12]. On y constate une intuition issue de la théorie de la turbulence, celle du transfert (ou de division) d'énergie de grandes échelles vers les petites échelles que l'on a esquissée au tout début du manuscript.

Démonstration. Schéma de la preuve :
On introduit d'abord le modèle des cascades multiplicatives de Mandelbrot, ensuite on énonce un lemme analogue aux théorèmes précédents dans ce cadre. Puis des techniques d'approximation nous donneront les théorèmes.

• "Cas discret" :
Rappelons la construction du modèle des cascades de Mandelbrot.
Prenons un pavé, disons l'intervalle $[0, 1[$. Prenons un entier c plus grand ou égal à 2. On divise successivement le pavé en $c, c^2, \cdots, c^n, \cdots$ pavés semblables, en divisant chaque pavé de la n-ième génération en c pavés égaux. Par exemple, on pourrait penser à un arbre de Cayley ou bien à l'écriture c-adique d'un réel appartenant à $[0, 1[$.

Définition 2.4. ***Intervalles c-adiques***
On se donne un entier c plus grand ou égal à 2. On note

$$I(j_1, j_2, \cdots, j_n) = [\sum_{k=1}^{n} j_k c^{-k}, \sum_{k=1}^{n} j_k c^{-k} + c^{-n}[$$

les intervalles c-adiques (de l'intervalle $[0, 1[$), où $n = 1, 2, \cdots$ désigne la "génération" et $j_k = 0, 1, \cdots, c-1$ le $(j_k + 1)$-ième descendant de la k-ième génération.

Maintenant on introduit des mesures aléatoires liées à cette division. Prenons la mesure de Lebesgue ν_0 sur le pavé initial. À chaque fois que l'on divise un pavé de la n-ième génération en c petits pavés égaux, on construit la mesure ν_{n+1} sur ces c pavés indépendamment de sorte que la densité de ν_{n+1} par rapport à ν_n soit donnée par la valeur d'un élément d'une suite de variables aléatoires i.i.d. positives d'espérances 1. Formellement :

Définition 2.5. ***Mesures aléatoires sur les pavés***
On se donne une variable aléatoire W positive d'espérance 1. On désigne par $W(j_1, j_2, \cdots, j_n)$ une suite de variables aléatoires indépendantes, chacune ayant la même distribution que W.
On définit alors ν_n la mesure sur $[0, 1[$ dont la densité par rapport à la mesure de Lebesgue sur l'intervalle $I(j_1, j_2, \cdots, j_n)$ est

$$W(j_1)W(j_1, j_2) \cdots W(j_1, j_2, \cdots, j_n)$$

Remarquons qu'alors ν_n est une martingale positive, donc converge p.s. vers une limite que l'on note ν. C'est ν que l'on veut étudier dans la suite. On commence par sa masse totale.
Notons

$$Y_n = ||\nu_n|| = c^{-n} \sum_{j_1, j_2, \cdots, j_n} W(j_1)W(j_1, j_2) \cdots W(j_1, j_2, \cdots, j_n)$$

la masse de la mesure aléatoire ν_n. C'est une martingale positive donc converge p.s. vers une variable aléatoire Y_∞ telle que $\mathbb{E}[Y_\infty] \leq 1$. Remarquons aussi que Y_∞ est la masse totale de ν au sens de la topologie faible.

Lemme 2.9. ***Équation fonctionnelle de cascades***
Par Fubini (ou par construction même), les variables Y_n vérifient une équation récurrente :

$$Y_n = c^{-1} \sum_{j=1}^{c-1} W(j) Y_{n-1}(j)$$

Rappelons que les variables aléatoires $W(j)$ et $Y_{n-1}(j)$ sont mutuellement indépendantes, et les $Y_{n-1}(j)$ ont la même distribution que Y_{n-1}.
Alors Y_∞ est solution de l'équation fonctionnelle suivante :

$$Z = c^{-1} \sum_{j=0}^{c-1} W_j Z_j \tag{3}$$

où les variables aléatoires W_j et Z_j sont mutuellement indépendantes, les W_j ayant la même distribution que W et les Z_j la même distribution que Z.

Le lemme suivant donne un critère d'existence de solutions pour cette équation fonctionnelle. Il donne aussi une condition nécessaire et suffisante d'existence de moment pour Y_∞.

Lemme 2.10. ***Analogues discrets***
On a les résultats suivants :
• *1) Sur la non-dégénérescence :*
Les assertions suivantes sont équivalentes :
a) $\mathbb{E}[Y_\infty] = 1$ *;*
b) $\mathbb{E}[Y_\infty] > 0$ *;*
c) Une solution Z *existe avec* $\mathbb{E}[Z] = 1$ *;*
d) $\mathbb{E}[W \ln W] < \ln c$.
• *2) Sur l'existence des moments :*
Soit $h > 1$. *Supposons que* $\mathbb{P}[W = 1] \neq 1$. *On a* $\mathbb{E}[Y_\infty^h] < +\infty$ *ssi* $\mathbb{E}[W^h] < c^{h-1}$.

Démonstration. Avant de faire la preuve, introduisons une fonction convexe associée à W :

$$\phi(h) = \log_c \mathbb{E}[W^h] - (h-1)$$

(où $\log_c x = \frac{\ln x}{\ln c}$) telle que $\phi(1) = 0$ et $\phi'_{gauche}(1) = \mathbb{E}[W \log_c W] - 1$.
Notons $D = 1 - \mathbb{E}[W \log_c W]$ l'opposé de cette valeur de dérivée, ainsi que α_0 (s'il existe) l'autre point d'annulation de la fonction ϕ.

• Pour 1) :
Visiblement $a)$ implique $b)$ et $b)$ implique $c)$.
Supposons alors $c)$. Soit alors Z une solution de (3). Par récurrence sur n, il existe une suite de v.a. indépendantes $W(j_1, j_2, \cdots, j_n)$ (comme dans la définition 2.5) ayant la même distribution que W et une suite de v.a. $Z(j_1, j_2, \cdots, j_n)$ ayant chacune la même distribution que Z, indépendantes des $W(i_1, i_2, \cdots, i_k)$ lorsque $k \leq n$, telles que, pour tout n :

$$Z = c^{-n} \sum_{j_1, \cdots, j_n} W(j_1) W(j_1, j_2) \cdots W(j_1, j_2, \cdots, j_n) Z(j_1, j_2, \cdots, j_n)$$

Alors l'espérance conditionelle de Z par rapport à la tribu engendrée par les $W(j_1, \cdots, j_k)$ $(k \leq n)$ est Y_n dans la définition 2.5. Il en découle que la martingale Y_n est uniformément intégrable et que $Z = Y_\infty$ p.s. (et donc $Z \geq 0$ p.s.).
On vient de montrer que $c)$ implique $a)$. Donc $a)$, $b)$, et $c)$ sont équivalentes.
Supposons encore $c)$ et montrons que ceci implique $d)$. Partant de (3), on a par l'inégalité de Minkowski, pour $0 < h < 1$:

$$\mathbb{E}[c^h Z^h] \leq \sum_{j=0}^{c-1} \mathbb{E}[(W_j Z_j)^h] = c\mathbb{E}[W^h]\mathbb{E}[Z^h]$$

avec $0 < \mathbb{E}[Z^h] \leq 1$. La fonction $\phi(h)$ est par conséquent positive sur $[0,1]$, donc $D \geq 0$.
On doit améliorer cette estimation pour avoir d). Voici quelques lemmes élémentaires :

Lemme 2.11. ***Amélioration de l'inégalité de Minkowski***
$(x+y)^h \leq x^h + hy^h$ *si* $x \geq y > 0$ *et* $0 < h < 1$.

Ceci est une conséquence du théorème des accroissements finis.

Lemme 2.12. *Soient X une variable aléatoire positive intégrable et X' une copie indépendante de X. Il existe alors un nombre $\epsilon_X > 0$ tel que*

$$\mathbb{E}[X^h \mathbf{1}_{\{X' \geq X\}}] \geq \epsilon_X \mathbb{E}[X^h]$$

pour $0 \leq h \leq 1$.

C'est parce que $\frac{\mathbb{E}[X^h \mathbf{1}_{\{X' \geq X\}}]}{\mathbb{E}[X^h]}$ est une fonction continue positive de h strictement positive sur le compact $[0,1]$.
Toujours par sous-additivité de $x \mapsto x^h$ pour $h \in [0,1[$, on a, partant de (3), presque sûrement,

$$c^h Z^h \leq \sum_{j=0}^{c-1} W_j^h Z_j^h$$

Le premier des deux lemmes précédents nous dit que si $W_1 Z_1 \geq W_0 Z_0$ alors

$$c^h Z^h \leq h W_0^h Z_0^h + \sum_{j=1}^{c-1} W_j^h Z_j^h$$

donc

$$\mathbb{E}[c^h Z^h] \leq \sum_{j=0}^{c-1} \mathbb{E}[W_j^h Z_j^h] - (1-h)\mathbb{E}[W_0^h Z_0^h \mathbf{1}_{\{W_1 Z_1 \geq W_0 Z_0\}}]$$

et alors le second des deux lemmes précédents nous apprend que

$$\mathbb{E}[c^h Z^h] \leq \mathbb{E}[W^h]\mathbb{E}[Z^h] - (1-h)\epsilon_{WZ}\mathbb{E}[W^h]\mathbb{E}[Z^h]$$

et donc, en divisant par $\mathbb{E}[Z^h]$ et en prenant les logarithmes,

$$\phi(h) + \log_c(1 - \frac{(1-c)\epsilon_{WZ}}{c}) \geq 0$$

valable pour $h \in [0,1]$.
On en déduit que $D > 0$ en prenant les dérivées. Ceci nous montre que c) implique d).

Il ne reste qu'à montrer, par exemple $d)$ implique $b)$ pour terminer cette première partie de la preuve.
Voici une autre amélioration de l'inégalité de Minkowski :

Lemme 2.13. ***Amélioration de l'inégalité de Minkowski bis***
$(x+y)^h \geq x^h + y^h - 2(1-h)(xy)^{\frac{h}{2}}$ pour $x > 0$, $y > 0$ et $h_0 < h < 1$ (avec, par exemple, $h_0 = 1 - \frac{\sqrt{3}}{3}$).
Comme corollaire, on a

$$(\sum_{j=1}^{c} x_j)^h \geq \sum_{j=1}^{c} x_j^h - 2(1-h)\sum_{i<j}(x_i x_j)^{\frac{h}{2}}$$

pour $x_j > 0$ $(j = 1, 2, \cdots, c)$ et $h_0 < h < 1$.

Le corollaire s'obtient par récurrence en utilisant la sous-additivité de la fonction $x \mapsto x^{\frac{h}{2}}$ pour $0 < h < 1$. En effet :

$$(\sum_{j=1}^{c} x_j)^h \geq x_1^h + (\sum_{j=2}^{c} x_j)^h - 2(1-h)x_1^{\frac{h}{2}}(\sum_{j=2}^{c} x_j)^{\frac{h}{2}} \geq \sum_{j=1}^{c} x_j^h - 2(1-h)\sum_{j>1}(x_1 x_j)^{\frac{h}{2}}$$

Montrons alors le lemme. Ceci est encore un exercice sur les fonctions élémentaires. On pose $f(t) = e^{th} + e^{-th} - (e^t + e^{-t})^h$. En divisant par $(xy)^{\frac{h}{2}}$ de chaque côtés, on voit qu'il suffit de montrer que $\sup_t f_t \leq 2(1-h)$ quand $h < 1$ est assez proche de 1. Il est facile de voir que $f(t)$ a un minimum local en $t = 0$ et tend vers 0 quand $t \to +\infty$. Aux points $t \neq 0$ où f' s'annule, $f(t) = 2\frac{e^{(1-h)t} - e^{-(1-h)t}}{e^t - e^{-t}}$.
On s'intéresse alors à la fonction $g(\epsilon) = e^{\epsilon t} - e^{-\epsilon t} - \epsilon(e^t - e^{-t})$. Il suffit de montrer que $g(\epsilon) \leq 0$ quand ϵ est proche de 0. En dérivant on voit que quand $\epsilon < \frac{\sqrt{3}}{3}$, $g(\epsilon) \leq 0$. D'où le lemme.
Appliquons le corollaire du lemme précédent avec $x_{j+1} = W_j X_j$ où $W_j = W(j)$ et $X_j = Y_{n-1}(j)$ à l'équation

$$Y = c^{-1}\sum_{j=0}^{c-1} W_j X_j \tag{4}$$

où $Y = Y_n$.
On obtient

$$c^h Y^h \geq \sum_{j=0}^{c-1} W_j^h X_j^h - 2(1-h)\sum_{i<j} W_i^{\frac{h}{2}} W_j^{\frac{h}{2}} X_i^{\frac{h}{2}} X_j^{\frac{h}{2}}$$

et en prenant les espérances et en revenant aux notation initiales :

$$\mathbb{E}[Y_n^h] \geq c^{1-h}\mathbb{E}[W^h]\mathbb{E}[Y_{n-1}^h] - c^{1-h}(c-1)(1-h)(\mathbb{E}[W^{\frac{h}{2}}])^2(\mathbb{E}[Y_{n-1}^{\frac{h}{2}}])^2$$

Or, on a $\mathbb{E}[Y_n^h] \leq \mathbb{E}[Y_{n-1}^h]$ par l'inégalité de Jensen, donc

$$\mathbb{E}[Y_n^h](c^{\phi(h)-1}) \leq c^{1-h}(c-1)(1-h)(\mathbb{E}[Y_{n-1}^{\frac{h}{2}}])^2$$

et en faisant tendre h vers 1, on obtient

$$D \ln c \leq (c-1)(\mathbb{E}[Y_{n-1}^{\frac{1}{2}}])^2$$

Par uniforme intégrabilité de la famille des $Y_n^{\frac{1}{2}}$ (car $\mathbb{E}[Y_n] = 1$), on a $\mathbb{E}[Y_\infty^{\frac{1}{2}}] = \lim_{n\to\infty} \mathbb{E}[Y_n^{\frac{1}{2}}]$.
Ainsi, $\mathbb{E}[Y_\infty^{\frac{1}{2}}] \neq 0$. Ceci entraîne bien b) et on a terminé la première partie de la preuve.

• Pour 2) :
Supposons d'abord l'existence d'une solution Z à l'équation (3) telle que $\mathbb{E}[Z^h] < +\infty$ pour $h > 1$ donné.
Sous l'hypothèse $\mathbb{P}[W = 1] \neq 1$, on a

$$c^h Z^h \geq \sum_{j=0}^{c-1} (W_j Z_j)^h$$

où l'inégalité est stricte sur un évènement de probabilité non nulle. Sur cet évènement, on a

$$c^h \mathbb{E}[Z^h] > c\mathbb{E}(W^h)\mathbb{E}[Z^h]$$

soit $\mathbb{E}[W^h] < c^{h-1}$.
Réciproquement, supposons que $\mathbb{E}[W^h] < c^{h-1}$ (i.e. $\phi(h) < 0$) et soit k l'entier tel que $k < h \leq k+1$. Alors on a, pour $x_j \geq 0$,

$$(x_1 + x_2 + \cdots + x_c)^h \leq (x_1^{\frac{h}{k+1}} + \cdots + x_c^{\frac{h}{k+1}})^{k+1} = x_1^h + \cdots + x_c^h + \cdots$$

Reprenons la formule (4). On obtient :

$$c^h \mathbb{E}[Y^h] \leq c\mathbb{E}[W^h]\mathbb{E}[X^h] + (c^{k+1} - c)\mathbb{E}[W^k]\mathbb{E}[X^k]$$

d'où, en utilisant $\mathbb{E}[Y_n^h] \geq \mathbb{E}[Y_{n-1}^h]$ (par Jensen) et en divisant par c^h :

$$\mathbb{E}[Y_n^h](1 - c^{1-h}\mathbb{E}[W^h]) \leq c\mathbb{E}[W^k]\mathbb{E}[Y_\infty^k]$$

car $\frac{c^{k+1}-c}{c^h} \leq c$.
En faisant tendre n vers l'infini, on voit que si $\mathbb{E}[Y_\infty^k] < +\infty$ alors $\mathbb{E}[Y_\infty^h] < +\infty$.
Donc pour $1 < h \leq 2$, c'est gagné.
Maintenant supposons que $h > 2$.
Par convexité, $\phi(h) < 0$ entraîne $\phi(l) < 0$ pour tout (entier) $l \leq h$. Donc $\mathbb{E}[Y_\infty^{l-1}] < +\infty$ implique $\mathbb{E}[Y_\infty^l] < +\infty$ pour tout $l = 2, \cdots, k$. Ceci termine la preuve. □

En voici une application dans un cas intéressant pour nous.
Prenons $T = \{1, 2, \ldots, c\}^{\mathbb{N}}$ avec $c \in \mathbb{N}^*$ muni de la distance c-adique

$$d(s,t) = c^{-d.\sup\{N \in \mathbb{N} : \forall k \leq N, \pi_k(t) = \pi_k(s)\}}$$

avec

$$p_n(t,s) = \begin{cases} u \text{ si } dist(t,s) \leq c^{-nd} \\ 0 \text{ si } dist(t,s) > c^{-nd} \end{cases}$$

On remarque alors que le poids $p_n(t)$ est p.s. constant sur chacun des c^n cylindres prescrits par ses n-premières coordonnées : on note dorénavant $I_n(t)$ celui parmi ces cylindres contenant t, les valeurs de $p_n(t)$ sur les cylindres disjoints sont indépendantes. On définit alors le noyau

$$q(t,s) = \sum_{n=1}^{\infty} p_n(t,s) = -u \frac{\ln d(t,s)}{\ln c}$$

ainsi que l'opérateur Q associé.
Choisissons comme mesure σ la mesure équidistribuée sur T, i.e. telle que $\sigma(I_n(t)) = c^{-n}$. Le lemme précédent donne alors dans ce cas :

Lemme 2.14. ***Cas de l'arbre***
Un tel opérateur Q est dégénéré en σ si $u \geq 2 \ln c$, et fortement non-dégénéré en σ si $u < 2 \ln c$.
De plus, $\mathbb{E}[Q(\sigma(T))^h] < +\infty$ ssi $uh < 2 \ln c$.

C'est cette version du lemme que l'on va utiliser dans la suite.

• "Cas continu" :
Revenons à notre chaos multiplicatif gaussien. Rappelons que l'on se place toujours dans le cas d'un noyau de la forme $u \ln^+ \frac{1}{|t-s|} + O(1)$ avec $u = \lambda^2$ et $t, s \in \mathbb{R}^d$.
On prend d'abord un ensemble totalement discontinu K dans $\mathbb{R}^d$ contruit de façon analogue à l'ensemble de Cantor :
– On prend une suite décroissante de compacts emboîtés $(K_n)_{n \in \mathbb{N}}$ telle que chaque K_n admette exactement c^n composantes connexes, chacune ayant un diamètre plus petit que d_n, et les distances mutuelles sont plus grandes que δ_n.
– Chaque composante de K_n contient exactement c composantes de K_{n+1}.
– K est défini comme l'intersection des K_n.
On suppose de plus que (lorsque $n \to +\infty$ pour δ_n)

$$d_n \leq c^{-\frac{n}{\alpha}}, \delta_n \geq c^{-\frac{n}{\alpha + o(1)}} \tag{5}$$

Soit σ la mesure qui donne la masse c^{-n} à chaque composante de K_n.
On a, dans ce cas :

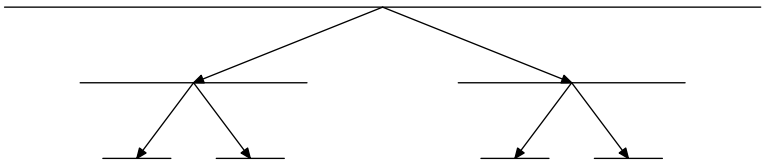

FIGURE 3 – Construction de la suite K_n à la Cantor

Lemme 2.15. ***Cas cascades***
L'opérateur du chaos multiplicatif gaussien Q est dégénéré sur σ si $u \geq 2\alpha$ et fortement non dégénéré si $u \leq 2\alpha$.
On a en plus $\mathbb{E}[Q\sigma(K)^h] \leq +\infty$ ssi $uh \leq 2\alpha$.

Preuve du lemme :
La preuve est une réécriture du cas discret expliqué plus haut.
Supposer d'abord que $\delta_{n+1} \geq \lambda c^{-n}$ avec $\lambda > 0$ une constante (par exemple si K est réunion de c portions qui lui sont semblables dans le même rapport $c^{-\alpha}$ construites par auto-similarité).
Choisissons un tel compact noté K_α^c. On peut alors identifier le compact T précédent avec K_α^c, en transportant les cylindres prescrits par les n premières coordonnées sur les composantes de K_n. Or on peut comparer la distance ultra-métrique sur l'arbre T avec la distance euclidienne sur K :

$$\lambda(d(t,s))^\alpha \leq |t-s| \leq (d(t,x))^\alpha$$

Remarquons que σ est invariante par cette identification (car $\sigma(I_n(t) = c^{-n})$). Le noyau $q(t,s)$ vérifie, via cette identification :

$$q(t,s) = \frac{u}{\alpha \ln c} \ln|t-s| + O(1)$$

et la conclusion dans ce cas en découle à cause de l'application dans le cas discret plus haut.
Maintenant dans le cas général, avec la condition 5, on voit que K s'obtient à partir de K_α^c par contraction, mais aussi que $K_{\alpha+\epsilon}^c$ s'obtient à partir de K par contraction locale. Ceci suffit pour établir le résultat énoncé.

Arrivant à la fin de la démonstration de ce lemme, on est en mesure de démontrer nos théorèmes. L'idée est de construire un ensemble de Cantor K proche de son "intervalle" de départ (au sens de la mesure) K_0.
Sans perte de généralité, on prend $K_0 \subset [0,1[^d$ et m la mesure de Lebesgue sur K. Prenons $c = 2^d$. On construit les K_n comme précédemment, de sorte que chacune de ses c^n composantes soit homothétique à K_0 dans le rapport $\rho_n = r_1 r_2 \cdots r_n$,

avec $r_k \in]0, \frac{1}{2}[$. Si chaque r_k est suffisamment proche de $\frac{1}{2}$ (mais pas trop pour que l'on ait toujours (5)), le compact K a pour mesure de Lebesgue arbitrairement proche de m, donc par le lemme précédent, on a obtenu le théorème. □

2.3.2 Non-linéarité du spectre puissance

Théorème 2.16. ***Caractère multifractal***
Pour tout $p \geq 0$ tel que Q admette un moment d'ordre p, il existe une constante $D_p > 0$ telle que, quand $t \to 0$,

$$\mathbb{E}[Q(tA)^p] \to D_p t^{\xi(p)}$$

où A est un ouvert borné non vide et pour tout $p \in \mathbb{R}$, $\xi(p) = (d + \frac{\gamma^2}{2})p - \frac{\gamma^2}{2}p^2$.

Démonstration. On peut supposer A est inclus dans $[0,1]^d$.
Pour $0 < t < 1$, on note $\bar{Q}^t$ le chaos associé au noyau $q(\cdot/t)$. Remarquons que $\bar{Q}^t(tA) = t^d Q(A)$ en loi.
On veut comparer les deux chaos Q et $\bar{Q}$. Définissons

$$g_t = \sup_{|r| \leq t} |g(r) - g(r/t)|$$

et remarquons que pour tout $|r| \leq t$,

$$q(r) \geq q(r/t) + \gamma^2 \log \frac{1}{t} - g_t$$

Soit $p \geq 1$. Grâce à l'inégalité de convexité de Kahane (théorème 5.4), on a

$$\mathbb{E}[Q(tA)^p] \geq \mathbb{E}[(e^{\sqrt{\gamma \log \frac{1}{t} - g_t} Y - \frac{1}{2}(\gamma^2 \log \frac{1}{t} - g_t)} \bar{Q}^t(tA))^p]$$

où Y suit une loi normale centrée réduite indépendante de $\bar{Q}^t$. On a alors

$$\mathbb{E}[Q(tA)^p] \geq \mathbb{E}[Q(A)^p] t^{dp} e^{\frac{(p^2-p)(\gamma^2 \log \frac{1}{t} - g_t)}{2}} = \mathbb{E}[Q(A)^p] t^{\xi(p)} e^{-\frac{(p^2-p)g_t}{2}}$$

En utilisant le fait que $g_t \to 0$ quand $t \to 0$, on a alors, quand $t \to 0$,

$$\mathbb{E}[Q(tA)^p] \geq \mathbb{E}[Q(A)^p] t^{\xi(p)}$$

Avec la même méthode mais en remplaçant g_t par $-g_t$, on peut montrer une inégalité du même type dans l'autre sens. D'où le résultat pour $p \geq 1$.
Le cas $p < 1$ se démontre en suivant exactement les mêmes idées. On remarque que comme $x \mapsto x^p$ est cette fois-ci concave, les inégalités changent de signes mais le résultat reste valable. □

3 Étude du cas critique

Dans la suite de ce mémoire, on se place dans le cas suivant : σ est la mesure de Lebesgue sur $\mathbb{R}^d$, et on considère, $\forall \gamma \geq 0$,

$$M^\gamma(dx) = \lim_{t\to\infty} M_t^\gamma(dx) = \lim_{t\to\infty} e^{\gamma X_t(x) - \frac{\gamma^2}{2}\mathbb{E}[X_t(x)^2]} dx$$

avec X un processus gaussien centré stationnaire défini sur (un domaine ouvert de) $\mathbb{R}^d$ avec X_t une suite de champs gaussiens approximant X (au sens où le noyau de covariance K de X et limite des noyaux K_t de X_t, voir la section précédente pour la définition du chaos multiplicatif gaussien).
On a vu dans la section précédente que le point $\gamma = \sqrt{2d}$ est un point critique (au sens où l'on y constate un phénomène de transition de phases) pour un noyau de la forme $\gamma^2 \log_+ \frac{1}{|x|} + g(x)$ où g est une fonction continue bornée sur $\mathbb{R}^d$. Il est souvent très intéressant d'étudier ce qui se passe lorsque l'on passe de l'un côté à l'autre du point critique, mais dans notre cas, la situation se simplifie car on sait déjà :

Théorème 3.1. ***Rappel sur le cas de dégénérescence de la mesure limite*** *Pour $\gamma \geq 2d$, p.s. $\lim_{t\to\infty} M_t^{\sqrt{2d}}(dx) = 0$.*

En revanche pour $\gamma < 2d$, la mesure limite M^γ est p.s. non-triviale.
Dans l'article récent [6], Duplantier, Rhodes, Scheffield et Vargas ont réussi à contruire une théorie analogue à la théorie de Kahane dans le cas sous-critique. Ils se sont intéressés à la martingale dérivée "en faisant la différentielle par rapport au paramètre γ" :

$$M'(A) = -\frac{\partial}{\partial\gamma}[M_\gamma(A)]_{\gamma=\sqrt{2d}} = [\int_A (\gamma\mathbb{E}[X(x)^2] - X(x)) e^{\gamma X(x) - \frac{\gamma^2}{2}\mathbb{E}[X(x)^2]} dx]_{\gamma=\sqrt{2d}}$$

Remarquons que cette martingale n'est pas a priori positive, l'existence même de la limite n'est pas évidente en soi.
Un exemple d'application spétaculaire a été l'article [7], dans lequel les mêmes auteurs, en étudiant les moments de cette martingale dérivée, ont réussi à établir la formule de Knizhnik-Polyakov-Zamolodchikov (KPZ) au point critique.
Le but de cette section est de rappeler la construction de la martingale dérivée pour la chaos multiplicatif gaussien au point critique de l'article [6]. Il est à noter qu'il y a de fortes connections avec le processus du branchement, malheureusement on ne traite pas cela spécifiquement dans ce rapport.

3.1 Construction de la martingale dérivée

On pose formellement la définition de la martingale dérivée :

Définition 3.1. ***Martingale dérivée du chaos multiplicatif gaussien***
Au voisinage du point critique $\gamma = \sqrt{2d}$, on introduit la martingale dérivée

$$M_t'(dx) = (\sqrt{2d}\mathbb{E}[X_t(x)^2] - X_t(x))e^{\sqrt{2d}X_t(x) - d\mathbb{E}[X_t(x)^2]}dx$$

Dans [6], on se propose d'étudier une classe particulière de processus gaussiens centrés stationnaires à accroissements indépendants $((X_t(x))_{x\in\mathbb{R}})_{t\geq 0}$ dont les fonctions de covariance sont de la forme :

$$K_t(x) = \mathbb{E}[X_t(0)X_t(x)] = \int_1^{e^t} \frac{k(ux)}{u}du$$

avec k un noyau de covariance de classe C^1 à support compact satisfaisant $k(0) = 1$. Remarquons tout de suite que sous ces conditions, en chaque point x, le processus $X_t(x)$ est un mouvement brownien réel standard.
Dans [6], le résultat suivant a été démontré :

Théorème 3.2. ***Convergence de la martingale dérivée***
Pour tout ouvert borné $A \in \mathbb{R}^d$, la martingale $(M_t'(A))_{t\geq 0}$ converge p.s. vers une variable aléatoire p.s. strictement positive que l'on notera $M'(A)$. En plus cette mesure limite est à support plein et sans atome.

Avant de faire la preuve, discutons un peu sur le noyau K et expliquons ainsi la méthode principale utilisée dans [6] dite de cut-off.
Le fait de pouvoir écrire le noyau K sous forme d'intégrale par rapport au temps nous dit immédiatement que le processus X est à accroissements indépendants, i.e. le processus $(X_t(x) - X_s(x))_{t>s}$ est indépendant de $((X_u(x))_{x\in\mathbb{R}^d})_{u\leq s}$. En plus, quand on impose la condition d'être à support compact à k, on observe un phénomène de décorrélation quand le temps t évolue, à savoir, pour $s < t$, les processus $(X_t(w) - X_s(w))_{w\in A}$ et $(X_t(x) - X_s(x))_{x\in B}$ sont indépendants dès que $dist(A, B) \geq e^{-s}$. Cette propriété nous apporte une information précieuse sur le comportement de notre processus, à savoir le fait de pouvoir trouver un moment de cut-off pour un couple de points (x, w), c'est à dire un moment $s_0(x, w)$ au-delà duquel l'évolution au point w ne dépend plus de l'évolution au point x. Ceci nous permet ainsi d'écrire le processus $(X_s(w))_{s_0\leq s\leq t}$ comme

$$X_s(w) = X_{s_0}(w) + W_{s-s_0}$$

où W est un mouvement brownien stardard indépendant du processus $(X_s(x))_{0\leq s\leq t}$ et du processus $(X_s(w))_{0\leq s\leq s_0}$.
On va donc exploiter cette propriété et prouver ce théorème dans ce qui suit. Il est à noter que l'hypothèse d'être à support compact sur k n'est pas essentielle et peut être affaiblie, ce qui est l'objet de la section 4.

3.2 Preuve du théorème 3.2

On présente maintenant la preuve originale de [6].
Stratégie de la preuve :
La martingale dérivée n'est pas positive, on ne peut pas dire directement qu'elle converge vers une limite (aléatoire) positive. On définit, pour $\mathcal{F}_t = \sigma\{X_s(x); s \leq t, x \in \mathbb{R}^d\}$, $A \in \mathbb{R}^d$ borélien et $t, \beta > 0$, les variables aléatoires :

$$Z_t^\beta(A) = \int_A (\sqrt{2d}t - X_t(x) + \beta)\mathbf{1}_{\{\tau^\beta > t\}} e^{\sqrt{2d}X_t(x) - d\mathbb{E}[X_t(x)^2]} dx$$

et

$$\tilde{Z}_t^\beta(A) = \int_A (\sqrt{2d}t - X_t(x))\mathbf{1}_{\{\tau^\beta > t\}} e^{\sqrt{2d}X_t(x) - d\mathbb{E}[X_t(x)^2]} dx$$

où τ^β est un $(\mathcal{F}_t)_t$-temps d'arrêt défini pour tout $x \in A$ par

$$\tau^\beta = \inf\{u > 0, X_u(x) - \sqrt{2d}u > \beta\}$$

Remarquons tout de suite que l'intégrant dans l'expression de $Z_t^\beta(A)$ est positif. Ces variables aléatoires servent à contrôler les parties négatives de l'intégrant dans la définition de la martingale dérivée M' en le coupant au niveau β. Le but est de démontrer que $Z_t^\beta(A)$ qui est positive converge (en t) vers une variable aléatoire $Z^\beta(A)$ qui converge (en β) vers la limite (en t) de $M'_t(A)$. La preuve se fait en passant par $\tilde{Z}_t^\beta(A)$: en effet, on montre que
– La différence entre $Z_t^\beta(A)$ et $\tilde{Z}_t^\beta(A)$ converge p.s. vers 0 quand $t \to +\infty$;
– $\tilde{Z}_t^\beta(A)$ et $M'_t(A)$ sont identiques pour β assez grand.
Entrons maintenant dans les détails de la preuve.

• Quelques vérifications et lemmes préparatoires :
On montre d'abord que $(Z_t^\beta(A))_{t\geq 0}$ est une $\mathcal{F}_t$-martingale continue positive. Elle converge donc p.s. vers une variable aléatoire positive que l'on note $Z^\beta(A)$.
Rappelons que $(X_t(x)_{t\geq 0}$ est un mouvmement brownien standard. Par le théorème de Girsanov, on peut éliminer la partie $\sqrt{2d}t$ (la partie drift) :

$$\mathbb{E}[(\sqrt{2d}t - X_t(x) + \beta)\mathbf{1}_{\{\tau^\beta > t\}} e^{\sqrt{2d}X_t(x) - d\mathbb{E}[X_t(x)^2]}] = \mathbb{E}[(-X_t(x) + \beta)\mathbf{1}_{\{\tau > t\}}]$$

où τ est un $(\mathcal{F}_t)_t$-temps d'arrêt défini par

$$\tau = \inf\{u > 0, X_u(x) > \beta\}$$

Il suffit de montrer que

Lemme 3.3.

$$\mathbb{E}[(-X_t(x) + \beta)\mathbf{1}_{\{\tau > t\}} | \mathcal{F}_s] = \mathbb{E}[(-X_s(x) + \beta)\mathbf{1}_{\{\tau > s\}}]$$

Par la propriété de Markov (faible) du mouvement brownien, on a, en notant W un mouvement brownien standard indépendant de X,

$$\begin{aligned}
&\mathbb{E}[(-X_t(x)+\beta)\mathbf{1}_{\{\tau>t\}}|\mathcal{F}_s] \\
&= \mathbb{E}[(-X_t(x)+\beta)\mathbf{1}_{\{\sup_{u\in[0,t]} X_u(x)\leq\beta\}}|\mathcal{F}_s] \\
&= \mathbb{E}[(-X_s(x)-W_{t-s}(x)+\beta)\mathbf{1}_{\{\sup_{u\in[0,s]} X_u(x)\leq\beta\}}\mathbf{1}_{\{\sup_{u\in[s,t]} X_s(x)+W_{t-s}(x)\leq\beta\}}|\mathcal{F}_s] \\
&= \mathbb{E}[(-X_s(x)+\beta)\mathbf{1}_{\{\tau>s\}}]
\end{aligned}$$

en appliquant le théorème d'arrêt à W (et la filtration associée) en considérant le temps d'arrêt $\tilde{\tau} = \inf\{W_{t-s} > \beta - X_s(w)\}$.

• Sur l'uniforme intégrabilité de la martingale $Z_t^\beta(A)$:
Sans perte de généralité, on fait quelques hypothèses qui simplient les calculs :
On suppose que le support de k est dans $B(0,1)$ et $A \subset B(0,\frac{1}{2})$ (car tout compact admet un recouvrement par des boules de rayon $\frac{1}{2}$).
On suppose aussi que $x.\nabla k(x) \leq 0$. Cette dernière condition est vraie au moins sur un voisinage de 0 par le caratère défini positif du noyau k. Quitte à reduire la taille de A, on suppose que ceci est vrai sur tout ouvert A.
Écrivons pour tout $x \in \mathbb{R}^d$,

$$f_t^\beta(x) = (\sqrt{2d}t - X_t(x) + \beta)\mathbf{1}_{\{\tau^\beta>t\}}e^{\sqrt{2d}X_t(x)-d\mathbb{E}[X_t(x)^2]}$$

de sorte que $Z_t^\beta(A) = \int_A f_t^\beta(x)dx$.
On définit ensuite une nouvelle mesure de probabilité sur $\mathcal{B}(A)\otimes\mathcal{F}_t$:

$$d\Theta_t^\beta = \frac{1}{|A|\beta} f_t^\beta(x)dxd\mathbb{P}$$

et notons $\Theta(\cdot|\mathcal{G})$ (resp. $\Theta(\cdot|y)$) l'espérance conditionnelle par rapport à $\mathcal{G}$ sous-σ-algèbre de $\mathcal{B}(A)\otimes\mathcal{F}_t$ (resp. la σ-algèbre engendrée par la variable aléatoire $\mathcal{B}(A)\otimes\mathcal{F}_t$-mesurable y) de sorte que $d\Theta_t^\beta(\cdot|x) = \frac{1}{\beta}f_t^\beta(x)d\mathbb{P}$.
Rappelons que (voir le rappel 5.2) sous $\Theta_t^\beta(\cdot|x)$, la loi du processus $(X_s(x)-\sqrt{2d}s-\beta)_{s\leq t}$ est la même que celle de $(-\beta_s)_{s\leq t}$ avec $(\beta_s)_{s\leq t}$ un processus de Bessel en dimension 3 issu de β.
Pour montrer l'uniforme intégrabilité de $(Z_t^\beta(A))_t$, on souhaite établir :

$$\lim_{\delta\to+\infty}\limsup_{t\to+\infty}\mathbb{E}[Z_t^\beta(A)\mathbf{1}_{\{Z_t^\beta(A)>\delta\}}] = 0$$

Or, comme

$$\mathbb{E}[Z_t^\beta(A)\mathbf{1}_{\{Z_t^\beta(A)>\delta\}}] = \beta|A|\Theta_t^\beta(Z_t^\beta(A)>\delta)$$

il suffit de montrer que

$$\lim_{\delta\to+\infty}\limsup_{t\to+\infty}\Theta_t^\beta(Z_t^\beta(A)>\delta)=0$$

Afin d'utiliser la propriété du cut-off, on écrit, en découpant A en $B(x,e^{-t})$ et son complémentaire :

$$\begin{aligned}
\Theta_t^\beta(Z_t^\beta(A)>\delta) &= \frac{1}{|A|}\int_A \Theta_t^\beta(Z_t^\beta(A)>\delta|x)dx\\
&= \frac{1}{|A|}\int_A \Theta_t^\beta(\Theta_t^\beta(Z_t^\beta(A)>\delta|x,(X_s(x))_{s\le t})|x)dx\\
&\le \epsilon+\frac{1}{|A|}\int_A \Theta_t^\beta(\Theta_t^\beta(Z_t^\beta(A)>\delta|x,(X_s(x))_{s\le t},\mathbf{B})|x)dx\\
&\le \epsilon+\frac{1}{|A|}\int_A \Theta_t^\beta(\Theta_t^\beta(Z_t^\beta(B(x,e^{-t}))>\frac{\delta}{2}|x,(X_s(x))_{s\le t},\mathbf{B})|x)dx\\
&\quad+\frac{1}{|A|}\int_A \Theta_t^\beta(\Theta_t^\beta(Z_t^\beta(B(x,e^{-t})^c)>\frac{\delta}{2}|x,(X_s(x))_{s\le t},\mathbf{B})|x)dx\\
&= \epsilon+\Sigma_1+\Sigma_2
\end{aligned}$$

où $\mathbf{B}$ est un évènement de probabilité au moins $1-\epsilon$ (qui nous servira pour contrôler les chemins du processus de Bessel β) que l'on choisit grâce au lemme de Motoo, voir 5.3 :

$$\mathbf{B}=\{\forall t\ge 0,\frac{\sqrt{t}}{R(\ln(2+t))^2}\le\beta_t\le R(1+\sqrt{t\ln(1+t)})\}$$

avec R assez grand.
Pour formaliser notre intuition sur le cut-off, on énonce un lemme de projection qui nous donne la loi conditionnelle de $(X_s(w))_{s\le t}$ sachant celle de $(X_s(x))_{s\le t}$.

Lemme 3.4. ***Un lemme de projection***
Pour tout couple $w\neq x$ et pour t, $(X_s(w))_{s\le t}$ s'écrit comme :

$$X_s(w)=P_s^{x,w}+Z_s^{x,w}$$

en loi, où
– $P_s^{x,w}=-\int_0^s g_{x,w}(u)X_u(x)du+\frac{\partial K_s(x-w)}{\partial s}X_s(x)$ *est $\sigma\{(X_s(x))_{s\le t}\}$-mesurable avec* $g_{x,w}(u)=\frac{\partial^2 K_u(x-w)}{\partial u^2}$ *;*
– $(Z_s^{x,w})_{s\le t}$ *un processus gaussien centré indépendant de $\sigma\{(X_s(x))_{s\le t}\}$ dont la structure de covariance est donnée par*

$$q_{x,w}(s,s')=\mathbb{E}[Z_{s'}^{x,w}Z_s^{x,w}]=\min(s,s')-\int_0^{\min(s,s')}(\frac{\partial K_u(x-w)}{\partial u})^2du$$

On vérifie par un calcul de covariance la validité de cette décomposition.
Maintenant on explique comment contrôler Σ_1 et Σ_2.

∘ Pour Σ_2 :
Rappelons que l'on a défini $s_0 = \ln \frac{1}{|x-w|}$ l'instant de cut-off : c'est l'instant à partir duquel l'évolution de $(X_s(w) - X_{s_0}(w))_{s_0 \leq s \leq t}$ devient indépendante du processus $(X_s(x))_{0 \leq s \leq t}$. On écrit donc, sous Θ_t^β, le processus $(X_s(w))_{s_0 \leq s \leq t}$ comme

$$X_s(w) = X_{s_0}(w) + W_{s-s_0}$$

où W est un mouvement brownien stardard indépendant du processus $(X_s(x))_{0 \leq s \leq t}$ et du processus $(X_s(w))_{0 \leq s \leq s_0}$.
On a donc par le théorème d'arrêt (voir le lemme 3.3) :

$$\begin{aligned}
&\Theta_t^\beta(f_t^\beta(w)|x, (X_s(x))_{0 \leq s \leq t}) \\
&= \frac{1}{\beta}\mathbb{E}[(\sqrt{2d}s_0 - X_{s_0}(w) + \beta)\mathbf{1}_{\{\sup_{u \in [0,s_0]} (X_u(w) - \sqrt{2d}u) \leq \beta\}} e^{\sqrt{2d}X_{s_0}(w) - ds_0}|x, (X_s(x))_{0 \leq s \leq t}]
\end{aligned}$$

En utilisant le lemme de projection 3.4, on a :

$$\begin{aligned}
&\Theta_t^\beta(f_t^\beta(w)|x, (X_s(x))_{0 \leq s \leq t}) \\
&= \frac{1}{\beta}\mathbb{E}[(\sqrt{2d}s_0 - P_{s_0}^{x,w} - Z_{s_0}^{x,w} + \beta)\mathbf{1}_{\{\sup_{u \in [0,s_0]} (P_u^{x,w} + Z_u^{x,w} - \sqrt{2d}u) \leq \beta\}} e^{\sqrt{2d}(P_{s_0}^{x,w} + Z_{s_0}^{x,w}) - ds_0}|x, (X_s(x))_{0 \leq s \leq t}] \\
&\leq \frac{1}{2\beta}\mathbb{E}[((\sqrt{2d}s_0 - P_{s_0}^{x,w} - Z_{s_0}^{x,w} + \beta)^2 + 1)e^{\sqrt{2d}(P_{s_0}^{x,w} + Z_{s_0}^{x,w}) - ds_0}|x, (X_s(x))_{0 \leq s \leq t}] \\
&= \frac{1}{2\beta}((\sqrt{2d}(s_0 - q_{x,w}(s_0, s_0)) - P_{s_0}^{x,w} + \beta)^2 + q_{x,w}(s_0, s_0) + 1)e^{\sqrt{2d}P_{s_0}^{x,w} - d(s_0 - q_{x,w}(s_0,s_0))}
\end{aligned}$$

La quantité $q_{x,w}(s_0, s_0)$ s'avère petite. En effet,

$$\begin{aligned}
q_{x,w}(s_0, s_0) &= s_0 - \int_0^{s_0} (\frac{\partial K_u(x,w)}{\partial u})^2 du \\
&= \int_0^{s_0} 1 - (\frac{\partial K_u(x,w)}{\partial u})^2 du \\
&= \int_{|x-w|}^1 (1 - k(y\frac{x-w}{|x-w|})^2)\frac{1}{y}dy \\
&\leq C
\end{aligned}$$

où C ne dépend que du noyau k ($C = \sup_{z \in B(0,1)} \frac{1-k(z)^2}{|z|}$ convient par exemple). Dans l'avant dernière ligne on a utilisé un changement de variables $y = e^{u-s_0}$.

Ceci nous dit que la partie $q_{x,w}(s_0, s_0)$ n'intervient pas dans les majorations qui suivent.
On utilise ensuite la représentation en processus de Bessel β, en utilisant le fait que l'on est sur l'évènement $\mathbf{B}$. On note

$$\begin{aligned} Y_{s_0}^{x,w} &= -\int_0^{s_0} g_{x,w}(u)(X_u(x) - \sqrt{2d}u - \beta)du \\ &= P_{s_0}^{x,w} - \sqrt{2d}K_{s_0}(x-w) + \beta(k(e^{s_0}(x-w)) - k(x-w)) \\ &= P_{s_0}^{x,w} - \sqrt{2d}s_0 + \theta_{x,w}(s_0) \end{aligned}$$

avec $\theta_{x,w}$ une fonction bornée indépendamment de x, w, t, A car k est bornée.
On a donc

$$\begin{aligned} &\Theta_t^\beta(f_t^\beta(w)|x, (X_s(x))_{0\le s\le t}, \mathbf{B}) \\ &\le \frac{1}{2\beta}(((\theta_{x,w}(s_0) - Y_{s_0}^{x,w})^2 + q_{x,w}(s_0,s_0) + 1)e^{\sqrt{2d}Y_{s_0}^{x,w} + ds_0 + dq_{x,w}(s_0,s_0) - \sqrt{2d}\theta_{x,w}(s_0))}|_{\mathbf{B}} \\ &\le \frac{1}{2\beta}((C - Y_{x_0}^{x,w})^2 + C)e^{\sqrt{2d}Y_{s_0}^{x,w} + ds_0 + C}|_{\mathbf{B}} \end{aligned}$$

où C ne dépend pas de x, w, t, A.
La suite de la preuve est technique : sauter pour l'instant quelques calculs et expliquons un peu les idées. Le fait que l'on est sur l'évènement $\mathbf{B}$ (rappelons qu'il est de mesure presque pleine pour un paramètre R assez grand) nous permet de contrôler le processus $Y_{s_0}^{x,w}$:

$$-C_R(1 + \sqrt{\ln\frac{1}{|x-w|}\ln(1 + \ln\frac{1}{|x-w|})}) \le Y_{s_0}^{x,w} \le -C_R\frac{\sqrt{\ln\frac{1}{|x-w|}}}{\ln(2 + \ln\frac{1}{|x-w|})^2} \quad (6)$$

où C_R ne dépend que du paramètre R et du noyau k. On obtient :

$$\Theta_t^\beta(f_t^\beta(w)|x, (X_s(x))_{0\le s\le t}, \mathbf{B}) \le \frac{e^C}{\beta|x-w|^d}G(\ln\frac{1}{|x-w|})$$

où

$$G(y) = (1 + \sqrt{y\ln(1+y)})^2 e^{-\sqrt{2d}C\frac{\sqrt{y}}{\ln(2+y)^2}}$$

avec la constante C éventuellement modifiée.
Finalement en rassemblant toutes les estimations, on obtient, en notant V_d le

volume de la boule d'unité de $\mathbb{R}^d$:

$$\begin{aligned}\Sigma_2 &\leq \frac{2}{|A|\delta}\int_A\int_{B(x,e^{-t})^c}\frac{e^C}{\beta|x-w|^d}G(\ln\frac{1}{|x-w|})dxdw\\ &\leq \frac{2V_d}{\delta}\int_{e^{-t}}^1\frac{e^C}{\beta r^d}G(\ln\frac{1}{r})r^{d-1}dr\\ &= \frac{2V_de^C}{\delta\beta}\int_0^t G(u)du\end{aligned}$$

Or G est intégrable, ce dernier converge vers 0 quand $\delta\to+\infty$ uniformément par rapport à t.
– Il reste à expliquer l'équation (6).
Rappelons que

$$g_{x,w}(u)=\sum_{i=1}^d(x-w)_ie^u\partial_ik(e^u(x-w))$$

Alors

$$\begin{aligned}Y_{s_0}^{x,w} = &= \int_0^{\ln\frac{1}{|x-w|}} g_{x,w}(u)=\sum_{i=1}^d(x-w)_ie^u\partial_ik(e^u(x-w))(\sqrt{2d}u+\beta-X_u(x))du\\ &= \int_{|x-w|}^1 y\frac{x-w}{|x-w|}\cdot\nabla k(y\frac{x-w}{|x-w|})(\sqrt{2d}\ln\frac{y}{|x-w|}+\beta-X_{\ln\frac{y}{|x-w|}}(x))dy\end{aligned}$$

Or rappelons aussi que sur $\mathbf{B}$ on a :

$$\forall u\geq 0,\frac{\sqrt{u}}{R(\ln(2+u))^2}\leq\beta-X_u(x)+\sqrt{2d}u\leq R(1+\sqrt{u\ln(2+u)})$$

Combinons les deux dernières équations, on obtient (rappelons aussi l'hypothèse $x.\nabla k(x)\leq 0$) :

$$Y_{s_0}^{x,w}\geq R\int_{|x-w|}^1 y\frac{x-w}{|x-w|}\cdot\nabla k(y\frac{x-w}{|x-w|})(1+\sqrt{\ln\frac{y}{|x-w|}\ln(1+\ln\frac{y}{|x-w|})})dy$$

et

$$Y_{s_0}^{x,w}\leq R\int_{|x-w|}^1 y\frac{x-w}{|x-w|}\cdot\nabla k(y\frac{x-w}{|x-w|})\frac{\sqrt{\ln\frac{y}{|x-w|}}}{\ln(2+\ln\frac{y}{|x-w|})^2}dy$$

Ceci donne (6).

∘ Pour Σ_1 :
Les calculs pour Σ_1 sont quasiment identiques que pour Σ_2. En effet, on n'a plus

besoin de couper le processus à un instant s_0, et les calculs restent valables car la quantité $q_{x,w}(t,t)$ est bornée indépendamment de t. Intuitivement, c'est parce que dans la boule $B(x, e^{-t})$, les processus $(X_s(w))_{0\leq s\leq t}$ et $(X_s(x))_{0\leq s\leq t}$ sont proches, donc la partie "orthogonale" à la projection devrait être petite.
Les lecteurs impatients peuvent donc survoler les calculs pour Σ_1 que l'on explicite maintenant dans les quelques lignes qui suivent.
En utilisant la projection 3.4, on a :

$$\begin{aligned}
&\Theta_t^\beta(f_t^\beta(w)|x,(X_s(x))_{0\leq s\leq t})\\
&= \frac{1}{\beta}\mathbb{E}[(\sqrt{2d}t - P_t^{x,w} - Z_t^{x,w} + \beta)\mathbf{1}_{\{\sup_{u\in[0,t]}(P_u^{x,w}+Z_u^{x,w}-\sqrt{2d}u)\leq\beta\}}e^{\sqrt{2d}(P_t^{x,w}+Z_t^{x,w})-dt}|x,(X_s(x))_{0\leq s\leq t}]\\
&\leq \frac{1}{2\beta}\mathbb{E}[((\sqrt{2d}t - P_t^{x,w} - Z_t^{x,w} + \beta)^2 + 1)e^{\sqrt{2d}(P_t^{x,w}+Z_t^{x,w})-dt}|x,(X_s(x))_{0\leq s\leq t}]\\
&= \frac{1}{2\beta}((\sqrt{2d}(t - q_{x,w}(t,t)) - P_t^{x,w} + \beta)^2 + q_{x,w}(t,t) + 1)e^{\sqrt{2d}P_t^{x,w}-d(t-q_{x,w}(t,t))}
\end{aligned}$$

La quantité $q_{x,w}(t,t)$ s'avère d'être petite. En effet,

$$\begin{aligned}
q_{x,w}(t,t) &= t - \int_0^t (\frac{\partial K_u(x,w)}{\partial u})^2 du\\
&= \int_0^t 1 - (\frac{\partial K_u(x,w)}{\partial u})^2 du\\
&\leq \int_0^1 (1 - k(y\frac{x-w}{|x-w|})^2)\frac{1}{y}dy\\
&\leq C
\end{aligned}$$

où C ne dépend que du noyau k.
Ceci montre que la partie $q_{x,w}(t,t)$ n'intervient pas dans les majorations qui suivent.
On utilise ensuite la représentation en processus de Bessel β, en utilisant le fait que l'on est sur l'évènement $\mathbf{B}$. On note, pour $s \leq t$

$$\begin{aligned}
Y_s^{x,w} &= -\int_0^s g_{x,w}(u)(X_u(x) - \sqrt{2d}u - \beta)du\\
&= P_s^{x,w} - \sqrt{2d}K_s(x-w) + \beta(k(e^s(x-w)) - k(x-w))\\
&= P_s^{x,w} - \sqrt{2d}t + \theta_{x,w}(s)
\end{aligned}$$

avec $\theta_{x,w}$ une fonction bornée indépendamment de x, w, s, t, A.

On a donc

$$\begin{aligned}
&\Theta_t^\beta(f_t^\beta(w)|x,(X_s(x))_{0\le s\le t},\mathbf{B})\\
&\le \frac{1}{2\beta}(((\theta_{x,w}(t)-Y_t^{x,w})^2+q_{x,w}(t,t)+1)e^{\sqrt{2d}Y_t^{x,w}+dt+dq_{x,w}(t,t)-\sqrt{2d}\theta_{x,w}(t))}|_{\mathbf{B}}\\
&\le \frac{1}{2\beta}((C-Y_{x_0}^{x,w})^2+C)e^{\sqrt{2d}Y_t^{x,w}+dt+C}|_{\mathbf{B}}
\end{aligned}$$

où C ne dépend pas de x,w,s,t,A.
Le fait que l'on est sur l'évènement $\mathbf{B}$ (rappelons qu'il est de mesure presque pleine pour un paramètre R assez grand) nous permet de contrôler le processus $Y_t^{x,w}$:

$$-C_R(1+\sqrt{t\ln(1+t)})\le Y_t^{x,w}\le -C_R\frac{\sqrt{t}}{\ln(2+t)^2} \tag{7}$$

où C_R ne dépend que du paramètre R et du noyau k. On a :

$$\Theta_t^\beta(f_t^\beta(w)|x,(X_s(x))_{0\le s\le t},\mathbf{B})\le \frac{e^C}{\beta}G(t)e^{dt}$$

où

$$G(y)=(1+\sqrt{y\ln(1+y)})^2e^{-\sqrt{2d}C\frac{\sqrt{y}}{\ln(2+y)^2}}$$

avec la constante C éventuellement modifiée.
Finalement en rassemblant toutes les estimations, on obtient :

$$\begin{aligned}
\Sigma_1 &\le \frac{2}{|A|\delta}\int_A\int_{B(x,e^{-t})}\frac{e^C}{\beta}G(t)e^{dt}dxdw\\
&\le \frac{2e^C}{\delta\beta}G(t)
\end{aligned}$$

Or G est bornée, ce dernier converge vers 0 quand $\delta\to+\infty$ uniformément par rapport à t.

• Identification des limites de martingales $Z_t^\beta(A)$ et $M_t'(A)$:
On passe par la variable aléatoire $\tilde{Z}_t^\beta(A)$. Rappelons sa définition :

$$\tilde{Z}_t^\beta(A)=\int_A(\sqrt{2d}t-X_t(x))\mathbf{1}_{\{\tau^\beta>t\}}e^{\sqrt{2d}X_t(x)-d\mathbb{E}[X_t(x)^2]}dx$$

D'abord remarquons que $\tilde{Z}_t^\beta(A)$ et $Z_t^\beta(A)$ ont p.s. la même limite car

$$|\tilde{Z}_t^\beta(A)-Z_t^\beta(A)|=\beta\int_A\mathbf{1}_{\{\tau^\beta>t\}}e^{\sqrt{2d}X_t(x)-d\mathbb{E}[X_t(x)^2]}dx\le\beta M_t^{\sqrt{2d}}(A)$$

et ce dernier converge vers 0 p.s. quand $t \to +\infty$ à cause du théorème de Kahane sur la dégénérescence de la mesure limite, voir le rappel 3.1.
Il reste donc à identifier $\tilde{Z}_t^\beta(A)$ et $M'_t(A)$ pour β assez grand. Pour ceci on utilise un résultat sur le supremum d'un champ gaussien log-corrélé, rappelé dans la partie suivante, qui implique notamment :

$$\sup_{t\in\mathbb{R}_+}(\sup_{x\in A} X_t(x) - \sqrt{2d}t) < +\infty$$

presque sûrement.
En découle alors

$$\forall t, M'_t(A) = \tilde{Z}_t^\beta(A)$$

pour β assez grand.
On conclut donc par la positivité de la martingale $Z_t^\beta(A)$ et les raisonnements plus hauts que p.s. $(M'_t(dx))_{t\leq 0}$ converge en loi vers une mesure aléatoire positive.

Remarque 3.1. *En exploitant cette preuve, on arrive à montrer (voir [6] pour plus de détails) que la mesure limite est à support plein et sans atome. On utilise notamment le fait que la mesure limite M' est solution à une classe d'équations dite $\star$-équations étudiées dans [2].*

3.3 Sur le supremum d'un champ gaussien log-corrélé

Dans cette sous-section on démontre un résultat simple sur le supremum d'un champ gaussien log-corrélé. Il est à souligner que beaucoup de résultats plus forts et plus précis, notamment de type convergence en loi, ont été démontrés très récemment (voir [3] pour le cas du champ libre gaussien discret, [6] pour une liste de conjectures, et [16] pour la réponse apportée à une de ces conjectures).
On rappelle ici, pour finir la preuve, un résultat relativement simple démontré dans [6] :

Théorème 3.5. ***Sur le maximum d'un champ gaussien log-corrélé***
*Soit k un noyau de classe C^1 avec $k(0) = 1$ et l-**lipschitzien** en 0 avec $l > 0$. Soit X le champ gaussien associé au noyau k défini précédemment. Alors pour tout $a \in [0, \frac{1}{2}[$ et tout ouvert borné $A \subset \mathbb{R}^d$, on a p.s. :*

$$\sup_{t\geq 0}(\sup_{x\in A} X_t(x) - \sqrt{2d}t + \frac{a}{\sqrt{2d}}\ln(t+1)) < +\infty$$

En particulier,

$$\sup_{t\in\mathbb{R}_+}(\sup_{x\in A} X_t(x) - \sqrt{2d}t) < +\infty$$

Remarquons d'abord qu'un noyau k de classe C^1 à support compact est clairement lipschitzien en 0, donc le théorème est valable dans le cas présent.

Démonstration. Cette preuve est basée sur la constuction du cône.

• Rappels sur la construction de la cascade multiplicative log-normale de Mandelbrot (voir aussi la preuve du théorème 2.7) :
On considère l'arbre $T = (\{0,1\}^d)^{\mathbb{N}^*}$ muni d'une distance ultra-métrique

$$\forall s,t \in T, dist(s,t) = 2^{-d.\sup\{N\in\mathbb{N}:\forall k\leq N, \pi_k(t)=\pi_k(s)\}}$$

où $\pi_k(t)$ désigne la k-ième composante de t, avec la convention que le supremum vaut 0 si l'ensemble est vide.
On définit ensuite une suite $((Y_n(t))_{t\in T})_n$ de processus gaussiens centrés deux à deux indépendants, définis sur T, de noyau p_n défini par

$$\forall s,t \in T, p_n(t,s) = \begin{cases} u \text{ si } dist(t,s) \leq 2^{-nd} \\ 0 \text{ si } dist(t,s) > 2^{-nd} \end{cases}$$

Remarquons qu'alors ce noyau est constant sur chacun des 2^{dn} cylindres prescrits selon les n premières coordonnées. On note dans la suite $I_n(t)$ le cylindre contenant t.
On définit ensuite

$$\forall t \in T, \overline{X}_n(t) = \sum_{k=1}^{n} Y_k(t)$$

de noyau $q_n = \sum\limits_{k=1}^{n} p_k$.
On rappelle aussi que l'arbre $T = (\{0,1\}^d)^{\mathbb{N}^*}$ peut être plongé naturellement dans la cube $[0,1[^d$, en itérant la division d'une cube en 2^d cubes plus petites. Par exemple, quand $d = 1$, ceci n'est autre que l'écriture dyadique de l'intervalle $[0,1[$. Dans la suite on écrit indifféremment $Y_n(t)$ (ou $\overline{X}_n(t)$) pour $t \in T$ ou $t \in [0,1[^d$ en utilisant cette identification.

• Rappels sur la construction du cône :
En suivant les rappels dans [6], on esquisse rapidement la construction du cône.
La construction du cône est une façon agréable d'avoir des mesures gaussiennes aléatoires sur l'espace $(\mathbb{R}\times\mathbb{R}_+, \mathcal{B}(\mathbb{R}\times\mathbb{R}_+))$, "spatialement" indépendantes. Le but est donc d'avoir une famille de variables aléatoires gaussiennes $(\mu(A), A \in \mathcal{B}(\mathbb{R}\times\mathbb{R}_+))$ telle que :
1) Pour tout ensemble mesurable $A \in \mathcal{B}(\mathbb{R}\times\mathbb{R}_+)$, $\mu(A)$ est une variable gaussienne ayant pour fonction caractéristique :

$$\mathbb{E}[e^{iq\mu(A)}] = e^{-\frac{q^2}{2}\Gamma(A)}$$

où la mesure (déterministe) Γ est donnée par

$$\Gamma(dx, dy) = \frac{1}{y^2} dx dy$$

2) Pour toute suite d'ensembles mesurables $(A_n)_n$ deux à deux disjoints dans $\mathcal{B}(\mathbb{R} \times \mathbb{R}_+)$, les mesures $(\mu(A_n))_n$ sont deux à deux indépendantes et

$$\mu(\bigcup_n A_n) = \sum_n \mu(A_n)$$

presque sûrement.
On définit ensuite un processus gaussien stationnaire $(\omega_l(x))_{x \in \mathbb{R}}$ par, pour $0 < l \leq 1$,

$$\omega_l(x) = \mu(\mathcal{A}_l(x))$$

où $\mathcal{A}_l(x)$ est la région $\{(u, y) \in \mathbb{R} \times \mathbb{R}_+^* : l \leq y \leq 1, -\frac{y}{2} \leq x - u \leq \frac{y}{2}\}$.

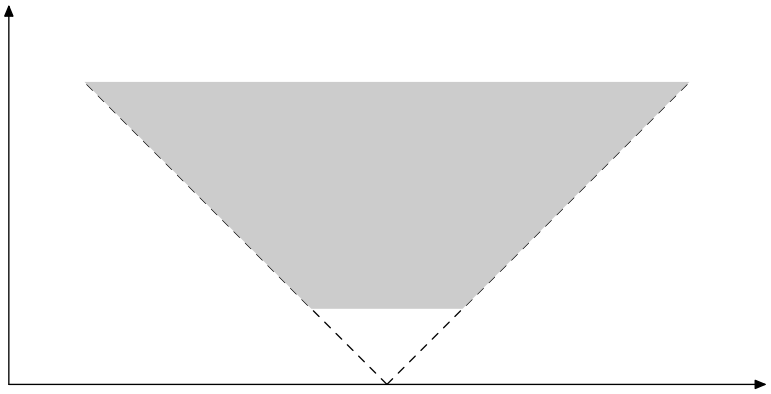

FIGURE 4 – Un cône

Le noyau de covariance du processus ω_l est donc

$$K_l(x) = \int_1^{\frac{1}{l}} \frac{(1 - |ux|)_+}{u} du$$

de sorte que $\omega_{e^{-t}}$ ait la même loi que X_t.
Maintenant on est en mesure d'énoncer un lemme de décomposition comme conséquence de la construction du cône :

Lemme 3.6. ***Un lemme de décomposition***
On fixe $n \in \mathbb{N}$ et on considère les intervalles $I_{i,n} = [\frac{i}{2^n}, \frac{i+1}{2^n}[$. On a la décomposition suivante pour tout $X_{s \ln 2}(x)$ avec $s \in [n, n+1]$ et $x \in I_{i,n}$:

$$X_{s \ln 2}(x) = X_{i,n} + Y_s^{i,n}(x)$$

qui vérifie :
– *Il existe une constante $C > 0$ indépendante de n telle que*

$$\mathbb{E}[X_{i,n}X_{j,n}] = n\ln 2 - (1 - \frac{1}{2^n})$$

si $i = j$ et

$$\mathbb{E}[X_{i,n}X_{j,n}] \geq \mathbb{E}[\overline{X}_n(\frac{i}{2^n})\overline{X}_n(\frac{j}{2^n})] - C$$

si $i \neq j$;
– *Pour tout i, le processus $(Y_s^{i,n}(x))_{x\in[n,n+1],x\in I_{i,n}}$ est continu et indépendant de $X_{i,n}$;*
– *Pour tout i, j, tout $s, s' \in [n, n+1]$ et $x \in I_{i,n}$, $x' \in I_{j,n}$,*

$$\mathbb{E}[Y_s^{i,n}(x)Y_s^{j,n}(x')] \geq 0$$

– *Pour tout i, j, tout $s \in [n, n+1]$ et $x \in I_{i,n}$,*

$$\mathbb{E}[Y_s^{i,n}(x)X_{j,n}] \geq 0$$

Montrons ce lemme.
Prenons $i \in \mathbb{N}$ tel que $0 \leq i \leq 2^n - 1$. On décompose $\mathcal{A}_{2^{-s}}(x)$ en deux parties :
– Une partie commune à tous les cônes du type $\mathcal{A}_{2^{-s}}(x)$ pour $s \in [n, n+1]$ et $x \in I_{i,n}$:

$$\begin{aligned}\mathcal{A}_{i,n} &= \bigcap_{s\in[n,n+1]} \bigcap_{x\in I_{i,n}} \mathcal{A}_{2^{-s}}(x) \\ &= \{(u, y) \in \mathbb{R} \times \mathbb{R}_+^* : 2^{-n} \leq y \leq 1, -\frac{y}{2} + \frac{i+1}{2^n} \leq u \leq \frac{y}{2} + \frac{i}{2^n}\}\end{aligned}$$

On lui associe le processus $X_{i,n} = \mu(\mathcal{A}_{i,n})$.
– La partie complémentaire

$$\mathcal{R}_s^{i,n}(x) = \mathcal{A}_{2^{-s}}(x) - \mathcal{A}_{i,n}$$

On lui associe le processus $Y_s^{i,n}(x) = \mu(\mathcal{R}_s^{i,n}(x))$.
On vérifie aisément par des calculs élémentaires que l'on obtient bien le lemme à l'aide de cette décomposition géométrique.

• La preuve :
Il suffit de faire le cas où $k(x) = (1 - \frac{|x|}{L})_+$. En effet, comme k est lipschzien en 0, il est plus grand que $(1 - \frac{|x|}{L})_+$ pour un certain L. Mais alors en utilisant le lemme de Slepian (lemme 5.6), on sait que

$$\mathbb{P}[\sup_{t\geq 0}(\sup_{x\in A} X_t(x) - \sqrt{2d}t + \frac{a}{\sqrt{2d}}\ln(t+1)) < +\infty]$$

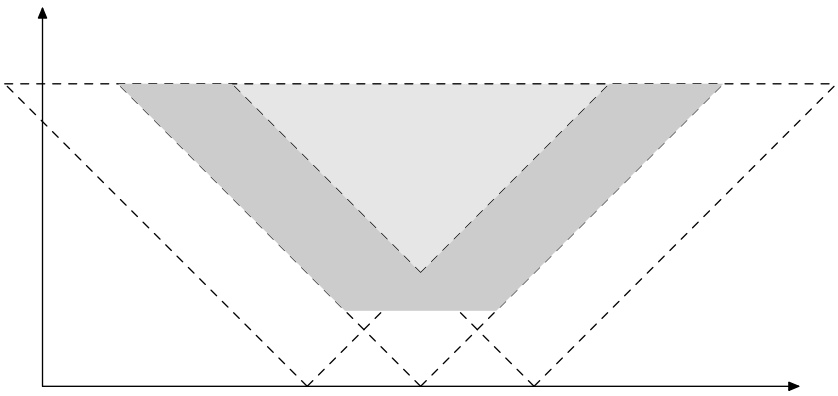

FIGURE 5 – Décomposition d'un cône

croît si l'on remplace $(1-\frac{|x|}{L})_+$ par k.
Dans la suite pour simplifier la présentation, on fait la preuve dans le cas $d=1$ et $k(x)=(1-|x|)_+$.
Soient Z une variable aléatoire gaussienne standard indépendante du processus $(X_{s\ln 2}(x))_x$ et $(\overline{Z}_i)_{0\leq i\leq 2^n-1}$ une suite de variables aléatoires gaussiennes standards indépendantes. On se donne ensuite une suite de processus indépendants $(\overline{Y}_s^{i,n}(x))_{s\in[n,n+1],x\in I_{i,n}}$ qui ont les mêmes lois que $(Y_s^{i,n}(t))_{s\in[n,n+1],x\in I_{i,n}}$.
Par l'inégalité de convexité de Kahane (théorème 5.7), on a :

$$\begin{aligned}
&\mathbb{P}[\sup_{0\leq i\leq 2^n-1}\sup_{s\in[n,n+1]}\sup_{x\in I_{i,n}}(X_{i,n}+\sqrt{1-\frac{1}{2^n}+C}Z+Y_s^{i,n}(x)-\sqrt{2}n\ln 2)\geq x]\\
&\leq \mathbb{P}[\sup_{0\leq i\leq 2^n-1}\sup_{s\in[n,n+1]}\sup_{x\in I_{i,n}}(\overline{X}_n(\frac{i}{2^n})+\sqrt{C}\overline{Z}_i+\overline{Y}_s^{i,n}(x)-\sqrt{2}n\ln 2)\geq x]
\end{aligned}$$

En effet :
– Pour $i=j$, $x,x'\in I_{i,n}$ et $s,s'\in[n,n+1]$:

$$\begin{aligned}
&\mathbb{E}[(X_{i,n}+\sqrt{1-\frac{1}{2^n}+C}Z+Y_s^{i,n}(x))(X_{i,n}+\sqrt{1-\frac{1}{2^n}+C}Z+Y_{s'}^{i,n}(x'))]\\
&=n\ln 2+C+\mathbb{E}[Y_s^{i,n}(x)Y_{s'}^{i,n}(x')]\\
&=\mathbb{E}[(\overline{X}_n(\frac{i}{2^n}+\sqrt{C}\overline{Z}_i+\overline{Y}_s^{i,n}(x))(\overline{X}_n(\frac{i}{2^n}+\sqrt{C}\overline{Z}_i+\overline{Y}_{s'}^{i,n}(x'))]
\end{aligned}$$

– Pour $i \neq j$, $x \in I_{i,n}$, $x' \in I_{j,n}$ et $s, s' \in [n, n+1]$:

$$\begin{aligned}
&\mathbb{E}[(X_{i,n} + \sqrt{1 - \frac{1}{2^n} + C}Z + Y_s^{i,n}(x))(X_{i,n} + \sqrt{1 - \frac{1}{2^n} + C}Z + Y_{s'}^{i,n}(x'))] \\
&\geq \mathbb{E}[X_{i,n}X_{j,n} + 1 - \frac{1}{2^n} + C] \\
&\geq \mathbb{E}[\overline{X}_n(\frac{i}{2^n})\overline{X}_n(\frac{j}{2^n})] \\
&= \mathbb{E}[(\overline{X}_n(\frac{i}{2^n} + \sqrt{C}\overline{Z}_i + \overline{Y}_s^{i,n}(x))(\overline{X}_n(\frac{j}{2^n} + \sqrt{C}\overline{Z}_j + \overline{Y}_{s'}^{j,n}(x'))]
\end{aligned}$$

Maintenant on se donne $\beta > 1$ et $r < 1$ tels que $\beta r < 1$ et $(\frac{3}{2} - a)\beta r > 1$. Alors :

$$\begin{aligned}
&\mathbb{P}[\sup_{0 \leq i \leq 2^n - 1} \sup_{x \in [n,n+1]} \sup_{x \in I_{i,n}} (\sqrt{2}\overline{X}_n(\frac{i}{2^n}) + \sqrt{2C}\overline{Z}_i + \sqrt{2}\overline{Y}_x^{i,n}(s) - 2n\ln 2 + a\ln(n+1)) \geq 1] \\
&= \mathbb{P}[\sup_{0 \leq i \leq 2^n - 1} (\sqrt{2}\overline{X}_n(\frac{i}{2^n}) + \sqrt{2C}\overline{Z}_i + \sqrt{2} \sup_{s \in [n,n+1], x \in I_{i,n}} \overline{Y}_s^{i,n}(x) - 2n\ln 2 + a\ln(n+1)) \geq 1] \\
&\leq (n+1)^{a\beta r} e^{-\beta r} \mathbb{E}[(\sum_{i=0}^{2^n - 1} e^{\beta(\sqrt{2}\overline{X}_n(\frac{i}{2^n}) + \sqrt{2C}\overline{Z}_i + \sqrt{2}\sup_{s \in [n,n+1], x \in I_{i,n}} \overline{Y}_s^{i,n}(x) - 2n\ln 2)})^r] \\
&= (n+1)^{a\beta r} e^{-\beta r} \mathbb{E}[\mathbb{E}[(\sum_{i=0}^{2^n - 1} e^{\beta(\sqrt{2}\overline{X}_n(\frac{i}{2^n}) + \sqrt{2C}\overline{Z}_i + \sqrt{2}\sup_{s \in [n,n+1], x \in I_{i,n}} \overline{Y}_s^{i,n}(x) - 2n\ln 2)})^r | \overline{X}_n]] \\
&\leq (n+1)^{a\beta r} e^{-\beta r} \mathbb{E}[(\mathbb{E}[\sum_{i=0}^{2^n - 1} e^{\beta(\sqrt{2}\overline{X}_n(\frac{i}{2^n}) + \sqrt{2C}\overline{Z}_i + \sqrt{2}\sup_{s \in [n,n+1], x \in I_{i,n}} \overline{Y}_s^{i,n}(x) - 2n\ln 2)} | \overline{X}_n])^r] \\
&= (n+1)^{a\beta r} e^{-\beta r} \mathbb{E}[e^{\beta(\sqrt{2C}\overline{Z}_i + \sqrt{2}\sup_{s \in [n,n+1], x \in I_{i,n}} \overline{Y}_s^{i,n}(x)}]^r \mathbb{E}[(\sum_{i=0}^{2^n - 1} e^{\beta(\sqrt{2}\overline{X}_n(\frac{i}{2^n}) - 2n\ln 2)})^r] \\
&\leq C_{\beta,r}(n+1)^{a\beta r} \mathbb{E}[(\sum_{i=0}^{2^n - 1} e^{\beta(\sqrt{2}\overline{X}_n(\frac{i}{2^n}) - 2n\ln 2)})^r] \\
&\leq \frac{C_{\beta,r}}{n^{(\frac{3}{2} - a)\beta r + o(1)}}
\end{aligned}$$

Où la première inégalité résulte de l'inégalité de Markov, la deuxième de l'inégalité de Jensen et la dernière résulte d'un théorème démontré dans le contexte du processus du branchement (voir le théorème 5.14).
Expliquons un peu la dernière inégalité :
Considérons l'arbre binaire correspondant à l'écriture dyadique des nombres $\frac{i}{2^n}$, i.e. écrivons

$$\frac{i}{2^n} = \sum_{k=1}^{n} \frac{e_k}{2^k}$$

avec $e_k \in \{0,1\}$. L'identification $\frac{i}{2^n} \mapsto e_1, \ldots, e_n$ nous dit que l'on peut voir $\frac{i}{2^n}$ comme un individu dans la n-ième génération si l'arbre binaire est étiquetté convenablement. Dans l'avant dernière ligne du calcul précédent on peut remplacer chaque $\overline{X}_n(\frac{i}{2^n})$ par $\sum_{k=1}^{n} Y_k(\sum_{i=1}^{k} \frac{i}{2^i})$ car rappelons que le noyau de Y_k est constant sur chaque intervalle $[\frac{i}{2^k}, \frac{i+1}{2^k}[$. Si l'on attache à chaque arête de l'arbre la variable aléatoire $2\ln 2 - Y_g(x)$ où g (resp. x) est la génération (resp. coordonnée) du fils de l'arête, on peut alors utiliser le résultat 5.14 (la constante $2\ln 2$ sert aussi à renormaliser pour avoir l'hypothèse 3 dans l'énoncé de ce théorème).
Il ne reste qu'à évoquer le lemme de Borel-Cantelli pour conclure. $\square$

4 Un petit résultat

Dans cette section nous tenterons de montrer rigoureusement une affirmation dans [7] (voir aussi [23] pour une autre formulation).

> **Liouville measure at criticality in dimension 2...**
> On peut obtenir des résultats analogues à ceux énoncés dans la section précédante sur la martingale dérivée du chaos multiplicatif gaussien au point critique dans le cas du champ libre gaussien, en modifiant légèrement la preuve dans [6].

Nous rappelons la définition d'un champ libre gaussien (massif) dans les sections 5.3.3, 5.3.4. Néanmoins discutons un peu de façon qualitative ce qui change dans cette nouvelle situation.

Remarque 4.1. ***Remarques préliminaires***
Soulignons ici ce qui change par rapport à la section précédente :
1) On constate que le champ libre gaussien n'est pas stationnaire ;
2) On constate que le champ libre gaussien est corrélé à toute distance (i.e. le noyau k n'est pas à support compact).
En dépit du manque de décorrélation à grande échelle qui est un élément fondamental dans la preuve de la section précédente, on constate que la fonction de corrélation décroît très vite (exponentiellement), ce qui suggère que l'on pourrait éventuellement contrôler les corrélations à grande distance.

Ici nous répondons à cette question dans le cas du champ libre gaussien massif. Nous attaquons ce problème en utilisant, à nouveau, la méthode du cut-off. Le phénomène n'est pas très différent de celui dans la section précédente, cependant il faut être judicieux sur le choix du cut-off qui est au coeur de cette méthode.

4.1 Énoncé du théorème dans le cas du champ libre gaussien massif

On considère le champ libre gaussien massif X de masse m sur $\mathbb{R}^2$.
On considère une approximation du champ X : prenons $((X_\epsilon(x))_{x\in\mathbb{R}^2})_{\epsilon>0}$ une famille de processus gaussiens centrés stationnaires ayant pour fonction de covariance

$$K_\epsilon(x) = \mathbb{E}[X_\epsilon(0)X'_\epsilon(x)] = \int_1^{\frac{1}{\epsilon}} \frac{k_m(ux)}{u} du$$

avec $k_m(z) = \frac{1}{2}\int_0^\infty e^{-\frac{m}{v}|z|^2-\frac{v}{2}} dv$ (voir la section 5.3.2 pour les rappels sur la fonction de Green massive). Dans la suite on va fixer un m et laisser l'indice.

On considère ensuite la martingale dérivée de façon analogue que dans la section 3 (mais avec un changement de varibles pour le paramètre du temps) :

$$M'_\epsilon(dx) = (2\ln\frac{1}{\epsilon} - X_\epsilon(x))e^{2X_\epsilon(x)-2\ln\frac{1}{\epsilon}}dx$$

et on énonce le même résultat

Théorème 4.1. ***Convergence de la martingale dérivée, cas du champ libre gaussien massif***
Pour tout ouvert borné $A \in \mathbb{R}^d$, la martingale $(M'_\epsilon(A))_{\epsilon\geq 0}$ converge p.s. vers une variable aléatoire p.s. strictement positive que l'on notera $M'(A)$.

Remarque 4.2. ***Sur l'unicité de la construction***
On souligne encore une fois qu'il n'y a pas encore de choix canonique pour construire cet objet, et l'unicité de la construction n'est pas encore démontrée.

4.2 Discussion sur le cut-off

On a vu que dans [6], le noyau k que l'on a choisi pour faire les calculs était à support compact. Ici dans le cas du massif, on ne se retrouve pas devant exactement la même situation : le noyau k_m n'est plus à support compact, mais il admet une décroissance exponentielle à l'infini, ce qui suggère que, quitte à proposer un nouveau cut-off, les résultats du [6] devront restés valides dans le cas du champ libre gaussien massif.
Cependant, sur le choix du cut-off, il faudrait être judicieux : si on coupe brutalement le noyau k_m du champ libre gaussien massif (par exemple en considérant $\frac{k(u(x-w))}{u}\mathbf{1}_{\{u\geq 1\}}$), on ne peut pas transposer directement les méthodes du [6]. En effet, il faudrait plutôt considérer le noyau k (ou k_m) comme une fonction à plusieurs variables, par exemple de ux, uw et de u, voir la remarque 2.2 dans [13] pour plus de discussions.
S'inpirant des techniques employées dans l'article [23], on propose un nouveau cut-off en considérant $\frac{k(u(x-w))}{u}\mathbf{1}_{\{u|x-w|\geq 1\}}$. Le point à remarquer ici, c'est que les processus ne sont pas complètement décorrélés à grande distance, en revanche la fonction de corrélation devient "presque" constante à partir d'une certaine distance. Le rôle joué par le théorème d'arrêt dans [6] sera donc remplacé par cette propriété, qui permet elle aussi de ramener les calculs à grandes distances à une échelle constante.
Le théorème suivant, analogue à celui présenté dans la section 3, à été démontré dans [23].

Théorème 4.2. ***Convergence de la martingale dérivée dans le cas de l'étude sur le mouvement brownien de Liouville critique***

On se donne $t > 0$, $x, z \in \mathbb{R}^2$, $\beta > 0$ et on définit

$$f_\epsilon^\beta(z) = (2\ln\frac{1}{\epsilon} - X_\epsilon(z + B_u))\mathbf{1}_{\{\tau_z^\beta < \epsilon\}} e^{2X_\epsilon(z+B_u) - 2\ln\frac{1}{\epsilon}}$$

On s'intéresse à la martingale

$$F^{\beta,\epsilon}(x,t) = \int_0^t (2\ln\frac{1}{\epsilon} - X_\epsilon(B_u^x))\mathbf{1}_{\{\tau_{B_u^x}^\beta < \epsilon\}} e^{2X_\epsilon(B_u^x) - 2\ln\frac{1}{\epsilon}} du = \int_0^t f_t^\beta(B_u^x) du$$

avec B_u^x un mouvement brownien plan issu de x et pour chaque $u \in [0,t]$, τ_u^β le $(\mathcal{F}_\epsilon)_\epsilon$-temps d'arrêt défini par $\tau_z^\beta = \sup\{r \leq 1, X_r(z) - 2\ln\frac{1}{r} > \beta\}$.
Alors pour $x \in \mathbb{R}^2$ et $t > 0$ fixés, p.s. (par rapport à B^x), la martingale $(F^{\beta,\epsilon}(x,t))_{\epsilon>0}$ est uniformément intégrable.

Rappelons l'idée géniale de la preuve de ce résultat dans l'article [23] : on décompose le champ en somme de trois mouvements browniens indépendents, avec une partie "commune" qui encode la corrélation. Formellement, si l'on écrit

$$h_1(s) = h_2(s) = \ln\frac{1}{s} - K_s(x - w), \bar{h}(s) = K_s(x - w)$$

et si l'on définit ensuite

$$P_s^{x,w} = B_{h_1(s)}^1, P_s^{w,x} = B_{h_2(s)}^2, Z_s = \bar{B}_{\bar{h}(s)}$$

avec B^1, B^2, $\bar{B}$ trois mouvements browniens standards indépendents, on a

$$(X_s(x), X_s(w))_{0\leq s\leq 1} = (P_s^{x,w} + Z_s, P_s^{w,x} + Z_s)_{0\leq s\leq 1}$$

en loi. Il s'avère que l'on peut montrer une convergence dans $\mathcal{L}^2$ de la martingale $(F^{\beta,\epsilon}(x,t))_{\epsilon>0}$, et en plus, ce qui compte vraiment dans les majorations, c'est la partie commune dans la décomposition.

$$\begin{tikzcd}
X(x) \arrow[rr, dash, "\sim\ \sim\ \sim\ \sim\ \sim"] \arrow[d] \arrow[dr] & & X(w) \arrow[dl] \arrow[d] \\
P^{x,w} & Z & P^{w,x}
\end{tikzcd}$$

FIGURE 6 – Décomposition en trois mouvements browniens indépendants

Les grandes lignes de cette première partie de la preuve seront exactement les mêmes que dans [23]. De façon heuristique, un petit calcul à la main nous montre que la partie commune devient "presque" constante une fois la distance entre x et w dépasse ϵ. Donc on peut utiliser les mêmes méthodes de majorations, quitte à changer quelques constantes et la mesure [3].

3. Dans [23], il s'agit d'intégrer par rapport à la mesure d'occupation, mais la preuve est quasi-identique, si ce n'est pas plus simple, si l'on travaille avec la mesure de Lebesgue.

4.3 Preuve du théorème 4.1

Démonstration. On montre d'abord l'uniforme intégrabilité de la martingale $Z_\epsilon^\beta(A)$. Notons

$$f_\epsilon^\beta(z) = (2\ln\frac{1}{\epsilon} - X_\epsilon(z))\mathbf{1}_{\{\tau_z^\beta<\epsilon\}}e^{2X_\epsilon(z)-2\ln\frac{1}{\epsilon}}$$

avec $\tau_z^\beta = \sup\{r \leq 1, X_r(z) - 2\ln\frac{1}{r} > \beta\}$.
Pour A un ouvert borné (disons inclus dans $B(0,\frac{1}{2})$) on définit :

$$Z_\epsilon^\beta(A) = \int_A f_\epsilon^\beta(z)dz$$

la martingale qui nous intéresse (on a déjà démontré que c'est une martingale dans la section précédente, voir le paragraphe 3.2).
On va montrer une convergence dans $\mathcal{L}^2$ de cette martingale.
On va représenter le champ X_ϵ à l'aide de plusieurs mouvements browniens indépendents comme l'on a expliqué précédemment :
On définit d'abord

$$K_s^{cut}(x-w) = \int_1^{\frac{1}{\epsilon}} \frac{k(u(x-w))}{u}\mathbf{1}_{\{u|x-w|\leq 1\}}du = \int_1^{\min(\frac{1}{\epsilon},\frac{1}{|x-w|})} \frac{k(u(x-w))}{u}du$$

et

$$K_s^{off}(x-w) = \int_1^{\frac{1}{\epsilon}} \frac{k(u(x-w))}{u}\mathbf{1}_{\{u|x-w|\geq 1\}}du = \int_{\min(\frac{1}{\epsilon},\frac{1}{|x-w|})}^{\frac{1}{\epsilon}} \frac{k(u(x-w))}{u}du$$

Rappelons alors que $K = K^{cut} + K^{off}$. Soulignons que les K^{cut} et K^{off} ne sont pas des noyaux gaussiens.
On définit ensuite

$$h_1(s) = h_2(s) = \ln\frac{1}{s} - K_s(x-w), h_{cut}(s) = K_s^{cut}(x-w), h_{off}(s) = K_s^{off}(x-w)$$

puis

$$P_s^{x,w} = B^1_{h_1(s)}, P_s^{w,x} = B^2_{h_2(s)}, Z_s^{cut} = B^{cut}_{h_{cut}(s)}, Z_s^{off} = B^{off}_{h_{off}(s)}$$

avec $B^1, B^2, B^{cut}, B^{off}$ quatre mouvements browniens standards indépendents.
On remarque que

$$(X_s(x), X_s(w))_{0\leq s\leq 1} = (P_s^{x,w} + Z_s^{cut} + Z_s^{off}, P_s^{w,x} + Z_s^{cut} + Z^{off})_{0\leq s\leq 1}$$

en loi.
Notons aussi $Z = Z^{cut} + Z^{off}$ en cohérence avec les notations de [23].

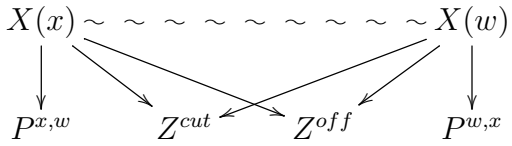

FIGURE 7 – Décomposition en quatre mouvements browniens indépendants

En vue d'utiliser le cut-off que l'on propose, on découpe l'espace de la façon suivante :

$$\begin{aligned}
\mathbb{E}[Z_\epsilon^\beta(A)^2] &= \int_A \int_A \mathbb{E}^X[f_\epsilon^\beta(x) f_\epsilon^\beta(w)] dw dx \\
&= \int_A \int_{B(x,\epsilon)} \mathbb{E}^X[f_\epsilon^\beta(x) f_\epsilon^\beta(w)] dw dx + \int_A \int_{C(x,\epsilon)} \mathbb{E}^X[f_\epsilon^\beta(x) f_\epsilon^\beta(w)] dw dx \\
&= \Sigma_\epsilon^1 + \Sigma_\epsilon^2
\end{aligned}$$

avec $C(x,\epsilon) = A - B(x,\epsilon)$ pourvu que $B(x,\epsilon) \subset A$.
Discutons un peu sur le comportement du champ X_ϵ à l'intérieur de chaque région.
– Pour la partie Σ_ϵ^1, on devrait observer une très forte corrélation, qui se traduit par le fait que dans la décomposition, la partie commune domine les autres. Heuristiquement, le processus $X_\epsilon(w)$ est donc très proche de $X_\epsilon(x)$ dans cette région.
– Pour la partie Σ_ϵ^2, la fonction de corrélation est "presque" constante. Heuristiquement, que l'on soit à l'infini ou à une distance ϵ, la partie commune se comporte à peu près de la même façon. On verra que ce qui joue vraiment dans les majorations c'est cette partie commune.
On entre maintenant dans les détails du calcul.
Tout d'abord, rappelons une conséquence du théorème d'arrêt qui permet de ramener les calculs à grande échelle à une échelle constante égale à $|x-w|$ déjà démontrée dans [6] (voir aussi 3.3).

Lemme 4.3. *Pour $x \neq w \in \mathbb{R}^2$ et β constante, on a*

$$\mathbb{E}[f_\epsilon^\beta(x) f_\epsilon^\beta(w)] = \mathbb{E}[f^\beta_{\max(\epsilon,|x-w|)}(x) f^\beta_{\max(\epsilon,|x-w|)}(w)]$$

Dans notre cadre on ne peut pas appliquer directement ce théorème d'arrêt à cause de la partie Z^{off}. Cependant ce n'est pas un grand souci car la partie Z^{off} est à

variance finie. En effet :

$$\begin{aligned}
K_s^{off}(x-w) &= \int_1^{\frac{1}{s}} \frac{k(u(x-w))}{u} \mathbf{1}_{\{u|x-w|\geq 1\}} du \\
&\leq \int_1^{+\infty} \frac{k(u(x-w))}{u} \mathbf{1}_{\{u|x-w|\geq 1\}} du \\
&= \int_{|x-w|}^{+\infty} \frac{k(u)}{u} \mathbf{1}_{\{u\geq 1\}} du \\
&\leq \int_1^{+\infty} \frac{k(u)}{u} du \\
&< +\infty
\end{aligned}$$

Maintenant on commence les calculs en suivant exactement les mêmes idées que dans [23].

• Pour Σ_ϵ^1 :
Par le théorème de Girsanov,

$$\begin{aligned}
\Sigma_\epsilon^1 = &\int_A \int_{B(x,\epsilon)} \mathbb{E}^X[(\beta - P_\epsilon^{w,x} - Z_\epsilon + 2\ln\frac{1}{\epsilon})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{w,x}+Z_r-2\ln\frac{1}{r}\leq\beta\}} \\
&(\beta - P_\epsilon^{x,w} - Z_\epsilon + 2\ln\frac{1}{\epsilon})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{x,w}+Z_r-2\ln\frac{1}{r}\leq\beta\}} e^{2P_\epsilon^{x,w}+4Z_\epsilon+2P_\epsilon^{w,x}-4\ln\frac{1}{\epsilon}}]dwdx \\
= &\int_A \int_{B(x,\epsilon)} \mathbb{E}^X[(\beta - P_\epsilon^{w,x} - Z_\epsilon)\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{w,x}+Z_r\leq\beta\}} \\
&(\beta - P_\epsilon^{x,w} - Z_\epsilon)\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{x,w}+Z_r\leq\beta\}} e^{2Z_\epsilon+2K_\epsilon(x-w)}]dwdx
\end{aligned}$$

On définit

$$\beta_\epsilon^{x,w} = \beta - \min_{s\in[\epsilon,1]} P_s^{x,w}$$

Observons que pour $w \in B(x,\epsilon)$, $\sup_{s\in[\epsilon,1]} h_1(s), \sup_{s\in[\epsilon,1]} h_2(s) \leq c$ pour une constante $c > 0$ qui ne dépend que du noyau k. En effet, comme k est l-lipschitzien en 0, on a, pour tout $s \in [\epsilon, 1]$ et $w \in B(x,\epsilon)$,

$$\begin{aligned}
h_1(s) = h_2(s) &= \ln\frac{1}{s} - \int_1^{\frac{1}{s}} \frac{k(u(x-w))}{u} du \\
&= \int_1^{\frac{1}{s}} \frac{1-k(u(x-w))}{u} du \\
&\leq \int_1^{\frac{1}{s}} \frac{lu|x-w|}{u} du \\
&\leq l(1-|x-w|) \\
&\leq l
\end{aligned}$$

Il s'ensuit que :

$$\Sigma_\epsilon^1 \leq C \int_A \int_{B(x,\epsilon)} \mathbb{E}^X[(1+(Z_\epsilon)^2)e^{2Z_\epsilon+2K_\epsilon(x-w)}(\beta_\epsilon^{x,w}-Z_\epsilon)\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} Z_r \leq \beta_\epsilon^{x,w}\}}]dwdx$$

On définit une nouvelle mesure de probabilité sur $\mathcal{F}_\epsilon$:

$$\mathbb{P}^{\beta,x,w}(dz) = \frac{1}{\beta_\epsilon^{x,w}}\mathbb{E}^Z[\mathbf{1}_{\{dz\}}(\beta_\epsilon^{x,w}-Z_\epsilon(x))\mathbf{1}_{\{\sup_{s\in[\epsilon,1]} Z_s(x)\leq\beta_\epsilon^{x,w}\}}|\beta_\epsilon^{x,w}]$$

Rappelons que sous cette nouvelle mesure de probabilité, le processus $(\beta_\epsilon^{x,w} - Z_s)_{\epsilon\leq s\leq 1}$ a la même loi que $(\beta_{K_s(x-w)})_{\epsilon\leq s\leq 1}$, où $(\beta_u)_u$ est un processus de Bessel en dimension 3 issu de $\beta_\epsilon^{x,w}$ (voir 5.2). On a donc :

$$\begin{aligned}\Sigma_\epsilon^1 &\leq C \int_A \int_{B(x,\epsilon)} \mathbb{E}^X[\beta_\epsilon^{x,w}\mathbb{E}^{\beta,x,w}[(1+(\beta_\epsilon^{x,w}-\beta_{K_\epsilon(x-w)})^2)e^{2\beta_\epsilon^{x,w}-2\beta_{K_\epsilon(x-w)}+2K_\epsilon(x-w)}]]dwdx \\ &\leq C \int_A \int_{B(x,\epsilon)} \mathbb{E}^X[\beta_\epsilon^{x,w}\mathbb{E}^{\beta,x,w}[(1+(\beta_\epsilon^{x,w})^2)e^{2\beta_\epsilon^{x,w}}(1+(\beta_{K_\epsilon(x-w)})^2)e^{-2\beta_{K_\epsilon(x-w)}+2K_\epsilon(x-w)}]]dwdx\end{aligned}$$

On souligne maintenant une propriété du champ libre gaussien massif (et aussi du champ libre gaussien si l'on n'est pas près du bord) que l'on peut facilement retrouver par le caractère lipschizien du noyau k : il existe une constante uniforme c ne dépendant que du noyau k telle que pour tout $w \in B(x,\epsilon)$,

$$\ln\frac{1}{\epsilon} - c \leq K_\epsilon(x-w) \leq \ln\frac{1}{\epsilon}$$

On calcule maintenant la partie $\mathbb{E}^{\beta,x,w}[(1+(\beta_{K_\epsilon(x-w)})^2)e^{-2\beta_{K_\epsilon(x-w)}}]$.
La loi d'un processus de Bessel en dimension 3 est donné par le carré de la norme d'un mouvement brownien en dimension 3 (voir 5.2). On se donne donc trois mouvements browniens standards unidimensionnels indépendants M^1, M^2 et M^3, et on a :

$$\begin{aligned}&\mathbb{E}^{\beta,x,w}[(1+(\beta_{K_\epsilon(x-w)})^2)e^{-2\beta_{K_\epsilon(x-w)}}] \\ &= \int_{\mathbb{R}^3}(1+(u-\beta_\epsilon^{x,w})^2+v^2+w^2)e^{-\sqrt{(u-\beta_\epsilon^{x,w})^2+v^2+w^2}}e^{-\frac{u^2+v^2+w^2}{2K_\epsilon(x-w)}}\frac{dudvdw}{(2\pi K_\epsilon(x-w))^{\frac{3}{2}}} \\ &\leq C(1+(\beta_\epsilon^{x,w})^2)e^{\beta_\epsilon^{x,w}}\int_{\mathbb{R}^3}(1+u^2+v^2+w^2)e^{-\sqrt{u^2+v^2+w^2}}e^{-\frac{u^2+v^2+w^2}{2K_\epsilon(x-w)}}\frac{dudvdw}{(2\pi K_\epsilon(x-w))^{\frac{3}{2}}} \\ &\leq C(1+(\beta_\epsilon^{x,w})^2)e^{\beta_\epsilon^{x,w}}\int_0^{+\infty}(1+r^2)e^{-r}e^{-\frac{r^2}{2\ln\frac{1}{\epsilon}}}\frac{r^2dr}{(\ln\frac{1}{\epsilon})^{\frac{3}{2}}}\end{aligned}$$

On trouve

$$\mathbb{E}^{\beta,x,w}[(1+(\beta_{K_\epsilon(x-w)})^2)e^{-2\beta_{K_\epsilon(x-w)}}] \leq C(1+(\beta^{x,w})^2)e^{\beta^{x,w}}H(\ln\frac{1}{\epsilon})$$

avec

$$H(a) = \int_0^{+\infty} (1+r^2)e^{-r}e^{-\frac{r^2}{2a}} \frac{r^2 dr}{a^{\frac{3}{2}}}$$

qui vérifie

$$H(a) \leq C(\max(1,a))^{-\frac{3}{2}}$$

pour tout $a \geq 0$.
Finalement

$$\Sigma_\epsilon^1 \leq CH(\ln \frac{1}{\epsilon})\epsilon^{-2} \int_A \int_{B(x,\epsilon)} dwdx \leq C|A|(\ln \frac{1}{\epsilon})^{-\frac{3}{2}}$$

qui tend vers 0 quand $\epsilon \to 0$.
On a utilisé le fait que $\mathbb{E}^X[C\beta_\epsilon^{x,w}(1+(\beta_\epsilon^{x,w})^2)^2 e^{3\beta_\epsilon^{x,w}}]$ est finie et ce indépendamment de x, w (voir 5.12).

• Pour Σ_ϵ^2 :
Remarquons d'abord, par définition même du cut-off, comme $\epsilon \leq |x-w|$ dans cette région, on a $Z_\epsilon^{cut} = Z_{|x-w|}^{cut}$ et rappelons aussi que la partie Z^{off} est à variance finie. Par le théorème de Girsanov,

$$\begin{aligned}
\Sigma_\epsilon^2 = &\int_A \int_{C(x,\epsilon)} \mathbb{E}^X[(\beta - P_\epsilon^{w,x} - Z_\epsilon + 2\ln\frac{1}{\epsilon})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{w,x}+Z_r-2\ln\frac{1}{r}\leq\beta\}} \\
&(\beta - P_\epsilon^{x,w} - Z_\epsilon + 2\ln\frac{1}{\epsilon})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{x,w}+Z_r-2\ln\frac{1}{r}\leq\beta\}} e^{2P_\epsilon^{x,w}+4Z_\epsilon+2P_\epsilon^{w,x}-4\ln\frac{1}{\epsilon}}]dwdx \\
= &\int_A \int_{C(x,\epsilon)} \mathbb{E}^X[(\beta - P_\epsilon^{w,x} - Z_\epsilon)\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{w,x}+Z_r\leq\beta\}} \\
&(\beta - P_\epsilon^{x,w} - Z_\epsilon)\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} P_r^{x,w}+Z_r\leq\beta\}} e^{2Z_\epsilon+2K_\epsilon(x-w)}]dwdx
\end{aligned}$$

On définit maintenant $\alpha_\epsilon^{off} = \sup_{s\in[\epsilon,1]} |Z_s^{off}|$, alors

$$\begin{aligned}
\Sigma_\epsilon^2 \leq &\int_A \int_{C(x,\epsilon)} \mathbb{E}^X[(\beta - Z_\epsilon^{cut} + \alpha^{off} - P_\epsilon^{w,x})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} Z_r^{cut}+P_r^{w,x}\leq\beta+\alpha^{off}\}} \\
&(\beta - Z_\epsilon^{cut} + \alpha^{off} - P_\epsilon^{x,w})\mathbf{1}_{\{\sup_{r\in[\epsilon,1]} Z_r^{cut}+P_r^{x,w}\leq\beta+\alpha^{off}\}} e^{2Z_{|x-w|}^{cut}+2\ln\frac{1}{|x-w|}+2\alpha^{off}}]dwdx \\
\leq &\int_A \int_{C(x,\epsilon)} \mathbb{E}^X[(\beta - Z_{|x-w|}^{cut} + \alpha^{off} - P_{|x-w|}^{w,x})\mathbf{1}_{\{\sup_{r\in[|x-w|,1]} Z_r^{cut}+P_r^{w,x}\leq\beta+\alpha^{off}\}} \\
&(\beta - Z_{|x-w|}^{cut} + \alpha^{off} - P_{|x-w|}^{x,w})\mathbf{1}_{\{\sup_{r\in[|x-w|,1]} Z_r^{cut}+P_r^{x,w}\leq\beta+\alpha^{off}\}} e^{2Z_{|x-w|}^{cut}+2\ln\frac{1}{|x-w|}+2\alpha^{off}}]dwdx
\end{aligned}$$

par le théorème d'arrêt quand l'on a déjà utilisé dans un autre contexte, voir 3.3 (le point c'est que la partie P ne bouge pas entre $|x-w|$ et ϵ donc tout est constant à

part Z^{cut}).
Ce qui suit est exactement le même raisonnement que dans [23], on remplace simplement $\beta^{x,w}$ par $\beta^{x,w}+\alpha^{off}$. À la fin la constante ne sera plus la même, mais comme tout est à variance finie, elle reste finie.
On définit donc $\beta^{x,w}=\beta+\alpha^{off}-\min\limits_{s\in[|x-w|,1]}P_s^{x,w}$ de façon analogue.
Observons que pour $w\in C(x,\epsilon)$, $\sup_{s\in[|x-w|,1]}h_1(s),\sup_{s\in[|x-w|,1]}h_2(s)\leq c$ pour une constante $c>0$ qui ne dépend que du noyau k (donc a fortiori pour h_{cut} aussi). En effet, comme k est l-lipschitzien en 0, on a, pour tout $s\in[|x-w|,1]$ et $w\in C(x,\epsilon)$,

$$\begin{aligned}
h_1(s)=h_2(s)&=\ln\frac{1}{s}-\int_1^{\frac{1}{s}}\frac{k(u(x-w))}{u}du\\
&=\int_1^{\frac{1}{s}}\frac{1-k(u(x-w))}{u}du\\
&\leq\int_1^{\frac{1}{s}}\frac{lu|x-w|}{u}du\\
&\leq l(1-|x-w|)\\
&\leq l
\end{aligned}$$

Il s'ensuit que :

$$\Sigma_\epsilon^2\leq C\int_A\int_{C(x,\epsilon)}\mathbb{E}^X[(1+(Z^{cut}_{|x-w|})^2)e^{2Z_{|x-w|}+2K_{x-w}(x-w)}(\beta^{x,w}-Z^{cut}_{|x-w|})\mathbf{1}_{\{\sup\limits_{r\in[|x-w|,1]}Z_r^{cut}\leq\beta^{x,w}\}}]dwdx$$

On définit une nouvelle mesure de probabilité sur $\sigma((Z_s^{cut})_{s\in[|x-w|,1]})$:

$$\mathbb{P}^{\beta,x,w}(dz)=\frac{1}{\beta^{x,w}}\mathbb{E}^{Z^{cut}}[\mathbf{1}_{\{dz\}}(\beta^{x,w}-Z^{cut}_{|x-w|}(x))\mathbf{1}_{\{\sup_{s\in[|x-w|,1]}Z_s^{cut}(x)\leq\beta^{x,w}\}}|\beta^{x,w}]$$

Rappelons que sous cette nouvelle mesure de probabilité, le processus $(\beta^{x,w}-Z_s^{cut})_{|x-w|\leq s\leq 1}$ a la même loi que $(\beta_{K_s(x-w)})_{|x-w|\leq s\leq 1}$, où $(\beta_u)_u$ est un processus de Bessel en dimension 3 issu de $\beta^{x,w}$ (voir 5.2). On a donc :

$$\begin{aligned}
\Sigma_\epsilon^2&\leq C\int_A\int_{C(x,\epsilon)}\mathbb{E}^X[\beta^{x,w}\mathbb{E}^{\beta,x,w}[(1+(\beta^{x,w}-\beta_{K_{|x-w|}(x-w)})^2)\\
&\quad e^{2\beta^{x,w}-2\beta_{K_{|x-w|}(x-w)}+2K_{x-w}(x-w)+2\alpha^{off}}]]dwdx\\
&\leq C\int_A\int_{C(x,\epsilon)}\mathbb{E}^X[\beta^{x,w}\mathbb{E}^{\beta,x,w}[(1+(\beta^{x,w})^2)e^{2\beta^{x,w}}(1+(\beta_{K_{|x-w|}(x-w)})^2)\\
&\quad e^{-2\beta_{K_{|x-w|}(x-w)}+2K_{x-w}(x-w)+2\alpha^{off}}]]dwdx
\end{aligned}$$

On souligne maintenant une propriété du champ libre gaussien massif (et aussi du champ libre gaussien si l'on n'est pas près du bord) que l'on peut facilement retrouver par le caractère lipschizien du noyau k : il existe une constante uniforme c ne dépendant que du noyau k telle que pour tout $w \in C(x, \epsilon)$,

$$\ln \frac{1}{|x-w|} - c \leq K_{|x-w|}(x-w) \leq \ln \frac{1}{|x-w|}$$

En faisant les mêmes calculs que pour la partie Σ^1_ϵ, on trouve

$$\mathbb{E}^{\beta,x,w}[(1+(\beta_{K_{|x-w|}(x-w)})^2)e^{-2\beta_{K_{|x-w|}(x-w)}}] \leq C(1+(\beta^{x,w})^2)e^{\beta^{x,w}} H(\ln \frac{1}{|x-w|})$$

Finalement

$$\sup_{\epsilon \in]0,1]} \Sigma^2_\epsilon \leq C' \int_A \int_{B(x,1)} \frac{H(\ln \frac{1}{|x-w|})}{|x-w|^2} dwdx < +\infty$$

On a utilisé le fait que $\mathbb{E}^X[C\beta^{x,w}(1+(\beta^{x,w}_\epsilon)^2)^2 e^{3\beta^{x,w}} e^{2\alpha^{off}}]$ est finie indépendamment de x, w (voir 5.12).
En conclusion, on a donc démontré la convergence en $\mathcal{L}^2$ de notre martingale.

• Le reste de la preuve est identique que dans la section précédente.
En effet, comme le noyau k_m pour le champ libre gaussien massif est l-lipschitzien en 0, le résultat sur le maximum d'un champ libre gaussien log-corrélé (théorème 3.5) reste valable. En suivant exactement le même raisonnement que dans la section précédente, on conclut que la martingale dérivée M' peut être construite d'après cette méthode, et qu'elle est p.s. strictement positive. □

Remarque 4.3. *Remarquons que cette preuve marche aussi pour les cut-offs qui vérifient les deux conditions suivantes :*
– ***Noyau** k **localement lipschitzien** : À partir d'un certain ϵ_0, la fonction de covariance K_ϵ est plus grand que*

$$k_\epsilon(r) = \int_{|r|}^{\frac{|r|}{\epsilon}} \frac{k(u)}{u} du$$

avec $k(u) = (1 - \frac{|u|}{T})\mathbf{1}_{[0,T]}(|u|)$ quand ϵ tend vers 0.
– ***Variance finie** : La partie "off" Z^{off} est à variance finie.*
En plus, on n'a pas besoin que k soit un noyau gaussien pour avoir la décomposition en quatre mouvements browniens.
Il en résulte que la même preuve marche aussi pour un champ libre gaussien (on s'intéresse à une partie intérieure du champ, de distance au moins δ du bord). En effet, le comportement du noyau $p^D(t; x, y)$ quand t tend vers l'infini est "presque"

le même que le noyau d'un champ libre gaussien massif. On peut alors récupérer les deux propriétés précédentes dans le cas d'un champ libre gaussien défini à l'intérieur d'un domaine D borné dans le plan, ce qui nous permet de construire de la même façon la martingale dérivée dans le cas critique.
Reste à savoir si toutes les constructions de la martingale dérivée donne la même limite (en loi). Ceci est encore conjectural.

5 Quelques rappels de probabilités

5.1 Quelques théorèmes sur les martingales et les mouvements browniens

On rassemble ici, sans preuve, quelques résultats classiques de probabilités qui nous sont utiles.

Théorème 5.1. ***Théorème de De la Vallée Poussin***
Soit $(M_n)_n$ une martingale. Elle est uniformément intégrable ssi il existe une fonction convexe $F : \mathbb{R}_+ \to \mathbb{R}_+$ et un α fixé positif tels que
1) $\frac{F(x)}{x} \to +\infty$ quand $x \to +\infty$;
2) $F(\lambda x) \leq \lambda^\alpha F(x)$ pour tout $\lambda > 0$;
3) $\sup_n \mathbb{E}[F|M_n|] < +\infty$.

Définition 5.1. ***Bruit blanc***
On rappelle simplement ici la règle de calcul pour les bruits blancs :
Soit W un bruit blanc défini sur un espace E. Alors pour tout couple de fonctions réelles continues (f, g) définies sur E, on a

$$\mathbb{E}[\int_E f(x)W(dx) \int_E g(x)W(dx)] = \int_E f(x)g(y)d\delta(x, y)$$

où $\delta(x, y) = x$ si $x = y$ et $\delta(x, y) = 0$ si $x \neq y$.

Définition 5.2. ***Processus de Bessel***
On considère un mouvment brownien standard d-dimensionnel ($d \geq 1$) B non issu de 0. Notons sa norme $Y_t = |B_t|$. Alors Y_t vérifie l'équation différenteille stochastique :

$$dY_t = \frac{a}{Y_t}dt + d\tilde{B}_t$$

avec $a = \frac{d-1}{2}$ et $\tilde{B}$ un mouvement brownien standard.
On dit que Y est un processus de Bessel d-dimensionnel.

Théorème 5.2. ***Mouvement brownien conditionné à rester positif***
Soit B un $\mathbb{P}$-mouvement brownien issu de x. On considère une nouvelle mesure de probabilité $\mathbb{Q}$ telle que

$$\frac{d\mathbb{Q}_t}{d\mathbb{P}} = x^{-1}B_t\mathbf{1}_{\{0\notin B[0,t]\}}$$

Alors sous $\mathbb{Q}_t$, $(B_s)_{s\leq t}$ vérifie l'équation différentielle stochastique suivante :

$$dB_s = \frac{1}{B_s}ds + d\tilde{B}_s$$

où $\tilde{B}$ est un mouvement brownien standard sous $\mathbb{Q}_t$.
Autrement dit, sous $\mathbb{Q}_t$, $(B_s)_{s\leq t}$ est un processus de Bessel en dimension 3.

Théorème 5.3. ***Lemme de Motoo***
Soit β un processus de Bessel en dimension 3 de loi de départ $\mathbb{P}_x$ (i.e. ce processus part du point x avec probabilité $\mathbb{P}_x$). Alors :
– Soit ϕ une fonction croissante vers $+\infty$ à l'infini telle que $\int_1^{+\infty} \frac{\phi(t)^3}{t} e^{-\frac{1}{2}\phi(t)^2} dt < +\infty$. On a alors

$$\mathbb{P}_x(\limsup_{t\to+\infty}(\beta_t - \sqrt{t}\phi(t)) \geq 0) = 0$$

– Soit ψ une fonction décroissante vers 0 à l'infini telle que $\int_1^{+\infty} \frac{\psi(t)}{t} dt < +\infty$. On a alors

$$\mathbb{P}_x(\liminf_{t\to+\infty}(\beta_t - \sqrt{t}\psi(t)) \leq 0) = 0$$

Les réciproques sont aussi vraies.

On pourra trouver les preuves de ces résultats dans par exemple [4], [1], [14], [20] et [19].

5.2 Quelques inégalités gaussiennes

Les inégalités gaussiennes sont souvent extrêmement simples mais étonnamment puissantes. Nous rappelons quelques inégalités importantes sur les gaussiens qui nous sont utiles.

Théorème 5.4. ***Inégalité de convexité de Kahane***
Soient $(X_i)_{i\in I}$ et $(Y_i)_{i\in I}$ deux familles finies de v.a. réelles gaussiennes. On suppose que $\forall i, j \in I$, $\mathbb{E}[X_iX_j] \leq \mathbb{E}[Y_iY_j]$. Soit $F : \mathbb{R}_+ \to \mathbb{R}$ une fonction convexe avec croissance au plus polynomiale à l'infini. Alors

$$\forall p_i \geq 0, \mathbb{E}[F(\sum_{i\in I} p_i \exp(X_i - \frac{1}{2}\mathbb{E}[X_i^2]))] \leq \mathbb{E}[F(\sum_{i\in I} p_i \exp(Y_i - \frac{1}{2}\mathbb{E}[Y_i^2]))]$$

Démonstration. On commence la preuve avec un lemme simple et connu :

Lemme 5.5. *Soient $X = (X_1, \ldots, X_k)$ un vecteur gaussien centré, et $h : \mathbb{R}^k \to \mathbb{R}$ de classe $\mathcal{C}^1$, telle que h et ses dérivées premières sont à croissance au plus polynomiale à l'infini. Alors $\forall 1 \leq i \leq k$,*

$$\mathbb{E}[X_i h(X)] = \sum_{j=1}^{k} \mathbb{E}[X_iX_j]\mathbb{E}[h_j(X)]$$

où $h_j = \frac{\partial h}{\partial x_j}$.

Montrons ce lemme. Supposons d'abord que la matrice de covariance de X est l'identité. Alors

$$\begin{aligned}\mathbb{E}[X_i h(X)] &= \int_{\mathbb{R}^k} x_i h(x) e^{-\frac{|x|^2}{2}} dx \\ &= \int_{\mathbb{R}^k} h_i(x) e^{-\frac{|x|^2}{2}} dx \\ &= \mathbb{E}[h_i(X)]\end{aligned}$$

où l'on a utilisé simplement une intégration par parties.
Maintenant on suppose que $C = A^T A$ la matrice de covariance de X, et on définit $h'(x) = h(Ax)$. Soit alors $X' = (X'_1, \ldots, X'_k)$ un vecteur gaussien de matrice de covariance la matrice identité. Alors $X = AX'$ en loi, et en notant a_{mn} (resp. a^T_{mn}) les éléments de A (resp. A^T), on a

$$\begin{aligned}\mathbb{E}[X_i h(X)] &= \mathbb{E}[\sum_{m=1}^k a_{im} X'_m h'(X')] \\ &= \sum_{m=1}^k a_{im} \mathbb{E}[h'_m(X')] \\ &= \sum_{m=1}^k a_{im} \mathbb{E}[\sum_{j=1}^k a_{jm} h_j(X)] \\ &= \sum_{j=1}^k \mathbb{E}[h_j(X)] \sum_{j=1}^k a_{im} a^T_{mj} \\ &= \sum_{j=1}^k \mathbb{E}[X_i X_j] \mathbb{E}[h_j(X)]\end{aligned}$$

Ce qui donne le lemme.
On définit

$$\phi(t) = \mathbb{E}[F(\sum_{i=1}^n p_i e^{Z_i(t) - \frac{1}{2}\mathbb{E}[Z_i^2(t)]})]$$

avec $Z_i(t) = \sqrt{t} X_i + \sqrt{1-t} Y_i$.
On note aussi

$$W_{n,t} = \sum_{i=1}^n p_i e^{Z_i(t) - \frac{1}{2}\mathbb{E}[Z_i^2(t)]}$$

Maintenant pour établir le théorème, il suffit de remarquer que la dérivée $\phi'(t)$ est

positive :

$$\begin{aligned}
\phi'(t) &= \mathbb{E}[\frac{1}{2}\sum_{i=1}^{n} p_i(\frac{1}{\sqrt{t}}X_i - \frac{1}{\sqrt{1-t}}Y_i)e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]}F'(\sum_{i=1}^{n} p_i e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]})] \\
&\quad - \mathbb{E}[\frac{1}{2}\sum_{i=1}^{n} p_i(\mathbb{E}[X_i^2]-\mathbb{E}[Y_i^2])e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]}F'(\sum_{i=1}^{n} p_i e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]})] \\
&= \mathbb{E}[\frac{1}{2}\sum_{i,j=1}^{n} p_i p_j(\frac{1}{\sqrt{t}}X_i - \frac{1}{\sqrt{1-t}}Y_i)Z_j]\mathbb{E}[e^{Z_j(t)-\frac{1}{2}\mathbb{E}[Z_j^2(t)]}e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]}F''(W_{n,t})] \\
&\quad + \frac{1}{2}\sum_{i=1}^{n} p_i\mathbb{E}[(\frac{1}{\sqrt{t}}X_i - \frac{1}{\sqrt{1-t}}Y_i)Z_j]\mathbb{E}[e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]}F'(W_{n,t})] \\
&\quad - \mathbb{E}[\frac{1}{2}\sum_{i=1}^{n} p_i(\mathbb{E}[X_i^2]-\mathbb{E}[Y_i^2])e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]}F'(\sum_{i=1}^{n} p_i e^{Z_i(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]})] \\
&= \frac{1}{2}\sum_{i,j=1}^{n} p_i p_j(\mathbb{E}[X_iX_j]-\mathbb{E}[Y_iY_j])\mathbb{E}[e^{Z_i(t)+Z_j(t)-\frac{1}{2}\mathbb{E}[Z_i^2(t)]-\mathbb{E}[Z_j^2(t)]}F''(W_{n,t})
\end{aligned}$$

On conclut alors par la convexité de F. □

On peut retrouver, à l'aide de l'inégalité de convexité de Kahane, le lemme de Slepian qui est une des (vieilles) inégalités classiques dites de comparaison pour les processus gaussiens.

Lemme 5.6. ***Lemme de Slepian***
Soient $(X_i)_{1\le i\le n}$ et $(Y_i)_{1\le i\le n}$ deux vecteurs gaussiens centrés tels que

$$\forall i,j \in [|1,n|], \mathbb{E}[X_iX_j] \le \mathbb{E}[Y_iY_j]$$

et

$$\forall j \in [|1,n|], \mathbb{E}[X_i^2] = \mathbb{E}[Y_i^2]$$

Alors pour toute fonction croissante $F : \mathbb{R}_+ \to \mathbb{R}$, on a :

$$\mathbb{E}[F(\sup_{i=[|1,n|]} Y_i)] \le \mathbb{E}[F(\sup_{i\in[|1,n|]} X_i)]$$

Démonstration. Grâce à Fubini, il suffit de montrer cette inégalité pour les $F = \mathbf{1}_{]x,+\infty[}$ avec $x \in \mathbb{R}$ fixé, i.e. $\mathbb{P}(\sup_{i\in[|1,n|]} X_i < x) \le \mathbb{P}(\sup_{i\in[|1,n|]} Y_i < x)$.

On choisit un $\beta \in \mathbb{R}_+$. On considère ensuite la fonction convexe $\phi(u) = e^{-e^{-\beta x}u}$, les vecteurs $(\beta X_i)_{i\in[|1,n|]}$, $(\beta Y_i)_{i\in[|1,n|]}$ et $(p_i)_{i\in[|1,n|]} = (e^{\beta^2\frac{\mathbb{E}[X_i^2]}{2}})_{i\in[|1,n|]}$. En appliquant l'inégalité de convexité de Kahane, on obtient :

$$\mathbb{E}[e^{-\sum_{i=1}^{n} e^{\beta(X_i-x)}}] \le \mathbb{E}[e^{-\sum_{i=1}^{n} e^{\beta(Y_i-x)}}]$$

En faisant tendre β vers $+\infty$, on trouve :

$$\mathbb{P}(\sup_{i\in[|1,n|]} X_i < x) \leq \mathbb{P}(\sup_{i\in[|1,n|]} Y_i < x)$$

ce qui nous permet de conclure. □

On énonce maintenant l'inégalité de convexité de Kahane sous forme d'intégrale, qui est une généralisation immédiate de la forme précédente (il suffit de considérer une discrétisation des intégrales en somme de Riemann).

Lemme 5.7. ***Inégalité de convexité de Kahane, cas continu***
Soient $(X_t)_{t\in\mathbb{R}}$ et $(Y_t)_{t\in\mathbb{R}}$ deux processus gaussiens centrés tels que leur noyaux de covariance f_X et f_Y soient continus et vérifient $\forall u, t \in \mathbb{R}$, $f_X(t,u) \leq f_Y(t,u)$. Soit μ une mesure de Radon positive sur $\mathbb{R}$. Alors, pour toute fonction convexe $F : \mathbb{R}_+ \to \mathbb{R}$ avec croissance au plus polynomiale à l'infini, on a :

$$\mathbb{E}[F(\int_a^b e^{X_t - \frac{1}{2}\mathbb{E}[X_t^2]}\mu(dt))] \leq \mathbb{E}[F(\int_a^b e^{Y_t - \frac{1}{2}\mathbb{E}[Y_t^2]}\mu(dt))]$$

On rappelle un résultat classique d'une autre classe d'inégalités gaussiennes importantes dites inégalités de concentration.

Théorème 5.8. ***Inégalité de Borell-Tsirelson-Ibragimov-Sudakov***
Soit f_t un processus gaussien centré p.s. borné défini sur un espace T séparable[4]*. On définit*

$$||f|| = ||f||_T = \sup_{t\in T} f_t$$

Alors $\mathbb{E}[||f||] < +\infty$ et pour tout $u > 0$, on a

$$\mathbb{P}[||f|| - \mathbb{E}||f|| > u] \leq e^{-\frac{u^2}{2\sigma_T^2}}$$

avec $\sigma_T^2 = \sup_{t\in T} \mathbb{E}[f_t^2]$.

Démonstration. Suivant [1], on présente une preuve simple basée sur plusieurs lemmes élémentaires.

Lemme 5.9. ***1. Sur le calcul de covariance***
Soient X et Y deux vecteurs gaussiens centrés k-dimensionnels indépendants, chacun ayant pour matrice de covariance Id. Soient $f, g : \mathbb{R}^k \to \mathbb{R}$ deux fonctions bornées de classe $\mathcal{C}^2$. Alors

$$Cov(f(X), g(X)) = \int_0^1 \mathbb{E}[\langle \nabla f(X), \nabla g(\alpha X + \sqrt{1-\alpha^2}Y)\rangle] d\alpha$$

4. Une conséquence immédiate de cette hypothèse est $\sup_{t\in T} f_t = \sup_{t\in D} f_t$ si $D \subset T$ est un ensemble dénombrable dense.

Preuve du lemme 1 :
Il suffit de montrer ce lemme avec $f(x) = e^{i\langle t,x\rangle}$ et $g(x) = e^{i\langle s,x\rangle}$, avec $s, t, x \in \mathbb{R}^k$.
Notons $\phi(t) = \mathbb{E}[e^{i\langle t,X\rangle}] = e^{\frac{|t|^2}{2}}$ la fonction caractéristique de X.
On vérifie que $Cov(f(X), g(X)) = \phi(s+t) - \phi(s)\phi(t)$.
Or

$$\begin{aligned}
&\int_0^1 \mathbb{E}[\langle \nabla f(X), \nabla g(\alpha X + \sqrt{1-\alpha^2}Y)\rangle] d\alpha \\
&= \int_0^1 d\alpha \mathbb{E}[\langle (it_j e^{i\langle t,X\rangle})_j, (is_j e^{i\langle s,\alpha X+\sqrt{1-\alpha^2}Y\rangle})_j] \\
&= -\int_0^1 d\alpha \sum_j s_j t_j \mathbb{E}[e^{i\langle t+\alpha s,X\rangle}]\mathbb{E}[e^{i\langle s,\sqrt{1-\alpha^2}Y\rangle}] \\
&= -\int_0^1 d\alpha \langle s,t\rangle e^{\frac{|t|^2+2\alpha\langle s,t\rangle+|s|^2}{2}} \\
&= -\phi(s)\phi(t)(1-e^{\langle s,t\rangle}) \\
&= \phi(s+t) - \phi(s)\phi(t)
\end{aligned}$$

D'où le lemme.

Lemme 5.10. *2. Une estimation sur le moment exponentiel*
On garde le même X que dans le lemme précédent. Si $h : \mathbb{R}^k \to \mathbb{R}$ est une fonction de classe $\mathcal{C}^2$ 1-lipschitzienne telle que $\mathbb{E}[h(X)] = 0$, alors pour tout $t > 0$,

$$\mathbb{E}[e^{th(X)}] \leq e^{\frac{t^2}{2}}$$

Preuve du lemme 2 :
Soient Y une copie indépendante de X et α une varible aléatoire uniforme sur $[0, 1]$.
On définit

$$(X, Z_\alpha) = (X, \alpha(X) + \sqrt{1-\alpha^2}Y)$$

En appliquant le lemme précédent avec $t \geq 0$ fixé et $g = e^{th}$:

$$\begin{aligned}
\mathbb{E}[h(X)g(X)] &= \int_0^1 \mathbb{E}[\langle \nabla g(X), \nabla h(Z_\alpha)\rangle] d\alpha \\
&= t\int_0^1 \mathbb{E}[\langle \nabla h(X), \nabla h(Z_\alpha)\rangle e^{th(X)}] d\alpha \\
&\leq t\mathbb{E}[e^{th(X)}]
\end{aligned}$$

où l'on a utilise le caractère lipschitzien de h. En définissant u de sorte que $e^{u(t)} = \mathbb{E}[e^{th(X)}]$, alors

$$\mathbb{E}[h(X)e^{th(X)}] = u'(t)e^{ut}$$

D'où $u'(t) \leq t$. Or $u(0) = 0$, on a donc $u(t) \leq \frac{t^2}{2}$, qui donne le lemme.

Lemme 5.11. ***3. Sur la probabilité de déviation***
On garde le même X que précédemment. Soit $h : \mathbb{R}^k \to \mathbb{R}$ σ-lipschitzienne. Alors $\forall u > 0$,

$$\mathbb{P}[h(X) - \mathbb{E}[h(X)] > u] \leq e^{-\frac{u^2}{2\sigma^2}}$$

Preuve du lemme 3 :
Par scaling, on peut supposer que $\sigma = 1$. Quitte à prendre une approximation en $\mathcal{C}^2$ de f et d'appliquer le lemme de Fatou, on peut supposer que $f \in \mathcal{C}^2$.
Pour tout $t, u > 0$,

$$\begin{aligned}\mathbb{P}[h(X) - \mathbb{E}[h(X)] > u] &\leq \int_{h(x)-\mathbb{E}[h(X)]>u} e^{t(h(x)-\mathbb{E}[h(X)]-u)} d\mathbb{P}(x) \\ &\leq e^{-tu}\mathbb{E}[e^{th(X)-\mathbb{E}[h(X)]}] \\ &\leq e^{\frac{1}{2}t^2-tu}\end{aligned}$$

En optimisant (prenons $t = u$), on obtient ce lemme.

On est maintenant en mesure de montrer l'inégalité de Borell-TIS.
On étudie d'abord le cas où T est fini. Disons $T = \{1, \ldots, k\}$.
Le cas i.i.d. a déjà été traité : c'est le lemme 3 car la constante de lipschitz pour la fonction sup est 1.
Soit donc $C = A^T A$ la matrice de covariance $(k \times k)$ de f sur T, de coefficients $c_{ij} = \mathbb{E}[f_i f_j]$, de sorte que

$$\sigma_T^2 = \max_{1\leq i\leq k} c_{ii} = \max_{1\leq i\leq k} \mathbb{E}[f_i^2]$$

On peut alors voir f comme une transformation affine d'un vecteur gaussien standard W de matrice de covariance Id_k : en effet, $f = AW$ en loi (donc $\max_i f_i = \max_i (AW)_i$ en loi).
Considérons ensuite $h(x) = \max_i (Ax)_i$, qui est de classe $\mathcal{C}^2$. Le théorème en découle dans ce cas si l'on peut montrer que

$$|\max_i (Ax)_i - \max_i (Ay)_i| \leq \sigma_T |x - y|$$

Ceci est une conséquence de l'inégalité de Cauchy-Schwarz. En effet, en notant e_i les vecteurs élémentaires :

$$\begin{aligned}|\max_i (Ax)_i - \max_i (Ay)_i| &= |\max_i (e_i Ax) - \max_i (e_i Ay)| \\ &\leq \max_i |e_i A(x - y)| \\ &\leq \max_u |e_i A| \cdot |x - y| \\ &= \sigma_T |x - y|\end{aligned}$$

car $|e_i A|^2 = (e_i)^T C e_i = c_{ii}$.
Passons maintenant au cas général.
Soit $(T_n)_{n\in\mathbb{N}}$ une suite croissante vers un ensemble dense dans T. Par séparabilité

$$\sup_{t\in T_n} f_t \to \sup_{t\in T} f_t$$

presque sûrement.
Or cette convergence est monotone, on a donc

$$\mathbb{P}[\sup_{t\in T_n} f_t \geq u] \to \mathbb{P}[\sup_{t\in T} f_t \geq u]$$

et

$$\mathbb{E}[\sup_{t\in T_n} f_t] \to \mathbb{E}[\sup_{t\in T} f_t]$$

Comme $\sigma^2_{T_n} \to \sigma^2_T < +\infty$ (de façon monotone), il suffit de montrer, pour établir l'inégalité de Borell-TIS, que le membre de droite $\mathbb{E}[\sup_{t\in T} f_t]$ est fini.
On procède par l'absurde. Supposons que $\mathbb{E}[||f||] = +\infty$. On choisit alors $u_0 > 0$ tel que

$$e^{-\frac{u_0^2}{\sigma_T^2}} \leq \frac{1}{4}, \mathbb{P}[\sup_{t\in T} f_t < u_0] \geq \frac{3}{4}$$

Choisissons T_n tel que $\mathbb{E}[||f||_{T_n}] > 2u_0$. En appliquant l'inégalité de Borell-TIS (version T fini) à T_n, on a

$$\begin{aligned}\frac{1}{2} \geq 2e^{-\frac{u_0^2}{\sigma_T^2}} \geq 2e^{-\frac{u_0^2}{\sigma_{T_n}^2}} &\geq \mathbb{P}[|||f||_{T_n} - \mathbb{E}[||f||_{T_n}]| > u_o] \geq \mathbb{P}[\mathbb{E}[||f||_{T_n}] - ||f||_T > u_o] \\ &\geq \mathbb{P}[||f||_T < u_0] \geq \frac{3}{4}\end{aligned}$$

Contradiction. Ceci finit d'établir l'inégalité de Borell-TIS. □

On énonce maintenant une conséquence importante cette inégalité qui dit, *grosso modo*, que la bornitude du supremum assure l'existence de certaines moments exponentiels pour les processus gaussiens centrés.

Lemme 5.12. ***Sur les moments exponentiels d'une v.a. gaussienne***
Soit f_t un processus gaussien centré. Alors

$$\mathbb{P}[||f|| < +\infty] = 1 \Longleftrightarrow \mathbb{E}[||f||] < +\infty \Longleftrightarrow \mathbb{E}[e^{\alpha||f||^2}] < +\infty$$

pour un α suffisamment petit.

Démonstration. On sait déjà que l'existence d'un moment exponentiel entraîne l'existence de $\mathbb{E}[||f||]$, qui à son tour entraîne la finitude p.s. de $||f||$.
L'inégalité de Borell-TIS nous apprend directement que la finitude p.s. de $||f||$ entraîne celle de $\mathbb{E}[||f||]$. Il suffit donc de montrer que la finitude p.s. de $||f||$ entraîne l'existence des moments exponentiels.
Ceci résulte encore de l'inégalité de Borell-TIS. On a

$$\begin{aligned}
\mathbb{E}[e^{\alpha||f||^2}] &= \int_0^{+\infty} \mathbb{P}[e^{\alpha||f||^2} > u]du \\
&\leq e^{\alpha} + \mathbb{E}[||f||] + 2\int_{\max(e^{\alpha},\mathbb{E}[||f||])}^{+\infty} \mathbb{P}[||f|| > \sqrt{\ln u^{\frac{1}{\alpha}}}]du \\
&\leq e^{\alpha} + \mathbb{E}[||f||] + 2\int_{\max(e^{\alpha},\mathbb{E}[||f||])}^{+\infty} \exp(\frac{-(\sqrt{\ln u^{\frac{1}{\alpha}}} - \mathbb{E}[||f||])^2}{2\sigma_T^2})du \\
&\leq e^{\alpha} + \mathbb{E}[||f||] + 4\alpha\int_0^{+\infty} u\exp(\frac{-(u-\mathbb{E}[||f||])^2}{2\sigma_T^2})\exp(\alpha u^2)du
\end{aligned}$$

et pour un α suffisamment petit, cette quantité est bornée. □

On remarque que ce résultat est valable pour $\sup_{t\in T}|f_t|$ au lieu de $||f||$, car

$$\mathbb{P}[\sup_{t\in T}|f_t| > u] \leq 2\mathbb{P}[\sup_{t\in T} f_t > u]$$

par symétrie.
On pourra trouver les preuves et les extensions de ces résultats dans par exemple [11], [22], [1] et [15].

5.3 Rappels sur les champs gaussiens

5.3.1 Définition du champ gaussien

Un champ gaussien est un processus gaussien défini sur un espace ambient. D'après [1], on dit "un champ gaussien" quand on s'intéresse davantage à ses propriétés géométriques.
Un champ gaussien défini sur $\mathbb{R}^d$ est dit stationnaire si pour tout $z \in \mathbb{R}^d$, $(X_t)_{t\in\mathbb{R}^d}$ et $(X_{z+t})_{t\in\mathbb{R}^d}$ ont la même loi. Lui est associé l'objet suivant :

Définition 5.3. ***Fonction de type-positif***
Si X est un processus gaussien stationnaire, alors son noyau de covariance $f_X(u,v)$ ne dépend que de la différence $u-v$. On définit alors

$$g(u-v) = f_X(u,v)$$

Remarquons qu'alors g est de type positif (c'est le caractère défini positif du noyau f_X), i.e.

$$\forall n \geq 1, \forall t_1, \ldots, t_n \in \mathbb{R}^d, \forall x_1, \ldots, x_n \in \mathbb{C}, \sum_{i,j=1}^{n} x_i \overline{x}_j g(t_i - t_j) \geq 0$$

On appelle aussi g la fonction de covariance du processus gaussien stationnnaire X. Tout comme la matrice de covariance caractérise la structure d'un vecteur gaussien, la fonction de covariance caractérise la structure d'un champ gaussien stationnaire :

Théorème 5.13. *Soit g une fonction réelle paire de type positif sur $\mathbb{R}^d$. Alors il existe un processus stationnaire centré gaussien réel admettant g pour fonction de covariance.*

5.3.2 Fonction de Green

La fonction de Green est l'un des objets fondamentaux en mathématiques qui apparaît dans beaucoup de domaines. Pour la simplicité de la présentation on rappelle ici simplement une façon probabiliste d'introduire la fonction de Green largement inspirée du livre de [14], via la théorie du potentiel (cf. [5] par exemple). Dans la suite on se restreint au cas $d = 2$, mais la construction est valide (et plus simple) en dimension supérieure.

Définition 5.4. ***Mouvement brownien tué au bord***
On se donne un domaine $D \subset \mathbb{R}^2$ ouvert connexe. Soit $x \in D$. On considère un mouvement brownien plan standard issu de x mais tué quand il touche le bord du domaine D noté $\not{B}$.
On note, pour $y \in D$, $p_D(t; x, y)$ la densité de transition du $\not{B}$, i.e.

$$p_D(t; x, y) = \lim_{\epsilon \to 0} \frac{1}{\pi \epsilon^2} \mathbb{P}^x(|\not{B}_t - y| < \epsilon, \tau_D > t) = \mathbb{P}^x(\not{B}_t \in dy, \tau_D > t)$$

où τ_D désigne le temps de sortie du mouvement brownien $\not{B}$ du domaine D, i.e. le premier instant qu'il atteint le bord du domaine D.
On dit que $p_D(t; x, y)$ est le semi-groupe de transition pour un mouvement brownien plan standard tué au bord de D.

Dans la suite on se restreint au cas où D est un domaine borné (pour assurer que $\mathbb{P}^x[\tau_D < +\infty]$, qui à son tour assure que la fonction de Green ne diverge pas en dehors de la diagonale, voir par exemple [10]).

Définition 5.5. ***Fonction de Green***
La fonction de Green G_D définie sur un domiane D borné est donnée par

$$\forall x, y \in D, G_D(x, y) = \int_0^{+\infty} p_D(t; x, y) dt$$

Définition 5.6. ***Une autre définition équivalente***
Une autre façon de définir la fonction de Green en dimension 2 (voir par exemple [10] pour une différente preuve) est de dire que c'est la plus petite fonction positive $G : D \times D \to \mathbb{R}_+$, $G = K + H$ parmi celles qui vérifie les conditions suivantes :
1) $G < +\infty$ en dehors de la diagonale ;
2) $G(a, b) = G(b, a)$;
3) $K = -\frac{1}{2\pi} \ln |b - a|$;
4) $\Delta_a H = \Delta_b H = 0$.

Sans vouloir entrer dans les détails techniques et de recopier les preuves classiques, expliquons de façon informelle comment on peut obtenir ces propriétés de façon probabiliste.
La positivité de G est immédiate car la densité de transition est positive.
La symétrie (propriété 2) résulte de la symétrie du noyau p^D. Intuitivement, il suffit d'"inverser" le chemin du mouvement brownien qui part de x et qui arrive sur le bord de $B(y, \epsilon)$, puis de faire une translation d'une distance ϵ pour obtenir un chemin du mouvement brownien qui part de y et qui arrive sur le bord de $B(x, \epsilon)$ tout en restant dans le domaine D. Le détail technique consiste à dire que pendant la translation la probabilité que le chemin touche le bord de D est petite : on évalue donc la probabilité que le tube de taille ϵ autour d'un chemin brownien de x vers y touche le bord de D, qui s'avère comporter comme un $o(\epsilon^2)$.
L'harmonicité (propriété 4) est assez simple, on peut la montrer par la propriété de la moyenne (en utilisant la propriété de Markov et de conditionner quand le mouvement brownien tué sort de $B(x, \epsilon)$ pour ϵ petit) par exemple.
Les propriétés 1 et 3 résultent par exemple de la comparaison de p^D avec la densité de transition p d'un mouvement brownien plan standard non tué, à savoir $p(t; x, y) = \frac{1}{2\pi t} e^{-\frac{|x-y|^2}{2t}}$. On constate que $\int_0^{+\infty} p^D(t; x, y)dt$ n'est pas très loin de $\int_0^1 p(t; x, y)dt$ (en montrant la convergence de $\int_1^{+\infty} p^D(t; x, y)dt$, voir [14], lemme 2.29), et un calcul montre que $\int_0^1 p(t; x, y)dt$ est égal à $\frac{1}{\pi} \ln \frac{1}{|x-y|}$ modulo une constante.

5.3.3 Champ libre gaussien (GFF)

On rappelle ici la définition et quelques propriétés du champs libre gaussien (ou ***g****aussian* ***f****ree* ***f****ield* en anglais) sur un domain borné $D \subset \mathbb{R}^2$. Pour un traité plus complet sur le champ libre gaussien on pourra consulter l'article [25].

Définition 5.7. ***Une construction directe du champs libre gaussien***
On considère un bruit blanc W distribué sur $D \times \mathbb{R}_+$. On définit alor

$$X(x) = \sqrt{\pi} \int_{D \times \mathbb{R}_+} p_D(\frac{s}{2}; x, y) W(dy, ds)$$

et on appelle X le champ libre gaussien défini sur le domain D.

On vérifie tout de suite que la fonction de covariance pour ce champ est donnée par

$$\mathbb{E}[X(x)X(x')] = \pi \int_0^{+\infty} p_D(s; x, x')ds = G_D(x, x')$$

Autrement dit, le champ libre gaussien défini sur un domaine borné $D \subset \mathbb{R}^2$ est un champ gaussien dans $\mathbb{R}^2$ dont la fonction de covariance est donnée par la fonction de Green sur le domaine D. Mais attention, comme le fonction de Green diverge sur la diagonale, très souvent dans les calculs liés au champ libre gaussien, on manipule plutôt des distributions au sens de Schwartz que des fonctions au sens classique.

Remarque 5.1. ***Invariance conforme***
Le champ libre gaussien possède la propriété remarquable d'invariance conforme, alors que le champ libre gaussien massif que l'on rappelle dans la suite n'en possède pas.

5.3.4 Champ libre gaussien massif (MGFF)

On rappelle ici la définition et quelques propriétés du champ libre gaussien massif (ou ***m**assive **g**aussian **f**ree **f**ield* en anglais) sur $\mathbb{R}^2$ (on pourra consulter par exemple [8], [25] pour une définition rigoureuse et complète) :
– On fixe un paramètre m (la masse).
– On définit la fonction de Green massive sur $\mathbb{R}^2$:

$$\forall x, y \in \mathbb{R}^2, G_m(x, y) = \int_0^{\infty} e^{-mu - \frac{|x-y|^2}{2u}} \frac{du}{2u}$$

Remarquons que cette fonction est finie en dehors de la diagonale. En effet, une autre façon de définir la fonction de Green massive analogue à celle présentée précédemment est d'utiliser un mouvmement brownien tué en un temps suivant la loi exponentielle de paramètre m (au lieu d'un mouvmement brownien tué au bord d'un domaine). On pourra consulter entre autres [18] pour plus de détails sur cette fonction.
– Le champ libre gaussien massif sur $\mathbb{R}^2$ est défini comme un champ gaussien ayant pour fonction de covariance la fonction de Green massive.
– On pourra réécrire G_m de la façon suivante :

$$G_m(x, y) = \int_1^{\infty} \frac{k_m(u(x-y))}{u} du$$

avec $k_m(z) = \frac{1}{2} \int_0^{\infty} e^{-\frac{m}{v}|z|^2 - \frac{v}{2}} dv$.
Cette écriture montre par ailleurs que le noyau est star-scale invariant, voir [2] par exemple.

5.4 Un lemme sur le processus du branchement

Ce théorème donne une estimation des petits moments de la fonction de partition d'un processus du branchement. Il a été démontré dans [9] (théorème 1.6).
Rappelons rapidement la situation. On considère un arbre de Galton-Watson $\mathbb{T}$. Écrivons $|u| = n$ si un individu u se trouve dans la n-ième génération.
Initialement, un individu se trouve au point 0. Ses enfants forment la première génération, et sont distribués sur $\mathbb{R}$ selon la loi d'un processus ponctuel. Chacun de ces enfants vont avoir ses enfants (qui forment la génération suivante), et leurs déplacements relatifs se font selon le même processus ponctuel indépendamment. Et ainsi de suite. On note la position d'un individu $V(u)$. $V(u)$ est donc la somme des déplacements des ses ancêtres.
On définit la fonction génératrice (logarithmique)

$$\phi(t) = \ln \mathbb{E}[\sum_{|u|=1} e^{-tV(u)}]$$

et la fonction de partition

$$W_{n,\beta} = \sum_{|u|=n} e^{-\beta V(u)}$$

pour $\beta > 0$.

Théorème 5.14. *Sous les trois hypothèses suivantes :*
1) $\mathbb{E}[(\sum_{|u|=1} 1)^{1+\delta}] < +\infty$ *;*
2) $\mathbb{E}[\sum_{|u|=1} e^{-(1+\delta_+)V(u)}] + \mathbb{E}[\sum_{|u|=1} e^{\delta_- V(u)}] < +\infty$ *;*
3) $\phi(0) > 0$, $\phi(1) = \phi'(1) = 0$.
pour certains $\delta > 0$, $\delta_+ > 0$, $\delta_- > 0$.
On a, pour $\beta > 1$ *et* $0 < r < \frac{1}{\beta}$ *:*

$$\mathbb{E}[W_{n,\beta}^r] = n^{-\frac{3r\beta}{2}+o(1)}$$

quand $n \to +\infty$.

Dans le cas qui nous intéresse, on considère un arbre de Cayley (ou plus simplement un arbre binaire), et on attache une variable aléatoire i.i.d. (dite potentiel) à chaque arête de l'arbre indépendamment les unes les autres. En réalité, on n'utilise que la partie "borne supérieure" dans ce théorème.

Références

[1] R. J. Adler et J. E. Taylor : *Random fields and geometry*, vol. 115. Springer, 2007.

[2] R. Allez, R. Rhodes et V. Vargas : Lognormal star-scale invariant random measures. *Probability Theory and Related Fields*, p. 1–38, 2013.

[3] M. Bramson, J. Ding et O. Zeitouni : Convergence in law of the maximum of the two-dimensional discrete gaussian free field. *arXiv preprint arXiv :1301.6669*, 2013.

[4] C. Dellacherie et P.-A. Meyer : *Probabilities and Potential, B : Theory of Martingales*. Elsevier, 2011.

[5] J. L. Doob : *Classical potential theory and its probabilistic counterpart*, vol. 262. Springer, 2001.

[6] B. Duplantier, R. Rhodes, S. Sheffield et V. Vargas : Critical gaussian multiplicative chaos : convergence of the derivative martingale. *arXiv preprint arXiv :1206.1671*, 2012.

[7] B. Duplantier, R. Rhodes, S. Sheffield et V. Vargas : Renormalization of critical gaussian multiplicative chaos and kpz formula. *arXiv preprint arXiv :1212.0529*, 2012.

[8] C. Garban, R. Rhodes et V. Vargas : Liouville brownian motion. *arXiv preprint arXiv :1301.2876*, 2013.

[9] Y. Hu et Z. Shi : Minimal position and critical martingale convergence in branching random walks, and directed polymers on disordered trees. *The Annals of Probability*, 37(2):742–789, 2009.

[10] K. Itô et H. P. MacKean : *Diffusion Processes and Their Sample Paths*, vol. 1431. Springer, 1996.

[11] J.-P. Kahane : Sur le chaos multiplicatif. *Ann. Sci. Math. Québec*, 1985.

[12] J.-P. Kahane et J. Peyrière : Sur certaines martingales de benoit mandelbrot. *Advances in Mathematics*, 22(2):131 – 145, 1976.

[13] H. Lacoin, R. Rhodes et V. Vargas : Complex gaussian multiplicative chaos. *arXiv preprint arXiv :1307.6117*, 2013.

[14] G. F. Lawler : *Conformally invariant processes in the plane*, vol. 114. AMS Bookstore, 2008.

[15] M. Ledoux et M. Talagrand : *Probability in Banach Spaces : isoperimetry and processes*, vol. 23. Springer, 1991.

[16] T. Madaule : Maximum of a log-correlated gaussian field. *arXiv preprint arXiv :1307.1365*, 2013.

[17] B. B. Mandelbrot : Intermittent turbulence in self-similar cascades- divergence of high moments and dimension of the carrier. *Journal of Fluid Mechanics*, 62(2):331–358, 1974.

[18] P. Mörters et Y. Peres : *Brownian motion*, vol. 30. Cambridge University Press, 2010.

[19] M. Motoo : Proof of the law of iterated logarithm through diffusion equation. *Annals of the Institute of Statistical Mathematics*, 10(1):21–28, 1959.

[20] D. Revuz et M. Yor : *Continuous martingales and Brownian motion*, vol. 293. Springer, 1999.

[21] R. Rhodes : Processus stochastiques multifractaux et applications. 2012.

[22] R. Rhodes et V. Vargas : Gaussian multiplicative chaos and applications : a review. *arXiv preprint arXiv :1305.6221*, 2013.

[23] R. Rhodes et V. Vargas : Liouville brownian motion at criticality. *en préparation*, 2013.

[24] R. Robert et V. Vargas : Gaussian multiplicative chaos revisited. *The Annals of Probability*, 38(2):605–631, 2010.

[25] S. Sheffield : Gaussian free fields for mathematicians. *Probability theory and related fields*, 139(3-4):521–541, 2007.

Quatrième partie

Mémoire de M1

Le problème de Noether pour les groupes abéliens

Diego IZQUIERDO & Yichao HUANG
Sous la direction d'Olivier WITTENBERG

2011

Table des matières

1 Introduction: le problème de Noether et la preuve de Fischer 3

2 Quelques prérequis d'algèbre et de théorie des nombres 5
2.1 Modules sur les anneaux de Dedekind 5
2.1.1 Modules projectifs 5
2.1.2 Anneaux de Dedekind 6
2.1.3 Modules de type fini sur un anneau de Dedekind 9
2.2 Entiers algébriques 12
2.2.1 Norme, trace et discriminant 13
2.2.2 Indice de ramification et degré résiduel 15
2.2.3 Anneau des entiers de $\mathbb{Q}(\zeta)$ 16
2.2.4 Anneau des entiers d'un corps quadratique 18
2.3 Norme d'un idéal 19

3 Le contre-exemple de Swan 21
3.1 Construction d'un invariant dans le groupe de Grothendieck 21
3.2 Construction d'un deuxième invariant dans le groupe des classes . . 24
3.3 Le contre-exemple de Swan 26

4 Résolution du problème de Noether pour un groupe abélien 29
4.1 Un peu de cohomologie des groupes finis 29
4.2 Notations, objectif et stratégie 31
4.3 Facteurs directs de permutation 32
4.4 Liens entre les modules de permutation et les extensions transcendantes pures 34
4.5 Construction du module F_ρ et liens avec les extensions transcendantes pures 37
4.6 Étude des modules I_q et J_q 43
4.7 Un lemme pour se ramener au cas où $car(k)$ ne divise pas l'ordre de G 50
4.8 Preuve du théorème de Lenstra 53

5 Quelques conséquences lorsque le groupe est cyclique 57

Références 63

1 Introduction: le problème de Noether et la preuve de Fischer

Soit k_0 un corps et soit $K_0 = k_0(X_1, ..., X_n)$ le corps des fractions rationnelles à n indéterminées. Soit G un sous-groupe du groupe symétrique $\mathcal{S}_n$. Faisons agir G sur K_0 par permutation des variables. L'extension $K_0^G|k_0$ est-elle transcendante pure?
Ce problème, dit "de Noether" même si Emmy Noether n'avait jamais conjecturé que la réponse serait affirmative, est apparu vers la fin du XIXème siècle. Il a attiré l'attention de nombreux mathématiciens, et est toujours un sujet de recherche. Le cas où $G = \mathcal{S}_n$ est un résultat classique: dans ce cas, K_0^G est engendré par les polynômes symétriques à n variables sur k_0, famille qui est bien algébriquement indépendante.
Le premier résultat général a été démontré par Fischer, en 1915, dans [Fis15]: il montre que le problème de Noether admet une réponse affirmative lorsque G est abélien, k_0 contient toutes les racines e-ièmes de l'unité où e est l'exposant de G et $car(k_0)$ ne divise pas e. À partir de là, tout le long de la deuxième moitié du XXème siècle, des articles sont parus donnant des réponses affirmatives au problème dans des cas particuliers. Ainsi, en 1955, Kuniyoshi prouve dans [Kun56] que si k_0 est de caractéristique $p > 0$ et si G est un p-groupe, alors K_0^G est bien une extension transcendante pure de k_0. En 1964, dans [Mat64], Matsuda améliore le résultat de Fisher dans le cas où G est cyclique. Parallèlement à ces études générales, Masuda a étudié le problème pour de petites valeurs de n. C'est ainsi qu'il montre en 1955 dans [Mas55] que lorsque $n \leq 7$, $car(k_0)$ ne divise pas n et G est cyclique d'ordre n, $K_0^G|k_0$ est transcendante pure. Il arrive ensuite à la même conclusion lorsque $n = 11$, $car(k_0) \neq 11$ et G est cyclique d'ordre n: la preuve se trouve dans [Mas68].
Cependant, dans certains cas, l'extension $K_0^G|k_0$ n'est pas transcendante pure. Jusqu'à la fin des années 1960, les mathématiciens conjecturent que le problème de Noether admet toujours une réponse affirmative. Si cette conjecture était vraie, elle permettrait de montrer à l'aide du théorème d'irréductibilité de Hilbert que lorsque k est un corps de nombres, tout groupe fini est le groupe de Galois d'une extension galoisienne de k. Mais en 1969, Swan publie l'article [Swa69] dans lequel il prouve que lorsque G est cyclique d'ordre n, $k_0 = \mathbb{Q}$ et n vaut 47, 113 ou 233, alors l'extension $K_0^G|k_0$ n'est pas transcendante pure. Un peu plus tard, en 1973, Endo et Miyata améliorent ces résultats dans [EM73] en arrivant à la même conclusion que Swan dans le cas où G est cyclique d'ordre 8, 121, 169...
Finalement, en 1974, Lenstra publie l'article [Len74] dans lequel il donne une condition nécessaire et suffisante pour que l'extension $K_0^G|k_0$ soit transcendante pure dans le cas où G est abélien fini et agit transitivement sur les n variables. Ce

résultat constitue un avancement majeur dans l'étude du problème de Noether. Cependant, encore de nos jours, le problème reste ouvert: dans le cas où le groupe G ne serait pas abélien, très peu de résultats sont connus, mais même dans des cas qui peuvent paraître simples, comme le cas où $G = \mathbb{Z}/53\mathbb{Z}$ et $k_0 = \mathbb{Q}$, le problème n'est pas résolu.
L'objet de ce mémoire est d'étudier le problème de Noether dans le cas d'un groupe abélien. Nous allons d'abord rappeler les résultats classiques d'algèbre et de théorie des nombres dont nous aurons besoin (partie 2). Nous supposons cependant connues la théorie de Galois, les représentations linéaires des groupes finis, ainsi que des notions d'algèbre commutative et d'algèbre multilinéaire. Ensuite, nous détaillerons le raisonnement de Swan pour prouver que dans le cas où $G = \mathbb{Z}/47\mathbb{Z}$, le problème a une réponse négative (partie 3). Puis nous montrerons le théorème de Lenstra (partie 4) dont nous donnerons un certain nombre de conséquences (partie 5).
Avant de commencer notre étude, nous voudrions remercier chaleureusement Olivier Wittenberg pour son soutien constant, sa disponibilité, l'aide précieuse qu'il a apportée au cours du travail et pour nous avoir fait découvrir ce problème passionnant.

Commençons par le théorème de Fischer qui donne une réponse affirmative au problème de Noether dans un cas très particulier.

Théorème 1.0.1. ***Théorème de Fischer***
Soient G un groupe abélien fini d'exposant e et V une représentation de dimension finie sur un corps k_0. Si le corps k_0 contient toutes les racines e-ièmes de l'unité et si la caractéristique de k_0 ne divise pas e, alors $k_0(V)^G/k_0$ est une extension transcendante pure, où $k_0(V)^G$ désigne le sous-corps fixe du corps des fractions de l'algèbre symétrique de V sur k_0.

Preuve. Comme G est abélien fini et le corps contient les racines e-ièmes de l'unité, la représentation V s'écrit comme somme directe de représentations de dimension 1. Prenons $(y_1, \ldots, y_n)$ une base adaptée à cette décomposition.
Comme V est engendré par la famille des $(y_i)_i$ en tant qu'espace vectoriel, un quotient dans le corps des fractions de l'algèbre symétrique de V s'écrit comme un élément dans $k_0(y_1, \ldots, y_n)$. La famille $(y_i)_i$ est algébriquement indépendante, donc le sous-groupe multiplicatif Y engendré par $(y_1, \ldots, y_n)$ du groupe $k_0(V)^*$ est abélien libre de base $(y_1, \ldots, y_n)$.
Considérons maintenant le morphisme de groupes Φ de Y dans $X = Hom(G, k_0^*)$ qui à chaque y_i associe le caractère de la représentation restreinte à la droite y_i. On affirme que si $I = Ker\Phi$, alors $k_0(V)^G$ s'identifie à $k_0(I)$. En effet, $k_0[I] = k_0[Y]^G$, et $k_0(I)^G$ est le corps des fractions de $k_0[I]^G$. Le groupe I étant un sous-groupe

de Y, qui est libre de type fini sur $\mathbb{Z}$, il est abélien libre de type fini, et donc $k_0(I) = k_0(V)^G$ est une extension transcendante pure de k_0. $\square$

Si dans le théorème précédent on choisit la représentation V l'espace vectoriel de base x_i avec l'action de G donnée par celle de permutation, on obtient exactement que le problème de Noether tel qu'il a été énoncé au début de cette partie admet une réponse affirmative lorsque G est abélien fini d'exposant e, $car(k_0)$ ne divise pas e et k_0 contient toutes les racines e-ièmes de l'unité.
La démonstration de Fischer met en évidence une méthode naturelle et directe de montrer qu'une extension est transcendante pure. Il est beaucoup plus difficile de montrer qu'une extension ne l'est pas. Le contre-exemple de Swan, qui montre que le problème de Noether n'admet pas toujours une réponse affirmative, consiste à attacher un invariant aux extensions de corps, s'annulant lorsque l'extension est transcendante pure. Mais avant d'établir ce contre-exemple, nous avons besoin de quelques prérequis.

2 Quelques prérequis d'algèbre et de théorie des nombres

2.1 Modules sur les anneaux de Dedekind

Dans cette partie, nous allons nous intéresser à des anneaux dits de Dedekind. Nous allons en particulier étudier la structure des idéaux dans un tel anneau, puis celle des modules. Nous verrons que, comme dans les anneaux principaux, tout idéal non nul s'écrit de manière unique comme produit d'idéaux premiers, puis nous remarquerons qu'il est possible d'établir une classification des modules sur un anneau de Dedekind qui rappelle énormément celle des modules sur un anneau principal.
On supposera dans cette section que les anneaux considérés sont commutatifs.

2.1.1 Modules projectifs

Soit A un anneau.

Définition 2.1.1. ***Modules projectifs***
On dit qu'un module P sur un anneau A est ***projectif*** *s'il vérifie l'une des trois propriétés équivalentes ci-dessous:*
1) Étant donnés M, M' deux A-modules quelconques, un morphisme surjectif g de M sur M' et un morphisme f de P dans M', il existe un morphisme h de P dans

M tel que le diagramme commute:

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"'] & M' \arrow[r] & 0 \end{tikzcd}$$

2) Quels que soient M et M' deux A-modules, dès que $0 \to M' \to M \to P \to 0$ est exacte, elle est scindée.
3) Il existe un A-module S tel que $P \oplus S$ soit libre.

Preuve. Montrons que ces trois propriétés sont bien équivalentes.
1) $\Rightarrow$ 2) On se donne une suite exacte $0 \to M' \to M \to P \to 0$, on note $g : M \to P$ la surjection de la suite exacte, et on considère

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "Id"] & \\ M \arrow[r, "g"'] & P \arrow[r] & 0 \end{tikzcd}$$

Le morphisme h fournit une section de la suite exacte.
2) $\Rightarrow$ 3) Il est aisé de trouver une suite exacte courte $F \to P \to 0$ où F est libre (par exemple, on choisit F dont une base est construite sur une famille génératrice de P). Alors la section donnée par 2) nous permet de d'écrire $F = P \oplus S$ pour un certain S.
3) $\Rightarrow$ 1) Comme $Hom_A(X \oplus Y, M) = Hom_A(X, M) \oplus Hom_A(Y, M)$, et comme $M \mapsto Hom_A(F, M)$ est un foncteur exact si F est libre, 3) impose que $M \mapsto Hom_A(P, M)$ est un foncteur exact. Il suffit de voir ensuite que si $M \mapsto Hom_A(P, M)$ est exacte, alors P vérifie 1). Par conséquent, si on se donne M, M', f et g comme en 1), on déduit de la suite exacte $0 \to Ker(g) \to M \to M' \to 0$ que la suite $0 \to Hom_A(P, Ker(g)) \to Hom_A(P, M) \to Hom_A(P, M') \to 0$ est exacte, et alors la partie droite de cette suite exacte montre 1). $\square$

2.1.2 Anneaux de Dedekind

Nous allons à présent définir les anneaux de Dedekind, puis nous allons étudier les idéaux dans un tel anneau.

Définition 2.1.2. ***Anneaux de Dedekind***
On dit qu'un anneau commutatif unitaire intègre A est ***de Dedekind*** *s'il vérifie les trois conditions suivantes:*
a) A est noethérien;
b) A est intégralement clos;
c) Tout idéal premier non nul de A est maximal.

L'étude des idéaux dans un anneau de Dedekind s'avère particulièrement intéressante, puisque, comme nous allons le voir, les idéaux fractionnaires forment un groupe (pour la multiplication d'idéaux).

Définition 2.1.3. ***Idéaux fractionnaires***
Soit A un anneau et soit K son corps des fractions. On appelle ***idéal fractionnaire*** *de A un sous-A-module non nul I de K tel qu'il existe un élément non nul d de A vérifiant $dI \subset A$. On appellera* ***idéal entier*** *un idéal au sens usuel, par opposition aux idéaux fractionnaires.*
De manière analogue à la multiplication usuelle des idéaux, on peut définir IJ comme l'ensemble des combinaisons linéaires finies de I et de J. On vérifie aussi que IJ est un idéal fractionnaire.
On définit enfin la ***divisibilité*** *des idéaux fractionnaires: $I|J$ s'il existe L idéal entier de A tel que $J = IL$.*

Dans la suite, A sera un anneau de Dedekind, et K son corps des fractions.

Lemme 2.1.4. ***Loi de simplification***
Soit I un idéal fractionnaire de A. Alors il existe un idéal fractionnaire J tel que IJ soit un idéal principal non nul de A.
Corollaire: Soient I, J, L trois idéaux fractionnaires de A. Si $IJ = IL$ alors $J = L$.

Preuve. Commençons par remarquer que tout idéal entier I non nul de A contient un produit fini d'idéaux premiers non nuls.
En effet, procédons par l'absurde. Supposons que l'ensemble $\mathbb{I}$ des idéaux ne contenant aucun produit fini d'idéaux premiers non nuls est non vide. Comme A est noethérien, toute suite croissante d'idéaux est stationnaire, donc l'inclusion sur $\mathbb{I}$ est un ordre inductif. D'après le lemme de Zorn, on peut trouver un idéal m maximal dans $\mathbb{I}$ qui ne contient pas de produit fini d'idéaux premiers non nuls. L'idéal m n'est pas premier et $m \neq A$, donc il existe r, s dans $A - m$ tels que $rs \in m$. Mais on remarque que $(m + (s))(m + (r))$ est dans m, et par maximalité de m, $m + (s)$ et $m + (r)$ contiennent chacun un produit fini d'idéaux premiers non nul, donc m aussi, ce qui est contradictoire.
Montrons un deuxième résultat préliminaire: si I est un idéal entier propre de A, alors il existe $d \in K - A$ tel que $dI \subset A$.
Soit $x \in I$ non inversible, et on choisit $p_1 \dots p_r \subset (x)$ avec r minimal ($r \neq 0$). I est inclus dans un idéal maximal p qui est premier. Alors $p_1 \dots p_r \subset p$, et par primalité de p, il existe p_i tel que $p_i \subset p$, disons $i = 1$. Cette inclusion est en fait une égalité par maximalité de p_i. Puis par minimalité de r, il existe un élément y dans $p_2 \dots p_r - (x)$, et alors $d = y/x$ convient.
Montrons maintenant le lemme.

Soit I un idéal fractionnaire, et soit $i \in I$ non nul. Considérons l'idéal $J = \{x \in A, xI \subset (i)\}$. Remarquons d'une part que J est non nul, d'autre part que $IJ \subset (i)$. S'il y a égalité dans la dernière inclusion, on a fini. Sinon, IJ/i est un idéal entier propre de A et on peut lui appliquer le résultat préliminaire: il existe $d \in K - A$ tel que $dIJ/i \subset A$. Montrons qu'on a forcément dans ce cas $d \in A$, ce qui fournira une contradiction.
Comme $i \in I$, on a $J \subset IJ/i$, donc $dJ \subset dIJ/i \subset A$. Par définition de J, on déduit que $dJ \subset J$. Maintenant on peut interpréter cette inclusion sous forme matricielle: soit $j_1, \ldots, j_m$ une famille de générateurs de J, alors on peut écrire chaque dj_k comme une combinaison linéaire d'éléments de cette famille, ce qui fournit une matrice M de taille $m \times m$ à coefficients dans A telle que $(d - M)(j_k) = 0$, (j_k) étant le vecteur colonne des j_k. En inversant le système à l'aide de la comatrice, on obtient que $det(d - M) = 0$. Or $det(d - M)$ est un polynôme unitaire en d, à coefficients dans A. Comme A est intégralement clos, $d \in A$, absurde.
Le corollaire de ce lemme en découle facilement: il suffit de multiplier I par un autre idéal bien choisi pour que le produit soit un idéal principal, puis d'effectuer une division par le générateur de cet idéal principal. □

Lemme 2.1.5. ***Les idéaux fractionnaires d'un anneau de Dedekind forment un groupe***
Dans un anneau de Dedekind, les idéaux fractionnaires forment un groupe.

Preuve. Le seul point qui manque est l'existence d'un inverse, ce qui est garanti par la première partie de la loi de simplification. □

Ce lemme nous permet de définir la notion de groupe des classes:

Définition 2.1.6. ***Groupe des classes***
On appelle ***groupe des classes*** *le groupe des idéaux fractionnaires quotienté par le sous-groupe des idéaux fractionnaires principaux.*

On remarque au passage que grâce au lemme précédent, la relation de division coïncide avec la relation d'inclusion pour les anneaux de Dedekind.

Théorème 2.1.7. ***Décomposition en produit d'idéaux premiers***
Si l'anneau de Dedekind A n'est pas un corps, alors chaque idéal non trivial I de A s'écrit de manière unique comme produit d'idéaux premiers.

Preuve. Commençons par montrer l'unicité de la même façon que pour la factorisation des nombres premiers.
Unicité: supposons que $I = P_1 \ldots P_r = Q_1 \ldots Q_s$, avec les P_i et les Q_i idéaux premiers non nuls pas forcément deux à deux distincts. Alors $P_1 \supset Q_1 \ldots Q_s$ donc $P_1 \supset Q_i$ pour un certain i par primalité. Cette inclusion est en fait une égalité par

maximalité puisque A est un anneau de Dedekind. Finalement, en vertu de la loi de simplification, par une récurrence simple, on peut identifier terme à terme les P_i et Q_i, d'où l'unicité.
Existence: Par l'absurde. Comme A est noethérien, en procédant comme pour la démonstration du lemme 2.1.4, avec le lemme de Zorn, on peut trouver un idéal m qui soit maximal dans l'ensemble des idéaux qui ne s'écrivent pas sous la forme d'un produit d'idéaux premiers et distincts de (0) et de (1). Alors m est inclus dans un idéal maximal p. D'après le lemme précédent, on peut trouver un idéal propre I tel que $m = pI$, et alors $m \subset I$. Mais si $m = I$ alors $pm = m$ donc $p = A$, absurde. Donc I est produit d'idéaux premiers par maximalité de m, et par conséquent m l'est aussi car $m = pI$, absurde. □

On peut aussi montrer que la décomposition en produit d'idéaux premiers est une condition nécessaire et suffisante pour qu'un anneau soit de Dedekind, mais on n'aura pas besoin dans la suite de cette caractérisation.

Remarque 2.1.8. ***Analogie et intérêt***
L'énoncé de cette dernière propriété est l'analogue du théorème de décomposition en facteurs premiers dans le cas d'un anneau factoriel. Dans les anneaux non factoriels (exemple classique: $\mathbb{Z}[\sqrt{-3}]$: on a $2 \times 2 = (1+\sqrt{-3})(1-\sqrt{-3})$), on ne peut pas espérer une factorialité en produit d'éléments premiers, mais on peut espérer qu'un tel anneau est de Dedekind, d'où une factorisation des idéaux.

La remarque suivante sera utile dans la suite:

Remarque 2.1.9. *Soit I un idéal de A. Alors I est engendré par deux éléments.*

Preuve. L'idéal I est de type fini: disons $I = (a_1, ..., a_n)$. Soit $J = (a_1)$. Montrons d'abord que tout idéal de A/J est principal. D'après le théorème des restes chinois, il suffit de le faire lorsque $J = P^s$, où P est un idéal premier. Les idéaux propres de A/J sont alors P/P^s, P^2/P^s,...,P^{s-1}/P^s. Pour chaque j, on choisit $x_j \in P^j - P^{j+1}$. Alors le pgcd de (x_j) et de P^s est P^j et donc $P^j = (x_j) + P^s$. Ainsi P^j/P^s est engendré par la classe de x_j et est principal. Par conséquent, tout idéal de A/J est bien principal.
On en déduit que I/J est un idéal principal de A/J. Soit $a \in I$ tel que la classe de a dans A/J est un générateur de I/J. Il est clair que $(a_1, a) \subseteq I$. Réciproquement, soit $b \in I$. Alors la classe de b modulo J est dans I/J et donc $b \in (a_1, a)$. Donc $I = (a_1, a)$ □

2.1.3 Modules de type fini sur un anneau de Dedekind

Afin de construire une classification des modules de type fini sur un anneau de Dedekind, nous aurons besoin de la proposition suivante:

Lemme 2.1.10. ***Somme directe des idéaux fractionnaires***
Soit I, J deux idéaux fractionnaires d'un anneau de Dedekind A. Alors $I \oplus J \cong A \oplus IJ$. On a donc aussi $\bigoplus_{i=1,\dots,n} I_i \cong A^{n-1} \oplus \prod_{i=1,\dots,n} I_i$, où les I_i sont des idéaux fractionnaires de A.

Preuve. On peut supposer que I et J sont premiers entre eux dans A quitte à multiplier par des éléments de K (rappelons que K désigne le corps des fractions de A). En effet, on peut déjà supposer que I et J sont dans A, quitte à multiplier par un élément de A. On peut alors les décomposer en produits d'idéaux premiers, disons $I = \prod P_i^{r_i}$ et $J = \prod P_i^{r'_i}$, avec des puissances positives. Puis on choisit un élément a tel que les ordres des P_i dans la décomposition de (a) soient exactement les r_i. Pour ce faire, on choisit pour chaque i un élément $x_i \in P_i^{r_i} - P_i^{r_i+1}$ et on prend a tel que $a \equiv x_i \pmod{P_i^{r_i+1}}$ pour tout i (grâce au théorème des restes chinois). Soit α idéal propre de A tel que $I\alpha = (a)$. De la même façon on choisit β idéal propre et un élément b tels que $\alpha\beta = (b)$, et tels que les P_i et les facteurs premiers de α ne soient pas facteurs premiers de β. Alors $bI/a = (\alpha\beta)I(\alpha^{-1}I^{-1}) = \beta$, qui est premier avec J par construction.
On définit alors l'application $\pi : I \oplus J \to A$ par $\pi(i,j) = i+j$, de noyau $I \cap J = IJ$ et d'image A car I et J sont premiers entre eux. Alors la suite

$$0 \longrightarrow IJ \longrightarrow I \oplus J \longrightarrow A \longrightarrow 0$$

est exacte et scindée car A est libre. D'où la conclusion. □

Étudions à présent la structure des modules projectifs:

Lemme 2.1.11. ***Stucture des modules projectifs de type fini sur un anneau de Dedekind***
Soient A un anneau de Dedekind et K son corps des fractions. Un module M de type fini sur A est projectif si, et seulement si, il est sans torsion.
De plus, si $M \neq 0$ est projectif, alors $M \cong A^{n-1} \oplus I$ où $n = rang(M) = dim_K(M \otimes_A K) > 0$ et I un idéal de A.

Preuve. Montrons qu'un module de type fini M sur A est projectif si et seulement s'il est sans torsion. Si M est projectif, alors il existe un module S tel que $S \oplus M$ libre en tant que A-module, donc M est sans torsion. Réciproquement, supposons que M est sans torsion, et procédons par récurrence sur $n = rang(M)$. Si $n = 1$, alors M est un sous A-module de type fini de $M \otimes_A K \cong K$, et donc il est isomorphe à un idéal fractionnaire, projectif d'après 2.1.10.
Maintenant si on choisit $n-1$ éléments de M tels que le sous-espace vectoriel V qu'ils engendrent dans $M \otimes_A K$ est de dimension $n-1$, on peut construire le sous-A-module $N = \{m \in M, m \otimes_A 1 \in V\}$ de M de rang $n-1$. La suite exacte

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

reste exacte après avoir tensorisé avec K, donc M/N est de rang 1. Donc M/N étant sans torsion, il est projectif et la suite est scindée. La récurrence est établie, et le résultat en découle par le lemme précédent. $\square$

Le lemme précédent nous donne l'existence d'un certain idéal I. Le lemme suivant nous donne l'unicité de cet idéal à isomorphisme près:

Lemme 2.1.12. *Soit A un anneau de Dedekind et K son corps des fractions. Soient n et m des entiers naturels et I et J des idéaux non nuls tels que $A^n \oplus I \cong A^m \oplus J$. Alors $n = m$ et $I \cong J$.*

Preuve. On a $I \otimes_A K \cong K$ et $J \otimes_A K \cong K$. En tensorisant l'isomorphisme donné, on a alors $K^{n+1} \cong K^{m+1}$, d'où $n = m$.
D'autre part, on a $\bigwedge^{n+1}(A^n \oplus I) \cong \bigwedge^{n+1}(A^n \oplus J)$, donc

$$\bigoplus_{p+q=n+1} (\bigwedge^p (A^n) \otimes \bigwedge^q (I)) \cong \bigoplus_{p+q=n+1} (\bigwedge^p (A^n) \otimes \bigwedge^q (J))$$

Comme I et J sont engendrés par au plus deux éléments, on obtient un isomorphisme $I \oplus \Lambda^2(I)^n \cong J \oplus \Lambda^2(J)^n$. Les deux éléments qui engendrent un idéal de A ne pouvant pas être libres, $\Lambda^2(I)$ et $\Lambda^2(J)$ sont de torsion, alors que I et J ne le sont pas. Donc $I \cong J$. $\square$

Nous pouvons finalement établir une classification des modules de type fini sur un anneau de Dedekind:

Théorème 2.1.13. ***Structure des modules de type fini sur un anneau de Dedekind***
Soit M un module de type fini sur un anneau de Dedekind A. Alors $M \cong M_0 \oplus M_1$, où M_0 est sans torsion et M_1 est de torsion. Si $M_0 \neq 0$, il existe un unique idéal non nul I à isomorphisme près et un unique entier naturel n tels que $M_0 \cong A^n \oplus I$. Il existe des idéaux premiers uniques $P_1, ..., P_q$ et des uniques entiers strictement positifs $r_1, ..., r_q$ tels que $M_1 \cong \bigoplus A/P_i^{r_i}$.

Preuve. Soit $Tor(M)$ le sous-module de torsion de M. La suite exacte $0 \to Tor(M) \to M \to M/Tor(M) \to 0$ est scindée puisque $M/Tor(M)$ est sans torsion et donc projectif (2.1.11). On peut donc écrire $M \cong M/Tor(M) \oplus Tor(M)$. $M/Tor(M)$ a déjà été étudié. Intéressons-nous à $Tor(M)$.
Notons J l'annulateur de $TorM$, i.e. $J = \{a | aTor(M) = 0\}$. Comme M est de type fini, $Tor(M)$ l'est aussi, donc J est non nul. Par le théorème de décomposition des idéaux premiers, $J = \prod P_i^{r_i}$, où P_i sont des idéaux premiers de A.
Le théorème des restes chinois permet d'écrire l'isomorphisme de A/J-modules: $Tor(M) \cong \bigoplus Tor(M)/P_i^{r_i} Tor(M)$. Afin d'étudier $Tor(M)/P^r Tor(M)$ pour un

idéal premier P et un entier strictement positif r, montrons le lemme suivant:
<u>Lemme:</u> Soit N un module de type fini sur A/P^r où A est un anneau de Dedekind, P un idéal premier non nul, et r un entier strictement positif. Alors N est isomorphe à une somme directe de modules de la forme A/P^s pour $1 \leq s \leq r$.
<u>Preuve du lemme:</u> Procédons par récurrence sur r. Pour $r = 1$, l'énoncé est évident par la théorie des espaces vectoriels, puisque A/P est un corps. Soit maintenant $r > 1$. Soit $x_1, ..., x_n$ une base du A/P-espace vectoriel $P^{r-1}N$. Soient $\alpha \in P^{r-1}/P^r$ et $y_1, ..., y_n \in N$ tels que $x_i = \alpha y_i$. Soit $N' = N/(y_1 A/P^r \oplus ... \oplus y_n A/P^r)$. Le module N' est alors un A/P^{r-1}-module, donc, par hypothèse de récurrence, on peut écrire: $N' = \bigoplus_{0<i<r}(A/P^i)^{a_i}$. On a alors la suite exacte:

$$0 \to y_1 A/P^r \oplus ... \oplus y_n A/P^r \to N \to \bigoplus_{i<r}(A/P^i)^{a_i} \to 0$$

Montrons qu'elle est scindée. Considérons $N'' = A/P^i$ un des facteurs directs de N'. Soit $x \in N$ dont la projection dans N' vaut $1 \in N''$. Soit $\beta \in P^i/P^r - P^{i+1}/P^r$. Alors $\beta x \in y_1 A/P^r \oplus ... \oplus y_n A/P^r$, d'où $P^{r-i}\beta x = 0$. Donc $\beta x \in y_1 P^i/P^r \oplus ... \oplus y_n P^i/P^r$. Il existe donc $y \in y_1 A/P^r \oplus ... \oplus y_n A/P^r$ tel que $\beta(x - y) = 0$. Soit $z = x - y$. On vérifie alors facilement qu'il existe un morphisme de A/P^r-modules $g : N'' \to N$ tel que $g(1) = z$. En sommant sur tous les facteurs N'' de N', on arrive à scinder la suite exacte précédente. On a donc

$$N \cong (A/P^r)^n \oplus \bigoplus_{0<i<r} (A/P^i)^{a_i}$$

Reste à voir l'unicité des P_i. Écrivons donc $N \cong \bigoplus_{P,i}(A/P^i)^{a_{P,i}} \cong \bigoplus_{P,i}(A/P^i)^{b_{P,i}}$, où P décrit les idéaux premiers et i les entiers naturels, avec $a_{P,0} = 0$. Étant donné un idéal premier P_0 et un entier j, la dimension du A/P_0-espace vectoriel $P_0^j N/P_0^{j+1}N$ est $\sum_{i=j+1}^{\infty} a_{P_0,i} = \sum_{i=j+1}^{\infty} b_{P_0,i}$. L'unicité en découle immédiatement. □

Exemple 2.1.14. $\mathbb{Z}[\zeta]$ ***est un anneau de Dedekind***
Si ζ est une racine de l'unité, $\mathbb{Z}[\zeta]$ est l'anneau de entiers de $\mathbb{Q}(\zeta)$ et est un anneau de Dedekind.

Preuve. La preuve fera l'objet de la section qui suit. □

2.2 Entiers algébriques

L'objectif central de cette partie va être de déterminer l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$, où ζ est une racine primitive de l'unité. Rappelons donc brièvement les notions d'entier et de fermeture intégrale.

Soient A un anneau intègre et K son corps des fractions. Soit $L|K$ une extension finie. On dit qu'un élément $b \in L$ est un **entier sur** A s'il est racine d'un polynôme unitaire à coefficients dans A. On parlera d'**entier algébrique** lorsque $A = \mathbb{Z}$. On appelle **fermeture intégrale** de A dans L l'ensemble des entiers sur A dans L. On parlera d'**anneau des entiers** lorsque $A = \mathbb{Z}$. On dit qu'un anneau est **intégralement clos** s'il est intègre et s'il est sa propre fermeture intégrale dans son corps des fractions. La fermeture intégrale de A dans L est alors intégralement close. Nous voulons donc déterminer la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(\zeta)$.

2.2.1 Norme, trace et discriminant

Commençons en définissant quelques notions liées aux extensions de corps qui vont être essentielles pour la suite. Considérons $L|K$ une extension finie de degré n. Nous allons définir la norme et la trace d'un élément de L:

Définition 2.2.1. ***Norme et trace d'un élément***
Soit $x \in L$. Soit $f_a : x \mapsto ax$. Il s'agit d'un endomorphisme du K-espace vectoriel L. On définit alors la ***norme*** *et la* ***trace*** *de x par: $N_{L/K}(a) = det(f_a)$ et $Tr_{L/K}(a) = Tr(f_a)$.*

On supposera dans le reste de cette section que l'extension est séparable. Dans ce cas, on peut alors calculer la norme et la trace d'un élément facilement grâce à la proposition suivante:

Proposition 2.2.2. ***Calcul explicite de la norme et la trace***
Soit Ω une clôture algébrique de K. Alors le polynôme caractéristique de f_a est donné par: $\chi(f_a) = \prod_\sigma (X - \sigma(a))$, où σ décrit les K-morphismes $L \to \Omega$.

Preuve. Soient d le degré de a et $d' = \dfrac{n}{d}$. On considère $a_1, ..., a_{d'}$ une base de $L|K(a)$. Soit $P = \sum c_k X^k$ le polynôme minimal de a. Alors, dans la base $(a^{i-1}a_j)_{1 \leq i \leq d, 1 \leq j \leq d'}$ de $L|K$, la matrice de f_a est diagonale par blocs, chaque bloc étant une matrice compagnon

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -c_{d-1} \end{pmatrix}$$

Donc $\chi(f_a) = P^{d'} = \prod_\sigma (X - \sigma(a))$, puisque, $L|K$ étant séparable, chaque racine de P apparaît exactement d' fois parmi les $\sigma(a)$. $\square$

On en déduit immédiatement les relations:

$$N_{L/K}(a) = \prod_{\sigma} \sigma(a)$$

et

$$Tr_{L/K}(a) = \sum_{\sigma} \sigma(a)$$

Définissons à présent le discriminant d'une base du K-espace vectoriel L:

Définition 2.2.3. ***Discriminant***
Si $b_1, \ldots, b_n$ est une base de L et Ω une clôture algébrique de K, on définit le ***discriminant*** *de $b_1, \ldots, b_n$ par: $d(b_1, \ldots, b_n) = det(\sigma_i(b_j))^2$, où les σ_i décrivent les K-morphismes $L \to \Omega$. Remarquons que, l'extension étant séparable, son degré et son degré séparable coïncident, et donc le discriminant est bien défini.*

De plus, en tenant compte de la proposition précédente, on remarque que la matrice $(Tr_{L/K}(b_i b_j))_{i,j}$ est égale au produit de la matrice $(\sigma_i(b_j))_{i,j}$ par sa transposée, donc $d(b_1, ..., b_n) = det(Tr_{L/K}(b_i b_j))$. Il semble donc naturel d'étudier le discriminant en s'intéressant à la forme bilinéaire symétrique du K-espace vectoriel L donnée par $\beta : (x, y) \to Tr_{L/K}(xy)$, d'où la proposition suivante:

Proposition 2.2.4. ***Le discriminant est non nul***
β est non dégénérée et $d(b_1, \ldots, b_n) \neq 0$.

Preuve. D'après le théorème de l'élément primitif, il existe $z \in L$ tel que $L = K(z)$. Alors, dans la base $(1, z, \ldots, z^{n-1})$, la matrice de β est $(Tr_{L/K}(z^{i-1} z^{j-1}))_{i,j}$, dont le déterminant est $d(1, z, ..., z^{n-1}) \neq 0$ puisque la matrice $(\sigma_i(z^j))$ est la matrice de Vandermonde associée aux conjugués de z. Donc β est non dégénérée, et sa matrice dans la base $(b_1, \ldots, b_n)$ étant $(Tr_{L/K}(b_i b_j))_{i,j}$, $d(b_1, \ldots, b_n) \neq 0$. □

Mais... pourquoi avons-nous défini le discriminant? Quel est le lien avec les entiers algébriques? Considérons A un anneau intègre et son corps des fractions K. Supposons que A est intégralement clos. Soient alors $L|K$ une extension finie séparable et B la fermeture intégrale de A dans L. Remarquons alors que, étant algébrique sur K, tout élément de L s'écrit $\frac{b}{a}$, avec $b \in B$ et $a \in A$. L'anneau A étant intégralement clos, $A = B \cap K$, et donc, si $b \in B$, les conjugués de b dans Ω étant aussi des entiers sur A, en vertu de $N_{L/K}(b) = \prod_{\sigma} \sigma(b)$ et $Tr_{L/K}(b) = \sum_{\sigma} \sigma(b)$, on a $N_{L/K}(b) \in A$ et $Tr_{L/K}(b) \in A$. Une fois ces remarques faites, l'utilité du discriminant découle de la proposition suivante:

Proposition 2.2.5. ***Propriété fondamentale du discriminant***
Soit $(b_1, \ldots, b_n)$ une base de L contenue dans B. Soit $d = d(b_1, \ldots, b_n)$. Alors $dB \subseteq b_1 A + ... + b_n A$.

Preuve. Soit $b = a_1b_1 + ... + a_nb_n \in B$, avec $a_i \in K$. Montrons que, pour tout i, $da_i \in A$. On remarque que, pour tout i, on a: $Tr_{L/K}(bb_i) = a_1Tr_{L/K}(b_1b_i) + \cdots + a_nTr_{L/K}(b_nb_i)$. On reconnaît ici un système linéaire dont les a_i sont solutions. La matrice de ce système est $T = (Tr_{L/K}(b_ib_j))_{i,j}$, dont le déterminant est d. Comme $d \neq 0$, T est inversible, d'inverse $\dfrac{{}^tCom(T)}{d}$, où ${}^tCom(T)$ est la transposée de la comatrice de T. Comme les coefficients de ${}^tCom(T)$ et les $Tr_{L/K}(bb_i)$ pour $1 \leq i \leq n$ sont dans A d'après les remarques précédentes, en inversant le système, on obtient bien que $da_i \in A$ pour tout i. □

2.2.2 Indice de ramification et degré résiduel

Gardons les notations et hypothèses de la partie précédente. Supposons de plus que A est de Dedekind. Commençons par montrer que B est aussi un anneau de Dedekind:

Proposition 2.2.6. ***La fermeture intégrale est un anneau de Dedekind*** *B est un anneau de Dedekind.*

Preuve. B est intégralement clos par définition.
Montrons qu'il est noethérien. Considérons une base $(b_1, \ldots, b_n)$ de L contenue dans B (elle existe puisque tout élément de L est quotient d'un élément de B par un élément de A). Alors, d'après les propositions 2.2.4 et 2.2.5, si l'on pose $d = d(b_1, \ldots, b_n)$, alors $d \neq 0$ et $B \subseteq \dfrac{b_1}{d}A + \cdots + \dfrac{b_n}{d}A$. L'anneau A étant noethérien et $\dfrac{b_1}{d}A + \cdots + \dfrac{b_n}{d}A$ étant un A-module de type fini, B l'est aussi, ainsi que tout idéal de B. Par conséquent, tout idéal de B est un B-module de type fini, et B est bien noethérien.
Reste à prouver que tout idéal premier non nul de B est maximal. Soit Π un idéal premier non nul de B. Alors $A \cap \Pi$ est un idéal premier non nul de A. Donc, comme les idéaux premiers non nuls de A sont maximaux, $A/(A \cap \Pi)$ est un corps, et B/Π est alors une algèbre intègre sur $A/(A \cap \Pi)$, de dimension finie. En écrivant alors le polynôme minimal d'un élément x non nul de B/Π, on s'aperçoit que x est inversible dans B/Π. Donc B/Π est un corps et Π est maximal. Nous avons ainsi montré que B est de Dedekind. □

Remarquons que nous avons prouvé que B est un A-module de type fini.
Soit π un idéal premier non nul de A. On note alors $\Pi = \pi B$: c'est un idéal de B, et il est distinct de B. En vertu de 2.1.7, B étant de Dedekind, on peut donc écrire $\Pi = \Pi_1^{e_1} \ldots \Pi_r^{e_r}$, où les Π_i sont des idéaux premiers de B. Remarquons que $\pi = \Pi_i \cap A$. On dit que les e_i sont les **indices de ramification** et les

$f_i = [B/\Pi_i : A/\pi]$ sont les **degrés résiduels**. Alors les indices de ramification et les degrés résiduels satisfont une équation remarquable:

Proposition 2.2.7. ***Lien entre les indices de ramification et les degrés résiduels***
$n = e_1 f_1 + \cdots + e_r f_r$.

Preuve. D'après le théorème des restes chinois, on a l'isomorphisme de A/π-espaces vectoriels: $B/\Pi \cong \bigoplus_{i=1}^{r} B/\Pi_i^{e_i}$. Montrons que $dim(B/\Pi) = n$ et que $dim(B/\Pi_i^{e_i}) = e_i f_i$.
B/Π est de dimension finie car B est un A-module de type fini. Soient $b_1, \ldots, b_k \in B$ tels que $\overline{b_1}, \ldots, \overline{b_k}$ est une base de B/Π.
Montrons d'abord que $b_1, \ldots, b_k$ est libre sur K. Supposons qu'elle ne l'est pas. Alors elle n'est pas libre sur A. Considérons donc une relation de liaison non triviale $\sum_{i=1}^{k} a_i b_i = 0$, $a_i \in A$. Soit l'idéal $I = (a_1, ..., a_k)$ dans A. Soit $a \in I^{-1} - I^{-1}\pi$. Alors, après passage modulo π, la relation $\sum_{i=1}^{k} a a_i b_i = 0$ fournit une relation de liaison non triviale entre les $\overline{b_i}$: absurde! Donc $b_1, \ldots, b_k$ est libre sur K.
Montrons à présent que $b_1, \ldots, b_k$ engendre L. Soient les A-modules $M = Ab_1 + \cdots + Ab_k$ et $N = B/M$. L'anneau B étant un A-module de type fini, M et N sont aussi des A-modules de type fini. Soient donc $\lambda_1, \ldots, \lambda_s$ des générateurs de N. Par définition de $b_1, \ldots, b_k$, $B = M + \Pi$, donc $N = \pi N$. On peut donc écrire $\lambda_i = \sum_{j=1}^{s} a_{ij}\lambda_j$, $a_{ij} \in \pi$. Notons T la matrice $(a_{ij}) - Id$, et $\Lambda =^t (\lambda_1, \ldots, \lambda_s)$. Alors $T\Lambda = 0$. Donc, en inversant avec la comatrice, $(detT)\Lambda = 0$, et alors $(detT)N = 0$, d'où $(detT)B \subseteq M$. Comme de plus $detT$ est non nul puisqu'il n'est pas congru à 0 modulo π, $L = (detT)L$ est bien engendré par $b_1, \ldots, b_k$. Donc $dim(B/\Pi) = n$.
Montrons finalement que $dim(B/\Pi_i^{e_i}) = e_i f_i$. Remarquons que, si $a \in \Pi_i^v - \Pi_i^{v+1}$, alors $B \to \Pi_i^v/\Pi_i^{v+1}$, $x \mapsto ax$ est une application linéaire surjective de noyau Π_i, puisque le pgcd de (a) et de Π_i^{v+1} est Π_i^v et alors $(a) + \Pi_i^{v+1} = \Pi_i^v$. On déduit que $\Pi_i^v/\Pi_i^{v+1} \cong B/\Pi_i$. Donc dans la suite d'espaces vectoriels emboîtés $(0) \subseteq \Pi_i^{e_i-1}/\Pi_i^{e_i} \subseteq \cdots \subseteq \Pi_i/\Pi_i^{e_i} \subseteq B/\Pi_i^{e_i}$, chaque quotient est isomorphe à B/Π_i, et $dim(B/\Pi_i^{e_i}) = e_i f_i$. □

2.2.3 Anneau des entiers de $\mathbb{Q}(\zeta)$

Soit ζ une racine primitive m-ième de l'unité. On se place ici dans le cas où $A = \mathbb{Z}$, $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta)$. On note toujours n le degré de $L|K$. Remarquons que l'extension $L|K$ est bien finie séparable et que A est bien intégralement clos. Pour déterminer l'anneau des entiers de $\mathbb{Q}(\zeta)$, nous allons procéder par récurrence. Le lemme suivant établit la propriété d'hérédité:

Lemme 2.2.8. ***Propriété d'hérédité***
Soient ζ_1 et ζ_2 des racines primitives m_1-ième et m_2-ième de l'unité, avec $m_1 \wedge$

$m_2 = 1$. *Soient* $m = m_1 m_2$ *et* ζ *une racine primitive* m*-ième de l'unité. Soient* $n_1 = [\mathbb{Q}(\zeta_1) : \mathbb{Q}]$ *et* $n_2 = [\mathbb{Q}(\zeta_2) : \mathbb{Q}]$. *On suppose que les anneaux des entiers dans* $\mathbb{Q}(\zeta_1)$ *et* $\mathbb{Q}(\zeta_2)$ *sont respectivement* $\mathbb{Z}[\zeta_1]$ *et* $\mathbb{Z}[\zeta_2]$. *On suppose de plus que les discriminants respectifs* $d_1 = d(1, \zeta_1, \ldots, \zeta_1^{n_1-1})$ *et* $d_2 = d(1, \zeta_2, \ldots, \zeta_2^{n_2-1})$ *sont des entiers premiers entre eux. Alors l'anneau des entiers* B *de* $\mathbb{Q}(\zeta)$ *est* $\mathbb{Z}[\zeta]$ *et* $d = d(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) = d_1^{n_2} d_2^{n_1}$.

Preuve. On remarque aisément que $(\zeta_1^i \zeta_2^j)_{0 \leq i < n_1, 0 \leq j < n_2}$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\zeta)$ (la famille est génératrice et a la bonne dimension). Montrons que c'est une base du $\mathbb{Z}$-module B. Soit $b = \sum_{i,j} a_{ij} \zeta_1^i \zeta_2^j \in B$, $a_{ij} \in \mathbb{Q}$. Montrons que $a_{ij} \in \mathbb{Z}$. Notons $\alpha_j = \sum_i a_{ij} \zeta_1^i$. Alors $b = \sum_j \alpha_j \zeta_2^j$. Notons $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_1)) = \{\sigma_1^{(2)}, \ldots, \sigma_{n_2}^{(2)}\}$ et $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_2)) = \{\sigma_1^{(1)}, \ldots, \sigma_{n_1}^{(1)}\}$. Les équations $\sigma_i^{(2)}(b) = \sum_j \alpha_j \sigma_i^{(2)}(\zeta_2^j)$ constituent un système linéaire dont les α_j sont solutions. La matrice de ce système est $T = (\sigma_i^{(2)}(\zeta_2^j))$. Or $(detT)^2 = d_2$. Comme de plus les coordonnées de T sont des entiers algébriques ainsi que les $\sigma_i^{(2)}(b)$, en inversant le système à l'aide de la comatrice de T, les $d_2 \alpha_j$ sont aussi des entiers algébriques. Ils sont de plus dans $\mathbb{Q}(\zeta_1)$. Donc, par hypothèse, les $d_2 a_{ij}$ sont entiers. Il en est de même des $d_1 a_{ij}$. Donc, par le théorème de Bezout, d_1 et d_2 étant premiers entre eux, les a_{ij} sont entiers. Donc l'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\bigoplus_{i,j} \zeta_1^i \zeta_2^j \mathbb{Z} = \mathbb{Z}[\zeta]$.
Calculons $d = [det(\sigma_k^{(1)}(\zeta_1^i)\sigma_l^{(2)}(\zeta_2^j))]^2$. La matrice $(\sigma_k^{(1)}(\zeta_1^i)\sigma_l^{(2)}(\zeta_2^j))$ s'écrit comme le produit d'une matrice diagonale par blocs ayant n' blocs égaux à $(\sigma_k^{(1)}(\zeta_1^i))$ par une matrice qui, quitte à réordonner les colonnes, est aussi diagonale par blocs ayant n blocs égaux à $(\sigma_l^{(2)}(\zeta_2^j))$. On en déduit que $d = d_1^{n_2} d_2^{n_1}$. □

Nous sommes actuellement en mesure de prouver le théorème suivant:

Théorème 2.2.9. ***Anneau des entiers pour une extension cyclotomique finie***
L'anneau des entiers de $\mathbb{Q}(\zeta)$ *est* $\mathbb{Z}[\zeta]$.

Preuve. Notons B l'anneau des entiers de $\mathbb{Q}(\zeta)$. Supposons dans un premier temps que $m = p^v$ où p est premier. Soit ϕ_m le m-ième polynôme cyclotomique. On a alors $\phi_m = \prod_{1 \leq i \leq m, i \wedge m = 1} (X - \zeta^i) = \sum_{i=0}^{p-1} X^{ip^{v-1}}$. On en déduit que $p = \prod_{1 \leq i \leq m, i \wedge m = 1} (1 - \zeta^i)$. Or, si $1 \leq i \leq m$ et $i \wedge m = 1$, en choisissant i' tel que $m | ii' - 1$, on a $\dfrac{\zeta^i - 1}{\zeta - 1} = 1 + \zeta + \cdots + \zeta^{i-1} \in O$ et $\dfrac{\zeta - 1}{\zeta^i - 1} = \dfrac{\zeta^{ii'} - 1}{\zeta^i - 1} = 1 + \zeta^i + \cdots + \zeta^{i(i'-1)} \in O$. Par conséquent, $\dfrac{\zeta^i - 1}{\zeta - 1}$ est une unité dans B, et donc p et $(\zeta - 1)^{\varphi(m)}$ sont associés, où φ est la fonction indicatrice d'Euler. Donc les idéaux pB et $(\zeta - 1)^{\varphi(m)}$ sont égaux. Appliquons la relation de la proposition 2.2.7

à $\pi = p\mathbb{Z}$. On a alors $\Pi = pB = (\zeta - 1)^{\varphi(m)}$. Si on note e_i et f_i les indices de ramification et les degrés résiduels respectivement, pour i allant de 1 à r, alors chaque e_i est multiple de $\varphi(m)$. Or $n = \varphi(m) = e_1 f_1 + \cdots + e_r f_r$. Par des inégalités évidentes, on a donc $r = 1$, $e_1 = \varphi(m)$ et $f_1 = 1$.
On en déduit que $(\zeta - 1)$ est premier et que $B/(\zeta - 1) \cong \mathbb{Z}/p\mathbb{Z}$. Par conséquent $B = \mathbb{Z} + (\zeta - 1)B$, d'où $B = \mathbb{Z}[\zeta] + (\zeta - 1)B$. En multipliant par $\zeta - 1$, $(\zeta - 1)B = (\zeta - 1)\mathbb{Z}[\zeta] + (\zeta - 1)^2 B$, puis en réinjectant, $B = \mathbb{Z}[\zeta] + (\zeta - 1)^2 B$. En itérant ce processus, par une récurrence simple, on obtient $B = \mathbb{Z}[\zeta] + (\zeta - 1)^k B$ pour tout entier naturel k. Reste à choisir k. On voudrait $(\zeta - 1)^k B \subseteq \mathbb{Z}[\zeta]$. En tenant compte de $pB = (\zeta - 1)^{\varphi(m)}$, il suffit de trouver l tel que $p^l B \subseteq \mathbb{Z}[\zeta]$ puis de choisir $k = l\varphi(m)$. C'est ici que la proposition 2.2.5 entre en jeu: si $d = d(1, \zeta, ..., \zeta^{\varphi(m)-1})$, on a $dB \subseteq \mathbb{Z}[\zeta]$. Il suffit donc de montrer que, au signe près, d est une puissance de p. Calculons d.
Notons $\zeta_1, ..., \zeta_{\varphi(m)}$ les conjugués de ζ. Alors, en remarquant que $(\sigma_i(\zeta^j))$ est la matrice de Van der Monde associée à $\zeta_1, ..., \zeta_{\varphi(m)}$, où les σ_i sont les $\mathbb{Q}$-morphismes de $\mathbb{Q}(\zeta)$ dans $\mathbb{C}$, on a $d = \pm \prod_{i \neq j}(\zeta_i - \zeta_j) = \pm \prod_i \phi'_m(\zeta_i)$. Donc, avec la proposition 2.2.2, $d = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi'_m(\zeta))$. En dérivant la relation $(X^{p^{v-1}} - 1)\phi_m = (X^{p^v} - 1)$ puis en évaluant en ζ, on obtient: $\zeta(\epsilon - 1)\phi'_m(\zeta) = p^v$, où $\epsilon = \zeta^{p^{v-1}}$ est une racine primitive p-ième de l'unité. Or $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta) = \pm 1$, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\epsilon - 1) = \pm \phi_p(1)^{p^{v-1}} = \pm p^{p^{v-1}}$ et $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(p^v) = p^{v\varphi(m)}$. Donc d est bien une puissance de p (au signe près) et nous avons montré le théorème lorsque m est la puissance d'un nombre premier.
Le cas général découle alors immédiatement du lemme 2.2.8. □

Nous avons ainsi déterminé l'anneau des entiers dans $\mathbb{Q}(\zeta)$. Nous aurons cependant aussi besoin dans la suite de connaître l'anneau des entiers dans un corps quadratique. C'est l'objet de la section suivante.

2.2.4 Anneau des entiers d'un corps quadratique

Soit d un entier relatif sans facteur carré. Nous nous intéressons ici au cas où $A = \mathbb{Z}$, $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$. La proposition suivante permet de caractériser les entiers algébriques à l'aide de leur norme et de leur trace:

Proposition 2.2.10. ***Entiers algébriques dans un corps quadratique***
Soit $a \in \mathbb{Q}(\sqrt{d})$. Alors a est un entier algébrique si, et seulement si, $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$.

Preuve. Notons $a = x + y\sqrt{d}$, avec $x, y \in \mathbb{Q}$. Un calcul élémentaire donne $N_{L/K}(a) = x^2 - dy^2$ et $Tr_{L/K}(a) = 2x$. Nous avons déjà montré que, si a est un entier algébrique, alors $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$. Réciproquement, si $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$, alors a est racine de $(X - x - y\sqrt{d})(X - x + y\sqrt{d}) = X^2 - Tr_{L/K}(a)X + N_{L/K}(a) \in \mathbb{Z}[X]$. □

Il est alors facile de déterminer l'anneau des entiers:

Théorème 2.2.11. ***Anneau des entiers pour une extension quadratique***
Soit B l'anneau des entiers dans $\mathbb{Q}(\sqrt{d})$.

(i) Si $d \equiv 2, 3\ [4]$, alors $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

(ii) Si $d \equiv 1\ [4]$, alors $B = \mathbb{Z} + \mathbb{Z}\dfrac{-1+\sqrt{d}}{2}$.

La preuve reposant sur des arguments arithmétiques élémentaires d'une extrême simplicité à partir de la proposition précédente, elle est laissée au lecteur.

2.3 Norme d'un idéal

Dans cette section, nous allons définir la norme d'un idéal, notion dont nous aurons besoin dans la suite. Considérons une extension finie séparable $L|K$. Soit A un sous-anneau de K dont le corps des fractions est K. Soit finalement B la fermeture intégrale de A dans L. Supposons que A est de Dedekind. Alors, d'après la proposition 2.2.6, B est aussi de Dedekind.

Définition 2.3.1. ***Norme relative d'un idéal***
*Soit I un idéal de B. Écrivons $I = \Pi_1^{e_1}...\Pi_r^{e_r}$, où les Π_i sont des idéaux premiers. Notons $\pi_i = \Pi_i \cap A$ et $f_1 = [B/\Pi_1 : A/\pi_1]$, ..., $f_r = [B/\Pi_r : A/\pi_r]$. On définit alors la **norme** de I, notée $N_{L|K}(I)$, par $N_{L|K}(I) = \prod_{i=1}^{r} \pi_i^{e_i f_i}$. Par convention, si $I = B$, alors $N_{L|K}(I) = A$, et si $I = 0$, alors $N_{L|K}(I) = 0$.*

Nous aurons alors besoin de trois propriétés essentielles de la norme. Établissons d'abord la compatibilité de la norme avec les tours d'extensions:

Proposition 2.3.2. ***Tours de normes***
Considérons une deuxième extension finie séparable $M|L$, et soit C la fermeture intégrale de A dans M. Alors, pour I idéal de C, on a $N_{M|K}(I) = N_{L|K}\big(N_{M|L}(I)\big)$.

Preuve. Par multiplicativité, il suffit de prouver la propriété lorsque I est un idéal premier de C. Notons $\Pi = I \cap B$ et $\pi = I \cap A$. Notons aussi $f_1 = [C/I : B/\Pi]$, $f_2 = [B/\Pi : A/\pi]$ et $f = [C/I : A/\pi]$. Comme $f = f_1 f_2$, on a $N_{M|K}(I) = \pi^f = \pi^{f_1 f_2} = N_{L|K}\big(N_{M|L}(I)\big)$. □

Intéressons-nous maintenant à la norme d'un idéal principal. Pour ce faire, nous avons d'abord besoin d'étudier la norme lorsque $L|K$ est galoisienne:

Lemme 2.3.3. ***Norme dans le cas d'une extension galoisienne***
Supposons $L|K$ galoisienne. Soit Π un idéal premier de B. Soit $\pi = \Pi \cap A$. Alors

$$N_{L|K}(\Pi)B = \prod_{\sigma \in Gal(L|K)} \sigma\Pi$$

Preuve. Écrivons $\pi B = \Pi_1^{e_1}...\Pi_r^{e_r}$ et $f_i = [B/\Pi_i : A/\pi]$. Notons $G = Gal(L|K)$. Fixons i entre 1 et r. Supposons que, pour tout $\sigma \in G$, $\sigma(\Pi_1) \neq \Pi_i$. Alors le théorème des restes chinois garantit l'existence de $b \in B$ tel que

$$b \equiv 0 \pmod{\Pi_i}$$
$$b \equiv 1 \pmod{\sigma(\Pi_1)} \text{ pour tout } \sigma \in G$$

Alors $N_{L|K}(b) = \prod_{\sigma \in G} \sigma(b)$ est dans $\Pi_i \cap A = \pi$. Comme cette norme est aussi dans Π_1 et ce dernier est premier, il existe $\sigma \in G$ tel que $\sigma(b) \in \Pi_1$, ce qui contredit la définition de b. Donc tous les Π_i sont conjugués via des éléments de G.
On déduit alors immédiatement que tous les f_i sont égaux, disons égaux à f. Comme pour $\sigma \in G$ on a $\pi B = \sigma(\pi B) = \prod_{i=1}^r \sigma(\Pi_i)^{e_i}$, on déduit que tous les e_i sont égaux, disons à e. La proposition 2.2.7 impose donc que $efr = [L : K] = Card(G)$. Le lemme découle alors immédiatement. □

Remarquons que, par multiplicativité, la formule montrée dans le lemme précédent est encore vraie si Π n'est pas premier. Nous ne supposons plus $L|K$ galoisienne. Nous pouvons à présent étudier la norme d'un idéal principal:

Proposition 2.3.4. ***Norme d'un idéal principal***
Supposons que $I = (\alpha)$ est principal. Alors $N_{L|K}(I)$ l'est aussi.

Preuve. On considère M la clôture galoisienne de $L|K$. Soit C la fermeture intégrale de A dans M. Alors, avec 2.3.2 et 2.3.3, on a

$$N_{M/K}(IC) = N_{L/K}(N_{M/L}(IC)) = N_{L|K}(I)^{[M:L]}$$
$$N_{M/K}(IC) = \prod_{\sigma \in Gal(M|K)} \sigma(IC) = (N_{L|K}(\alpha))^{[M:L]}$$

La proposition découle immédiatement de ces deux relations. □

Pour terminer, étudions la norme dans le cas particulier où $K = \mathbb{Q}$:

Proposition 2.3.5. ***Norme absolue***
Soit I un idéal de B. Alors $N_{L|\mathbb{Q}}(I)$ est engendré par l'indice de I dans B.

Preuve. Décomposons $I = \Pi_1^{e_i}...\Pi_r^{e_r}$, où les Π_i sont des idéaux premiers. Notons $p_i\mathbb{Z} = \Pi_i \cap \mathbb{Z}$ et $f_i = [B/\Pi_i : \mathbb{Z}/p_i\mathbb{Z}]$. Alors $N_{L|\mathbb{Q}}(I) = \left(\prod_{i=1}^r p_i^{e_i f_i}\right)\mathbb{Z}$. D'après le théorème des restes chinois, $B/I \cong \prod_{i=1}^r B/\Pi_i^{e_i}$. Il suffit donc de montrer que, pour tout i, $[B : \Pi_i^{e_i}] = p_i^{e_i f_i}$. Cela découle immédiatement de la démonstration de la proposition 2.2.7, où l'on prouve qu'il y a une filtration $(0) \subseteq \Pi_i^{e_i-1}/\Pi_i^{e_i} \subseteq \cdots \subseteq \Pi_i/\Pi_i^{e_i} \subseteq B/\Pi_i^{e_i}$ dont les quotients successifs sont des $\mathbb{Z}/p_i\mathbb{Z}$-espaces vectoriels de dimension f_i. □

3 Le contre-exemple de Swan

Nous avons vu que le théorème de Fischer donne une réponse affirmative au problème de Noether dans certains cas. Cependant, le problème de Noether admet parfois une réponse négative. C'est ainsi que Richard Swan proposa en 1969 un contre-exemple, que nous allons développer ici.

3.1 Construction d'un premier invariant dans le groupe de Grothendieck

Considérons un corps L et H un groupe fini d'automorphismes de L. Soit k un sous-corps de L stable par H tel que L soit une extension de type fini de k. Attention, remarquons qu'on ne suppose pas que les éléments de k sont fixes par H. Si A est un sous-anneau de L, on note A^H l'ensemble des éléments fixes par H.

Définition 3.1.1. ***Module de permutation***
On dit qu'un $\mathbb{Z}[H]$-module P est un ***module de permutation*** *si P est libre sur $\mathbb{Z}$, et possède une base permutée par H.*

Remarque 3.1.2. *Un module de permutation est une somme directe de modules de la forme $\mathbb{Z}[H/H']$ où H' désigne un sous-groupe de H.*

Nous allons à présent construire un invariant pour la famille des anneaux vérifiant les cinq propriétés suivantes:
P1: Le corps des fractions de A est L.
P2: A est une k-algèbre de type fini.
P3: A est stable par H.
P4: A est factoriel.
P5: A^*/k^* est un groupe abélien de type fini. Ici, A^* (resp. k^*) désigne le groupe des unités de A (resp. k).
Dans la suite, nous noterons $\mathcal{F}$ la famille des anneaux vérifiant les propriétés $P1$ à $P5$.

Lemme 3.1.3. ***Passage entre anneaux***
Soient A, A' deux anneaux dans $\mathcal{F}$. Alors il existe $a \in A^H$, $a' \in A'^H$ avec $A[a^{-1}] = A'[a'^{-1}]$.

Preuve. A' étant une k-algèbre de type fini ($P2$), considérons $a'_1, \ldots, a'_s$ une famille de générateurs. D'après la propriété $P1$ appliquée à A, on peut écrire $a'_i = x_i/c_i$ avec x_i, c_i dans A. Considérons le produit $c = \prod_{i=1}^{s} c_i$, et soit $b = \prod_{\sigma \in H} \sigma(c)$. On vérifie sans peine que $b \in A^H$, $a'_i \in A[b^{-1}]$ et par conséquent $A' \subset A[b^{-1}]$.
Il suffit maintenant de montrer le lemme pour $A[b^{-1}]$ et A'. En effet, si on suppose

le lemme montré pour A' et $A[b^{-1}]$ avec $b \in A^H$, en choisissant $a \in A[b^{-1}]^H$, $a' \in A'^H$ tels que $A[b^{-1}][a^{-1}] = A'[a'^{-1}]$ et en écrivant a sous la forme d/b^n avec $d \in A^H$, on a $A[b^{-1}][a^{-1}] = A[(bd)^{-1}]$.
On peut donc supposer que $A' \subset A$. En inversant les rôles de A et A' dans le raisonnement précédent, on trouve un élément $a \in A'^H$ tel que $A \subset A'[a^{-1}]$. Notons que $a \in A^H$. En remarquant de plus que $A'[a^{-1}] \subset A[a^{-1}]$ (car $A' \subset A$) et que $A[a^{-1}] \subset A'[a^{-1}]$ (car $A \subset A'[a^{-1}]$), on déduit que $A[a^{-1}] = A'[a^{-1}]$. □

Le lemme précédent nous permet de passer de $A[a^{-1}]$ à $A'[a'^{-1}]$ pour a et a' bien choisis. Le lemme suivant nous permettra de passer de A à $A[a^{-1}]$ et de A' à $A'[a'^{-1}]$:

Lemme 3.1.4. ***Une suite exacte***
Soit A un anneau dans $\mathcal{F}$. Soit $a \in A^H$ non nul. Alors il existe une suite exacte

$$0 \longrightarrow A^* \longrightarrow A[a^{-1}]^* \longrightarrow P \longrightarrow 0$$

où P est un module de permutation de type fini sur $\mathbb{Z}[H]$.
De plus, $A[a^{-1}]$ est dans $\mathcal{F}$.
Corollaire immédiat: la suite

$$0 \longrightarrow A^*/k^* \longrightarrow A[a^{-1}]^*/k^* \longrightarrow P \longrightarrow 0$$

est exacte.

Preuve. Établissons d'abord la suite exacte. Pour cela, nous allons construire une application de $A[a^{-1}]^*$ dans P après avoir bien choisi P.
Notons $(p_i)_{1 \leq i \leq r}$ les diviseurs irréductibles de a dans A (non associés) et écrivons $a = up_1^{v_1} \dots p_r^{v_r}$ avec u une unité de A, v_i entiers strictement positifs. Comme $a \in A^H$, $\forall \sigma \in H$, $a = \sigma(a) = \sigma(u)\sigma(p_1)^{v_1} \dots \sigma(p_r)^{v_r}$. L'anneau A étant factoriel, par unicité de la factorisation de a, nous déduisons que les idéaux premiers (p_i) sont permutés par H.
Faisons correspondre à chaque idéal (p_i) un élément e_i et considérons le module de permutation P de base $e_1, \dots, e_r$, de telle sorte que H agit sur cette base de la même façon que sur les idéaux premiers $(p_i)_{1 \leq i \leq r}$. Définissons ensuite l'application de $A[a^{-1}]^*$ dans P, en envoyant p_i sur e_i, i.e. en envoyant $x \in A[a^{-1}]^*$ sur $\sum val_{p_i}(x)e_i$. C'est un morphisme de $\mathbb{Z}[H]$-modules. Un élément $a^{-n}p_1^{m_1} \dots p_r^{m_r}$ dans $A[a^{-1}]^*$ avec n, m_i entiers positifs a pour image $\sum(m_i - n.v_i)e_i$ dans P. Comme tous les v_i sont strictement positifs, cette application est surjective.
Cherchons son noyau. Un élément $y = a^{-n}x$ de $A[a^{-1}]^*$ avec n entier positif est dans le noyau si et seulement si $val_{p_i}(a^{-n}x) = 0$, $\forall i \in I$. Dans ce cas, $val_{p_i}(a^n) = val_{p_i}(x)$ pour tout $i \in I$, et il vient du caractère factoriel de l'anneau A que $a^n \mid x$, donc $y \in A$. Le même raisonnement marche pour y^{-1}, donc $y^{-1} \in A$

et y est inversible dans A.
On vient de démontrer que l'application surjective qu'on a construite a pour noyau A^*. D'où l'exactitude de la suite

$$0 \longrightarrow A^* \longrightarrow A[a^{-1}]^* \longrightarrow P \longrightarrow 0$$

On en déduit immédiatement l'exactitude de la suite

$$0 \longrightarrow A^*/k^* \longrightarrow A[a^{-1}]^*/k^* \longrightarrow P \longrightarrow 0$$

Montrons à présent que $A[a^{-1}]$ vérifie les propriétés $P1$ à $P5$.
$P1$, $P2$ et $P3$ sont trivialement satisfaites par $A[a^{-1}]$.
$P4$: Notons $(p_i)_{i\in I}$ les diviseurs irréductibles de a dans A, $(p_j)_{j\in J}$ les autres éléments irréductibles de A. Les $(p_j)_{j\in J}$ sont exactement les éléments irréductibles de $A[a^{-1}]$ (à unité près). Prenons un élément d/a^n dans $A[a^{-1}]$, avec $d \in A$. On obtient l'existence de la factorisation en factorisant d dans A, et l'unicité découlde de celle de A.
Donc $A[a^{-1}]$ est dans $\mathcal{F}$. □

Nous sommes à présent en mesure de définir le premier invariant. Cependant, nous avons préalablement besoin de définir le groupe de Grothendieck:

Définition 3.1.5. ***Groupe de Grothendieck***
On définit le ***groupe de Grothendieck*** *de la catégorie des $\mathbb{Z}[H]$-modules de type fini de la façon suivante:*
Soit S le groupe abélien libre dont une base est donnée par les symboles $[A]$, où A décrit les classes d'isomorphisme de $\mathbb{Z}[H]$-modules de type fini. Soit R le sous-groupe engendré par tous les élément de la forme $[A]+[C]-[B]$ dès que A, B, C s'inscrivent dans une suite exacte

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

Le groupe de Grothendieck est alors défini comme le quotient S/R.

Notons $K_0(H)$ le groupe de Grothendieck de la catégorie des $\mathbb{Z}[H]$-modules de type fini. La suite exacte dans le lemme précédent nous incite à nous intéresser à ce groupe. Afin de prendre en compte le fait que P est un module de permutation, nous considérons le quotient de $K_0(H)$ par le sous-groupe engendré par tous les modules de permutation P. Notons $Sw(H)$ le groupe ainsi construit. Alors de tout ce qui a été vu jusqu'ici découle un invariant:

Théorème 3.1.6. ***Invariant dans le groupe*** $Sw(H)$
L'image de A^*/k^* dans $Sw(H)$ ne dépend pas du choix de l'anneau A vérifiant les propriétés $P1$ à $P5$.

Preuve. Soient A et A' deux anneaux dans $\mathcal{F}$. Choisissons a et a' comme dans le lemme 3.1.3. La suite exacte du lemme 3.1.4 donne alors immédiatement les relations $[A^*/k^*] = [A[a^{-1}]^*/k^*]$ et $[A'^*/k^*] = [A'[a'^{-1}]^*/k^*]$ dans $Sw(H)$. Comme de plus $A[a^{-1}]^* = A'[a'^{-1}]^*$, on a $[A^*/k^*] = [A'^*/k^*]$ dans $Sw(H)$. $\square$

3.2 Construction d'un deuxième invariant dans le groupe des classes

On suppose à présent que H est un groupe cyclique d'ordre n. Soit σ un générateur. Soit ϕ_n le n-ième polynôme cyclotomique. Considérons l'anneau $O = \mathbb{Z}[H]/(\phi_n(\sigma))$. Isomorphe à $\mathbb{Z}[\zeta]$ où ζ est une racine primitive n-ième de l'unité, d'après la proposition 2.2.6, c'est un anneau de Dedekind. Soit M un O-module de type fini. Alors, d'après l'étude des modules de type fini sur un anneau de Dedekind développée dans la section 2.1.3, on peut écrire $M \cong N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$, où N est libre, I est un idéal de O et les Π_i sont des idéaux premiers non nuls de O. Notons $J = \Pi_1^{\alpha_1}...\Pi_q^{\alpha_q}$. On définit alors la **classe de M**, notée $c(M)$, par la classe de IJ^{-1} dans le groupe des classes défini en 2.1.2 si $I \neq 0$, celle de J^{-1} sinon. Il est immédiat que la classe est compatible avec la somme directe, au sens où $c(M \oplus M') = c(M)c(M')$: en effet, si $M \cong N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$ et $M' \cong N' \oplus I' \oplus \bigoplus_{i=1}^{q'} O/\Pi_i'^{\alpha_i'}$ avec N et N' libres, alors $M \oplus M' \cong N \oplus N' \oplus O \oplus II' \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i} \oplus \bigoplus_{i=1}^{q'} O/\Pi_i'^{\alpha_i'}$ en tenant compte du fait que $I \oplus I' \cong O \oplus II'$. Cependant, la compatibilité de la classe avec les suites exactes est beaucoup moins triviale et s'exprime ainsi:

Proposition 3.2.1. ***Compatibilité de la classe avec les suites exactes*** *Soit $0 \to A \to B \to C \to 0$ une suite exacte de O-modules. Alors $c(B) = c(A)c(C)$.*

Preuve. Écrivons $C = N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$, où N est libre, et notons $J = \prod_{i=1}^{q} \Pi_i^{\alpha_i}$ et $D = N \oplus O \oplus I$ puis considérons le diagramme suivant:

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & J \arrow[r, equal] \arrow[d] & J \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & B \times_C D \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

où $B \times_C D$ est le produit fibré de B et D au-dessus de C. Il est facile de voir que le diagramme est exact en lignes et en colonnes. Par définition de la classe, on a toujours $c(D) = c(J)c(C)$. Comme la classe est compatible avec la somme directe, comme D est sans torsion (et donc projectif), $c(B \times_C D) = c(A)c(D)$. Si de plus B est sans torsion, on a $c(B \times_C D) = c(J)c(B)$, et les trois relations trouvées entre les classes imposent que $c(B) = c(A)c(C)$. Donc la proposition 3.2.1 est vraie dès que B est sans torsion. Maintenant, si l'on ne suppose rien pour B mais on suppose que A est sans torsion, alors $B \times_C D \cong A \oplus D$ est sans torsion, et donc $c(B \times_C D) = c(J)c(B)$. On conclut que la proposition 3.2.1 est vraie dès que A est sans torsion. Finalement, si l'on ne suppose rien, on déduit de ce qui précède que $c(B \times_C D) = c(J)c(B)$ puisque J est sans torsion. La proposition est donc prouvée en toute généralité. □

Pour un $\mathbb{Z}[H]$-module M, nous considérons le O-module $M^{\phi_n(\sigma)} = \{m \in M, \phi_n(\sigma)m = 0\}$. Nous pouvons alors énoncer le lemme suivant qui établit une compatibilité partielle avec les suites exactes de $\mathbb{Z}[H]$-modules:

Lemme 3.2.2. ***Compatibilité de la classe avec les suites exactes de*** $\mathbb{Z}[H]$***-modules***
Soit P un $\mathbb{Z}[H]$-module de permutation.

(i) $P^{\phi_n(\sigma)}$ est un O-module libre.

(ii) Si $0 \to M \to N \to P \to 0$ est une suite exacte de $\mathbb{Z}[H]$-modules, alors $0 \to M^{\phi_n(\sigma)} \to N^{\phi_n(\sigma)} \to P^{\phi_n(\sigma)} \to 0$ est une suite exacte de O-modules.

Preuve.

(i) P étant un module de permutation, on peut écrire $P \cong \mathbb{Z}[H]^r \oplus \bigoplus_i \mathbb{Z}[H/H_i]$, où les H_i sont des sous-groupes de H non triviaux. Pour chaque i, si $d = [H : H_i]$, alors $(\sigma^d - 1)\mathbb{Z}[H/H_i] = 0$. Or on a aussi $\phi_n(\sigma)\mathbb{Z}[H/H_i]^{\phi_n(\sigma)} = 0$. Donc, comme $(X^d - 1) \wedge \phi_n = 1$, grâce à l'identité de Bezout, $\mathbb{Z}[H/H_i]^{\phi_n(\sigma)} = 0$. D'autre part, soit $\psi_n \in \mathbb{Z}[X]$ tel que $X^n - 1 = \phi_n\psi_n$ et considérons $f : \mathbb{Z}[H] \to \mathbb{Z}[H]^{\phi_n(\sigma)}, x \mapsto \psi_n(\sigma)x$. L'application f est un morphisme de $\mathbb{Z}[H]$-modules, dont le noyau est $\phi_n(\sigma)\mathbb{Z}[H]$ et dont l'image est $\mathbb{Z}[H]^{\phi_n(\sigma)}$ tout entier. En effet, il existe des polynômes à coefficients entiers A et B et un entier non nul m tels que $A\phi_n + B\psi_n = m$, et $\mathbb{Z}[X]/(\phi_n)$ et $\mathbb{Z}[X]/(\psi_n)$ sont des groupes sans torsion, donc l'annulateur de $\phi_n(\sigma)$ est $(\psi_n(\sigma))$ et l'annulateur de $\psi_n(\sigma)$ est $(\phi_n(\sigma))$. Donc $\mathbb{Z}[H]^{\phi_n(\sigma)} \cong \mathbb{Z}[H]/\phi_n(\sigma)\mathbb{Z}[H]$. Par conséquent, $P^{\phi_n(\sigma)} \cong O^r$.

(ii) Notons $P_1 = \mathbb{Z}[H]^r$ et $P_2 = \bigoplus_i \mathbb{Z}[H/H_i]$. Soit N_2 l'image réciproque de P_2 dans N. On a alors les suites exactes de $\mathbb{Z}[H]$-modules:

$$0 \to N_2 \to N \to P_1 \to 0$$
$$0 \to M \to N_2 \to P_2 \to 0$$

P_1 étant libre, la première suite exacte donne $N \cong N_2 \oplus P_1$, donc $N^{\phi_n(\sigma)} = N_2^{\phi_n(\sigma)} \oplus P_1^{\phi_n(\sigma)}$. La deuxième suite exacte permet d'établir $0 \to M^{\phi_n(\sigma)} \to N_2^{\phi_n(\sigma)} \to P_2^{\phi_n(\sigma)} = 0$ d'après (i), donc $M^{\phi_n(\sigma)} \cong N_2^{\phi_n(\sigma)}$. On en déduit alors que $0 \to M^{\phi_n(\sigma)} \to N^{\phi_n(\sigma)} \to P^{\phi_n(\sigma)} \to 0$ est une suite exacte de O-modules.

□

Le lemme précédent montre alors que $N^{\phi_n(\sigma)} \cong M^{\phi_n(\sigma)} \oplus P^{\phi_n(\sigma)}$ et que $c(M^{\phi_n(\sigma)}) = c(N^{\phi_n(\sigma)})$. Nous sommes à présent en mesure de définir l'invariant de Swan, qui va jouer un rôle majeur dans la suite:

Théorème 3.2.3. ***Invariant dans le groupe des classes***
La classe $c((A^*/k^*)^{\phi_n(\sigma)})$ est indépendante du choix de l'anneau A vérifiant les conditions (P1) à (P5).

Preuve. Soient A et A' deux anneaux vérifiant les conditions (P1) à (P5). D'après le lemme 3.1.3, il existe a et a' dans A^H et A'^H tels que $A[a^{-1}] = A'[a'^{-1}]$. Notons $B = A[a^{-1}] = A'[a'^{-1}]$. Alors, d'après le lemme 3.1.4, on a les suites exactes de $\mathbb{Z}[H]$-modules suivantes:

$$0 \to A^*/k^* \to B^*/k^* \to P \to 0$$
$$0 \to A'^*/k^* \to B^*/k^* \to P' \to 0$$

où P et P' sont des modules de permutation. Donc le lemme 3.2.2 impose que $c((A^*/k^*)^{\phi_n(\sigma)}) = c((B^*/k^*)^{\phi_n(\sigma)}) = c((A'^*/k^*)^{\phi_n(\sigma)})$, d'où le théorème. □

Nous noterons à partir d'ici $\alpha(k, L, H) = c((A^*/k^*)^{\phi_n(\sigma)})$. Dans la suite, il s'agira de déterminer que cet invariant est toujours le même dès que le problème de Noether admet une réponse affirmative, puis de montrer qu'en choisissant judicieusement les paramètres du problème on obtient un invariant différent.

3.3 Le contre-exemple de Swan

Commençons par calculer l'invariant précédent dans le cas d'une extension transcendante pure.
Fixons p un entier premier de $\mathbb{Z}$: ultérieurement, on prendra $p = 47$. Soit k_0 un corps, qui sera pris égal à $\mathbb{Q}$ plus tard. Notons k le corps obtenu à partir de k_0 par adjonction des racines p-ièmes de l'unité. On suppose que $[k : k_0] = p - 1$, ce qui est évidemment vérifié lorsque $k_0 = \mathbb{Q}$. Soit $K_0 = k_0(x_1, \ldots, x_p)$ le corps des fractions rationnelles sur k_0.
Soit G le groupe cyclique d'ordre p qui opère sur K_0 en permutant circulairement

$x_1, \ldots, x_p$. On note $L_0 = K_0^G$ le corps fixe sous l'action de G. Notons K et L les corps obtenus à partir de K_0 et L_0 respectivement par adjonction des racines p-ièmes de l'unité. Il est alors clair que $[K : K_0] = [L : L_0] = p - 1$. On choisit ensuite pour H le groupe de Galois de K/K_0, qui est canoniquement isomorphe aux groupes de Galois de L/L_0 et de k/k_0 par restriction. H est alors le groupe cyclique à $n = p - 1$ éléments.

Théorème 3.3.1. ***Cas d'une extension transcendante pure***
Si L_0/k_0 est une extension transcendante pure, alors on a $\alpha(k, L, H) = 1$.

Preuve. Si $L_0 = k_0(y_1, \ldots, y_p)$, avec les y_i algébriquement indépendants sur k_0, alors en prenant $A = k[y_1, \ldots, y_p]$, A vérifie les conditions $P1$ à $P5$. Or A^*/k^* n'est autre que l'élément neutre, on a donc par définition $\alpha(k, L, H) = 1$. □

Par conséquent, pour montrer qu'une extension n'est pas transcendante pure, il suffit de calculer $\alpha(k, L, H)$ et de voir que l'on n'obtient pas 1, ce qui revient à voir qu'un certain idéal n'est pas principal. Pour cela, nous aurons besoin du lemme suivant:

Lemme 3.3.2. ***47 est un nombre magique***
Si ζ est une racine primitive 46-ième de l'unité, et $\mathfrak{p}$ un idéal premier de $\mathbb{Z}[\zeta]$ tel que $Card(\mathbb{Z}[\zeta]/\mathfrak{p}) = 47$, alors $\mathfrak{p}$ n'est pas principal.

Preuve. La preuve est basée sur l'étude de la norme relative de l'idéal $\mathfrak{p}$ (section 2.1.3).
Raisonnons par l'absurde.
Tout d'abord, d'après le théorème 2.2.9, on sait que $\mathbb{Z}[\zeta]$ est la clôture intégrale de $\mathbb{Z}$ dans le corps k. Ce corps contient le corps $\mathbb{Q}(\sqrt{-23})$. En effet, si ξ est une racine primitive 23-ème de l'unité, on remarque que

$$\phi_{23}(1) = 23 = \prod_{i=1}^{22}(1 - \xi^i) = \prod_{i=1}^{11}(1 - \xi^i)(1 - \xi^{23-i}) = -\xi^{-66}\left(\prod_{i=1}^{11}(\xi^i - 1)\right)^2$$

et on a donc bien que $\sqrt{-23} \in k$.
Comme $\mathbb{Q}(\sqrt{-23})$ est un corps quadratique avec $-23 \equiv 1$ [4], le théorème 2.2.11 impose que l'anneau des entiers de $\mathbb{Q}(\sqrt{-23})$ est engendré par 1 et $\frac{1+\sqrt{-23}}{2}$.
Si $\mathfrak{p}$ était principal, sa norme relativement à $\mathbb{Q}(\sqrt{-23})$ serait encore un idéal principal (α) d'après la proposition 2.3.4. Si $\alpha = \frac{x+y\sqrt{-23}}{2}$ $(x \equiv y\ [2])$, on a $N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}(\alpha) = \frac{x^2+23y^2}{4}$. De plus, avec la proposition 2.3.5, on a $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{p}) = 47$. La proposition 2.3.2 impose alors $47 = \frac{x^2+23y^2}{4}$. En examinant les cas où $|y| = 0, 1, 2$, on remarque que l'équation précédente n'a pas de solutions, d'où la contradiction. □

La définition suivante sera utile dans la suite:

Définition 3.3.3. ***Résolvantes de Lagrange***
Soit ω une racine p-ième de l'unité. On appelle ***résolvantes de Lagrange*** *les y_i définis par: $\forall i \in \{0, 1, \ldots, p-1\}$, $y_i = \sum_{j=1}^{p} \omega^{-ij} x_j$.*

Nous sommes à présent en mesure d'établir le contre-exemple de Swan:

Théorème 3.3.4. ***Contre-exemple de Swan***
On prend $p = 47$, $k_0 = \mathbb{Q}$, G le groupe $\mathbb{Z}/47\mathbb{Z}$ agissant sur les x_i par permutation cyclique, $K_0 = \mathbb{Q}(x_1, \ldots, x_{47})$. Alors L_0, le corps des fractions rationnelles invariantes par G, n'est pas une extension transcendante pure de $\mathbb{Q}$.

Preuve. Rappelons que nous avons choisi pour H le groupe de Galois de K/K_0 isomorphe aux groupes de Galois de L/L_0, k/k_0: il est cyclique d'ordre $n = p-1$. Notons y_i les résolvantes de Lagrange définies précédemment, pour i allant de 0 à $p-1$. On remarque que les actions de G et H sur K commutent. Le groupe H fixe y_0 et le sous-$\mathbb{Z}$-module M' de K^* de base $y_1, \ldots, y_{p-1}$ est libre sur $\mathbb{Z}[H]$. En effet, H permute (transitivement) les y_i et donc ce module est monogène (engendré par y_1) sur $\mathbb{Z}[H]$. On utilise bien sûr ici que la matrice de Van der Monde qui traduit le changement de variables donné par les résolvantes de Lagrange est inversible.
On considère ensuite le sous-module M de M' défini par $M = M' \cap L^*$. On va montrer que M est un sous-module d'indice p de M'. Par un calcul simple on voit que y_1^p et $y_1^{-i} y_i$ sont des éléments de M. Ils engendrent un sous-module d'indice p de M'. Si c'est M, il n'y a rien à montrer. Sinon, $M = M'$ donc $M' \subset L^*$ ce qui est absurde puisque y_1 n'est pas dans L. Donc M est un sous-module d'indice p de M'. On voit aussi que M est de rang $p-1$ en tant que $\mathbb{Z}$-module. Soit $m_1, \ldots, m_{p-1}$ une base de M.
Maintenant considérons A l'anneau $k[y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1}]$, alors A vérifie les propriété $P1$ à $P5$. En effet, la seule difficulté est de montrer que le corps des fractions de A est L. Pour cela, on utilise que le degré de l'extension K/L est p (car l'extension est galoisienne), et on va le comparer au degré de K sur le corps des fractions de A (noté $Frac_A$). Mais $K = k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})(y_1)$, donc le degré d'extension de ce dernier sur $k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})$ est au plus p. Mais alors on a

$$\begin{tikzcd} Frac_A \arrow[r, hook] \arrow[rr, hook, bend left, "\leq p"] & L \arrow[r, hook, "p"'] & K \end{tikzcd}$$

ce qui montre que $L = k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})$, le corps des fractions de A. On remarque aussi que A^*/k^* est égal à M.

Par définition du second invariant, $\alpha(k, L, H) = c(M^{\phi_n(\sigma)})$. En regardant la suite exacte

$$0 \longrightarrow M^{\phi_n(\sigma)} \longrightarrow M'^{\phi_n(\sigma)} \longrightarrow M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)} \longrightarrow 0$$

on a $\alpha(k, L, H) = c(M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)})^{-1}$ par compatibilité de la classe avec les suites exactes (proposition 3.2.1 et proposition 3.2.2). Le module M étant un sous-module d'indice p de M', $M^{\phi_n(\sigma)}$ est un sous-O-module d'indice 1 ou p de $M'^{\phi_n(\sigma)}$. Montrons que $M^{\phi_n(\sigma)} \neq M'^{\phi_n(\sigma)}$. Pour ce faire, on va construire un élément annulé par $\phi_n(\sigma)$ dans M' mais qui n'est pas dans M. Regardons par exemple l'élément

$$T = \prod_{d|n, d\neq n} (\sigma^d - 1) \in \mathbb{Z}[H]$$

Alors $T.y_1$ est annulé par $\phi_n(\sigma)$. Montrons que son image dans M'/M est non nulle. On sait que M'/M est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, engendré par y_1, et l'action de σ sur M'/M est une multiplication par r où r est l'élément dans $\mathbb{Z}/p\mathbb{Z}$ tel que $\sigma(\omega) = \omega^r$. Donc T agit sur M'/M par multiplication par l'élément de $\mathbb{Z}/p\mathbb{Z}$

$$\prod_{d|n, d\neq n} (r^d - 1)$$

qui est non nul car l'ordre de r dans $(\mathbb{Z}/p\mathbb{Z})^*$ est n. Par conséquent T est injectif et donc $T.y_1$ est non nul.
Donc $M^{\phi_n(\sigma)}$ est un sous-O-module d'indice p de $M'^{\phi_n(\sigma)} \cong O$. Par conséquent, $M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)}$ est isomorphe à un quotient $\mathbb{Z}[\zeta]/\mathfrak{p}$, $\mathfrak{p}$ idéal premier, et donc $\alpha(k, L, H) = 1$ si, et seulement si, $\mathfrak{p}$ est principal. Or, avec $p = 47$, la propriété "47 est un nombre magique" (proposition 3.3.2) impose immédiatement que $\mathfrak{p}$ n'est pas principal. □

4 Résolution du problème de Noether pour un groupe abélien

4.1 Un peu de cohomologie des groupes finis

Dans la suite, nous aurons besoin de définir quelques notions de cohomologie des groupes. Soit G un groupe fini, et définissons:

Définition 4.1.1. H^1 ***et*** $\widehat{H}^{-1}$
Soit M un $\mathbb{Z}[G]$-module. Soit $N : M \to M, m \mapsto \sum_{g\in G} gm$. Soit I_G l'idéal de $\mathbb{Z}[G]$ engendré par les éléments de la forme $g - 1$, pour $g \in G$. Alors on définit les groupes:

$$H^1(G, M) = \frac{\{f : G \to M | \forall g, g' \in G, f(gg') = gf(g') + f(g)\}}{\{G \to M, g \mapsto ga - a; a \in M\}}$$

$$\widehat{H}^{-1}(G,M) = KerN/I_G M$$

Considérons $0 \to A \to B \to C \to 0$ une suite exacte de $\mathbb{Z}[G]$-modules. Il est alors immédiat que la suite $0 \to A^G \to B^G \to C^G$ est exacte, mais la dernière flèche n'est pas nécessairement surjective. Le groupe H^1 permet alors de compléter cette suite, comme l'exprime la proposition suivante:

Proposition 4.1.2. ***Suite exacte de cohomologie***
Soit $0 \to A \to B \to C \to 0$ une suite exacte de $\mathbb{Z}[G]$-modules. Alors la suite $0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B)$ est aussi une suite exacte de $\mathbb{Z}[G]$-modules.

Preuve. Soit $\pi : B \to C$ la projection. On considère $\psi : C^G \to H^1(G,A), c \mapsto (g \mapsto gb - b)$ où b est un élément de B tel que $\pi(b) = c$ et $i : H^1(G,A) \to H^1(G,B)$ l'inclusion canonique. On vérifie immédiatement que l'image de c par ψ ne dépend pas du choix de b, puis que, comme $\pi(gb - b) = g\pi(b) - \pi(b) = gc - c = 0$, on a bien $gb - b \in A$. ψ est donc bien définie. L'exactitude de la suite proposée est alors facile à établir. □

On énonce maintenant un théorème classique connu sous le nom du "théorème de Hilbert 90" qui sera utile dans la suite:

Théorème 4.1.3. ***Théorème de Hilbert 90***
Soit L/K une extension galoisienne finie de groupe de Galois $G = Gal(L/K)$. Alors $H^1(G, L^*) = 0$.

Preuve. Les opérations sont notées multiplicativement dans cette preuve. Soit $f : G \to L^*$ une application non nulle telle que $f(gg') = gf(g') \cdot f(g)$. On veut trouver un élément c dans L^* tel que $f(g) = gc \cdot c^{-1}$. On considère pour cela un élément b de la forme $b = \sum_{g \in G} f(g) \cdot g(a)$ avec $a \in L^*$ que l'on déterminera ultérieurement. Un calcul montre que $\forall g \in G$, $gb = f(g)^{-1}b$. Si $b \neq 0$, alors, en posant $c = b^{-1}$, on a $\forall g \in G$, $f(g) = gc \cdot c^{-1}$.
Reste à montrer que l'on peut choisir $a \in L^*$ tel que $b \neq 0$. Autrement dit il suffit de voir que l'application $a \mapsto \sum_{g \in G} f(g) \cdot g(a)$ soit non nulle. Ceci résulte de l'indépendance des automorphismes de corps. □

Pour terminer, nous aurons besoin du lemme de Shapiro, que nous admettrons:

Lemme 4.1.4. ***Lemme de Shapiro***
Soient H un sous-groupe de G et M un $\mathbb{Z}[H]$-module. Nous pouvons munir $Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)$ d'une structure de $\mathbb{Z}[G]$-module par:

$$(gf)(a) = f(ag) \text{ pour } g \in G \text{ et } f \in Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) \text{ et } a \in \mathbb{Z}[G].$$

Alors on a l'isomorphisme

$$H^1(G, Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)) \cong H^1(H, M)$$

4.2 Notations, objectif et stratégie

Considérons un corps k et G un groupe abélien fini qui agit sur $k(\{x_g, g \in G\})$ par permutation des variables. Notons $k_G = k(\{x_g, g \in G\})^G$. On cherche à établir une condition nécessaire et suffisante pour que k_G soit une extension transcendante pure de k.
Étant donné un groupe cyclique ρ d'ordre m et de générateur τ, on définit $\mathbb{Z}(\rho) = \mathbb{Z}[\rho]/\Phi_m(\tau)\mathbb{Z}[\rho]$. $\mathbb{Z}(\rho)$ est alors un anneau de Dedekind isomorphe à $\mathbb{Z}[\zeta_m]$, où ζ_m est une racine primitive m-ième de l'unité. Remarquons que cet anneau est indépendant du choix de τ.
Notons à présent k_c l'extension cyclotomique maximale de k dans une clôture algébrique. Donnons-nous un sous-corps K de k_c contenant k tel que $\rho_K = Gal(K/k)$ est cyclique, de générateur τ_K. Soient $\mathbb{P}$ l'ensemble des nombres premiers et $T = (\mathbb{P} - \{2, car(k)\}) \times \mathbb{N}^*$. Pour $(p, s) \in T$, on considère l'idéal $\mathfrak{a}_K(p^s)$ de $\mathbb{Z}(\rho_K)$ par:

$$\mathfrak{a}_K(p^s) = \mathbb{Z}(\rho_K) \text{ si } K \neq k(\zeta_{p^s})$$
$$\mathfrak{a}_K(p^s) = (\tau_K - t, p) \text{ si } K = k(\zeta_{p^s}) \text{ et } t \in \mathbb{Z} \text{ vérifie } \tau_K(\zeta_p) = \zeta_p^t$$

Remarquons que cette définition est indépendante du choix de τ_K.
On définit alors pour un groupe abélien fini H:

$$\mathfrak{a}_K(H) = \prod_{(p,s)\in T} \mathfrak{a}_K(p^s)^{m(H,p,s)}$$

où $m(H, p, s) = dim_{\mathbb{Z}/p\mathbb{Z}}(p^{s-1}H/p^sH)$.
Notons finalement $v(G)$ la plus grande puissance de 2 divisant l'exposant de G.
Nous sommes maintenant en mesure d'énoncer le théorème de Lenstra:

Théorème 4.2.1. ***Théorème de Lenstra***
Avec les définitions et notations précédentes, k_G est une extension transcendante pure de k si, et seulement si, les deux assertions suivantes sont vérifiées:

(i) quel que soit le sous-corps K de k_c contenant k tel que ρ_K est cyclique, $\mathfrak{a}_K(G)$ est principal.

(ii) Si $car(k) \neq 2$, alors $k(\zeta_{v(G)})$ est une extension cyclique de k.

La démonstration de ce théorème est délicate et longue. Décrivons la stratrégie suivie.
Dans un premier temps (parties 4.3 et 4.4), nous allons nous essayer d'établir des

liens entre les modules de permutation et les extemsions transcendantes pures, afin de montrer le théorème 4.4.6. Ensuite, dans un deuxième temps, afin de relier la nature de l'extension $k_G|k$ à l'idéal $\mathfrak{a}_K(G)$, nous allons construire un module F_ρ puis nous allons relier F_ρ à l'extension $k_G|k$ (partie 4.5 théorème 4.5.6) et aux idéaux de la forme $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ (partie 4.6 théorème 4.6.7). Pour ce faire, nous aurons besoin d'introduire dans la partie 4.6 deux modules que nous appellerons I_q et J_q et qui joueront aussi un rôle important dans les parties suivantes. Après cela, dans la partie 4.7, le théorème 4.7.4 nous permettra d'éviter tous les problèmes de caractéristique, en particulier la situation problématique où $car(k)$ divise $|G|$. Finalement, la partie 4.8 permettra de montrer le théorème de Lenstra en établissant d'abord quelques isomorphismes de corps puis en combinant tous les résultats vus jusque là.
L'énoncé du théorème de Lenstra n'est pas particulièrement simple ni joli. Il est assez difficile à appréhender et assez technique. Cependant, il est puissant et il permet d'obtenir de très belles conséquences, en particulier dans le cas où G est cyclique. Nous donnerons quelques unes de ces conséquences dans la partie 5.

4.3 Facteurs directs de permutation

Soit π un groupe fini. En nous inspirant de la définition des modules projectifs, nous posons la définition suivante:

Définition 4.3.1. ***Facteurs directs de permutation***
On dit qu'un $\mathbb{Z}[\pi]$-module P est un ***facteurs directs de permutation*** *s'il existe un $\mathbb{Z}[\pi]$-module P' tel que $P \oplus P'$ est un module de permutation.*

Intéressons-nous d'abord à la cohomologie des facteurs directs de permutation:

Proposition 4.3.2. ***Cohomologie des facteurs directs de permutation***
Soit P un $\mathbb{Z}[\pi]$-module, facteur direct de permutation. Soit ρ un sous-groupe de π. Alors $H^1(\rho, P) = \widehat{H}^{-1}(\rho, P) = 0$.

Preuve. Comme P est un $\mathbb{Z}[\rho]$-module facteur direct de permutation, on peut supposer $\rho = \pi$. Il existe alors P' tel que $P \oplus P'$ est une somme directe de modules de la forme $\mathbb{Z}[\pi/\pi']$, pour π' sous groupe de π. On peut donc supposer que $P = \mathbb{Z}[\pi/\pi']$. En appliquant le lemme de Shapiro (4.1.4), on obtient que $H^1(\pi, P) = H^1(\pi, Hom_{\mathbb{Z}[\pi']}(\mathbb{Z}[\pi], \mathbb{Z})) = H^1(\pi', \mathbb{Z}) = 0$.
D'autre part, on vérifie facilement à la main que $KerN = I_\rho P$, où $N : P \to P, p \mapsto \sum_{g\in\rho} gp$ et I_ρ est l'idéal de $\mathbb{Z}[\rho]$ engendré par les éléments de la forme $g - 1$, pour $g \in \rho$. Donc $\widehat{H}^{-1}(\rho, P) = 0$. □

On peut alors énoncer les caractérisations suivantes des facteurs directs de permutation:

Proposition 4.3.3. ***Caractérisations des facteurs directs de permutation***
Soit P un $\mathbb{Z}[\pi]$-module. Les propositions suivantes sont équivalentes:

(i) P est un facteur direct de permutation.

(ii) Pour tout morphisme de $\mathbb{Z}[\pi]$-modules $f : P_1 \to P_2$ induisant des surjections $P_1^\rho \to P_2^\rho$ quel que soit le sous-groupe ρ de π, l'application induite $Hom_{\mathbb{Z}[\pi]}(P, P_1) \to Hom_{\mathbb{Z}[\pi]}(P, P_2)$ est surjective.

(iii) Si L est un $\mathbb{Z}[\pi]$-module tel que $H^1(\rho, L) = 0$ quel que soit ρ sous-groupe de π, alors toute suite exacte de $\mathbb{Z}[\pi]$-modules $0 \to L \to M \to P \to 0$ est scindée.

Preuve. Supposons (i). Écrivons $S = P \oplus P'$ de telle sorte que S soit un module de permutation. Soit $f : P_1 \to P_2$ un morphisme de $\mathbb{Z}[\pi]$-modules induisant des surjections $P_1^\rho \to P_2^\rho$ quel que soit le sous-groupe ρ de π. Soit $h \in Hom_{\mathbb{Z}[\pi]}(P, P_2)$. Alors on peut prolonger h par 0 sur P', obtenant ainsi $\widehat{h} : S \to P_2$. Le module S s'écrit comme somme directe de facteurs de la forme $\mathbb{Z}[\pi/\rho]$, pour ρ sous-groupe de π. Considérons $N = \mathbb{Z}[\pi/\rho]$ un de ces facteurs. L'élément $\widehat{h} \downharpoonright_N (1)$ appartient à P_2^ρ: on peut donc choisir $x_0 \in P_1^\rho$ tel que $\widehat{h} \downharpoonright_N (1) = f(x_0)$. Posons alors $k(1) = x_0$ et prolongeons k par $\mathbb{Z}[\pi]$ linéarité à N. On a alors $\widehat{h} \downharpoonright_N = f \circ k$. Il est donc possible de trouver k' dans $Hom_{\mathbb{Z}[\pi]}(S, P_1)$ tel que $\widehat{h} = f \circ k'$. Il suffit alors de restreindre k' à P pour montrer que h est bien dans l'image de $Hom_{\mathbb{Z}[\pi]}(P, P_1) \to Hom_{\mathbb{Z}[\pi]}(P, P_2)$, d'où (ii).
Supposons (ii). Soient L un $\mathbb{Z}[\pi]$-module tel que $H^1(\rho, L) = 0$ quel que soit ρ sous-groupe de π et une suite exacte de $\mathbb{Z}[\pi]$-modules $0 \to L \to M \to P \to 0$. En écrivant la suite exacte de cohomologie, on obtient alors, pour tout sous-groupe ρ de π, l'exactitude de la suite $0 \to L^\rho \to M^\rho \to P^\rho \to 0$, donc $M^\rho \to P^\rho$ est surjective. Donc, avec (ii), $Hom_{\mathbb{Z}[\pi]}(P, M) \to Hom_{\mathbb{Z}[\pi]}(P, P)$ est surjective, ce qui permet immédiatement de scinder la suite $0 \to L \to M \to P \to 0$, d'où (iii).
Supposons (iii). Soit M le $\mathbb{Z}[\pi]$-module qui, en tant que groupe, est le groupe abélien libre de base $(e_p)_{p \in P}$ indexée par P, et sur lequel la multiplication par les éléments de $\mathbb{Z}[\pi]$ est donnée par: $\forall \lambda \in \mathbb{Z}[\pi], \forall p \in P, \lambda e_p = e_{\lambda p}$. On a alors une surjection naturelle $M \to P$, qui envoie e_p sur p, et M est un $\mathbb{Z}[\pi]$-module de permutation. Soit L le noyau de la surjection $M \to P$. Alors la suite $0 \to L \to M \to P \to 0$ est exacte, et, pour tout sous-groupe ρ de π, on a la suite exacte de cohomologie: $0 \to L^\rho \to M^\rho \to P^\rho \to H^1(\rho, L) \to H^1(\rho, B) = 0$, en tenant compte de la proposition précédente. Or la flèche $M^\rho \to P^\rho$ est clairement surjective, donc $H^1(\rho, L) = 0$. En appliquant (iii), on obtient que $M = L \oplus P$, et donc P est un facteur direct de permutation. □

Cette caractérisation rappelle celle des modules projectifs.

4.4 Liens entre les modules de permutation et les extensions transcendantes pures

Soit l un corps sur lequel π agit fidèlement par automorphismes de corps. Lorsque M est un $\mathbb{Z}[\pi]$-module, libre et de rang fini sur $\mathbb{Z}$, on fait agir π sur $l[M]$, l'anneau de groupe de M, par $\sigma(\sum_{m\in M}\lambda_m m) = \sum_{m\in M}\sigma(\lambda)\sigma(m)$, pour $\sigma \in \pi$, et $(\lambda_m)_{m\in M}$ une famille presque nulle d'éléments de l. On étend cette action à $l(M)$, corps des fractions de $l[M]$, par $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1}$.

Proposition 4.4.1. ***Une base formée d'éléments fixes***
Soit V un l-espace vectoriel sur lequel π agit semi-linéairement, au sens où V est un $\mathbb{Z}[\pi]$-module tel que:

$$\forall v \in V, \forall \sigma \in \pi, \forall \lambda \in l, \sigma(\lambda v) = \sigma(\lambda)\sigma(v)$$

Alors il existe une base de V contenue dans V^π.

Preuve. Il suffit de montrer que toute forme linéaire sur V s'annulant sur V^π est nulle. Soit donc f une telle forme linéaire. Soit $v \in V$. Pour tout $\lambda \in l$, $\sum_{\sigma\in\pi}\sigma(\lambda v) \in V^\pi$, donc $0 = f(\sum_{\sigma\in\pi}\sigma(\lambda v)) = \sum_{\sigma\in\pi} f(\sigma v)\sigma(\lambda)$. Étant donné que les automorphismes de corps sont linéairement indépendants et que l'action de π est fidèle, on a $f(v) = 0$, d'où le résultat. □

Nous allons à présent montrer un certain nombre de propriétés exprimant les liens entre les extensions transcendantes pures et les facteurs directs de permutation. Le premier résultat concerne les modules de permutation.

Proposition 4.4.2. ***Extension transcendante pure associée à un module de permutation***
Soit P un $\mathbb{Z}[\pi]$-module de permutation de type fini. Alors $l(P)^\pi/l^\pi$ est une extension transcendante pure.

Preuve. Considérons $(e_1, ..., e_r)$ une $\mathbb{Z}$-base de P permutée par π. Soit V le sous-l-espace vectoriel de $l(P)$ engendré par $e_1, ..., e_r$. La proposition précédente impose alors qu'il existe $f_1, ..., f_r$ une base de V contenue dans V^π. On a alors $l(P) = l(f_1, ..., f_r)$, et $(f_1, ..., f_r)$ est une famille transcendante pure sur l. Par conséquent, $l(P)^\pi = l^\pi(f_1, ..., f_r)$, d'où le résultat. □

Le résultat suivant permet d'établir un isomorphisme de corps lorsqu'une certaine suite est exacte. Nous aurons besoin ici du théorème de Hilbert 90, démontré en 4.1.3:

Proposition 4.4.3. ***Suite exacte et isomorphisme***
Considérons $0 \to M_1 \to M_2 \to P \to 0$ une suite exacte de $\mathbb{Z}[\pi]$-modules de type fini, libres en tant que groupes abéliens. On suppose de plus que P est un facteur direct de permutation. Alors les corps $l(M_2)^\pi$ et $l(M_1 \oplus P)^\pi$ sont l^π-isomorphes.

Preuve. Notons $p : M_2 \to P$ la projection. On a une inclusion naturelle de $l(M_1)$ dans $l(M_2)$. Soit H le sous-groupe de $l(M_2)^*$ engendré par $l(M_1)^*$ et M_2. C'est un $\mathbb{Z}[\pi]$-module. Soit $f : H \to P$ définie par:

$$\forall \lambda \in l(M_1)^*, \forall m \in M_2, f(\lambda m) = p(m)$$

La suite

$$0 \longrightarrow l(M_1)^* \longrightarrow H \xrightarrow{f} P \longrightarrow 0$$

est alors exacte. Pour ρ sous-groupe de π, d'après le théorème de Hilbert 90, on a $H^1(\rho, l(M_1)^*) = H^1(Gal(l(M_1)|l(M_1)^\rho), l(M_1)^*) = 0$. D'après la caractérisation des facteurs directs de permutation (4.3.3), la suite exacte précédente est scindée. La section $P \to H$ permet alors de construire un isomorphisme entre $l(M_2)$ et $l(M_1 \oplus P)$ qui commute à l'action de π, d'où le résultat. □

On en déduit le corollaire suivant:

Corollaire 4.4.4. ***Suite exacte et extension transcendante pure***
Considérons $0 \to M_1 \to M_2 \to P \to 0$ une suite exacte de $\mathbb{Z}[\pi]$-modules de type fini, libres en tant que groupes abéliens. On suppose de plus que P est de permutation. Alors $l(M_2)^\pi$ est une extension transcendante pure de $l(M_1)^\pi$.

Preuve. D'après la proposition précédente, les corps $l(M_2)^\pi$ et $l(M_1 \oplus P)^\pi$ sont l^π-isomorphes. En appliquant la proposition 4.4.2, en prenant $l(M_1)$ comme corps de base, on obtient que $l(M_1 \oplus P)^\pi \cong l(M_1)(P)^\pi$ est une extension transcendante pure de $l(M_1)^\pi$, d'où le résultat. □

Nous sommes à présent en mesure d'énoncer le théorème central de cette partie. Pour le montrer, nous ferons appel à des résultats montrés dans la partie 3, afin d'établir le contre-exemple de Swan:

Théorème 4.4.5. ***Modules de permutation et extensions transcendantes pures***
Soit M un $\mathbb{Z}[\pi]$-module de type fini, libre en tant que groupe abélien. Les affirmations suivantes sont équivalentes:

(i) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(ii) Il existe des modules de permutation P_1 et P_2 de type fini rendant exacte la suite

$$0 \to M \to P_2 \to P_1 \to 0$$

Preuve. Supposons (i). Écrivons $L = l(M)^\pi(x_1, ..., x_r) = l^\pi(y_1, ..., y_{r+s})$, où $(x_1, .., x_r)$ et $(y_1, ..., y_{r+s})$ sont des familles algébriquement indépendantes sur $l(M)^\pi$ et l^π respectivement. Faisons agir π sur $l(M)(x_1, ..., x_r) = l(M) \otimes_{l(M)^\pi} l(M)^\pi(x_1, .., x_r)$ à travers le premier facteur, c'est-à-dire, $\sigma(a \otimes b) = \sigma(a) \otimes b$. Posons finalement $A = l[M][x_1, ..., x_r]$ et $A' = l[y_1, ..., y_{r+s}]$. Vérifions que ces anneaux vérifient les propriétés $(P1) - (P5)$.
$(P1)$: Le corps des fractions de A est clairement $l(M)(x_1, ..., x_r)$. Le corps des fractions de A' est $l(y_1, ..., y_{r+s})$, et on a le diagramme:

$$\begin{tikzcd}
l(y_1, ..., y_{r+s}) \arrow[r, hook] & l(M)(x_1, ..., x_r) \\
l^\pi(y_1, ..., y_{r+s}) \arrow[u, hook, "degre=|\pi|"] \arrow[r, equal] & l(M)^\pi(x_1, ..., x_r) \arrow[u, hook, "degre=|\pi|"']
\end{tikzcd}$$

Donc $l(M)(x_1, ..., x_r)$ est le corps des fractions de A'.
$(P2)$: A et A' sont clairement des l-algèbres de type fini.
$(P3)$: A est clairement stable par π. On a de plus le diagramme:

$$\begin{tikzcd}
 & l(y_1, ..., y_{r+s}) \\
l^\pi(y_1, ..., y_{r+s}) \arrow[ur, hook, "degre=|\pi|"] \arrow[r, hook] & l(y_1, ..., y_{r+s})^\pi \arrow[u, hook, "degre=|\pi|"']
\end{tikzcd}$$

Donc $l^\pi(y_1, ..., y_{r+s}) = l(y_1, ..., y_{r+s})^\pi$. Donc $y_1, ..., y_{r+s} \in l(y_1, ..., y_{r+s})^\pi$ et A' est bien stable par π.
$(P4)$: A et A' sont bien factoriels.
$(P5)$: $A^*/l^* = M$ et $A'^*/l^* = 1$ sont bien des groupes abéliens de type fini.
D'après 3.1.3, il existe $a \in A^\pi$ et $a' \in A'^\pi$ tels que $A[a^{-1}] = A'[a'^{-1}]$. Notons B cet anneau. La propriété 3.1.4 permet alors d'établir l'existence de deux $\mathbb{Z}[\pi]$-modules de permutation de type fini P_1 et P_2 rendant exactes les deux suites:

$$0 \to A^*/l^* \to B^*/l^* \to P_1 \to 0$$

$$0 \to A'^*/l^* \to B^*/l^* \to P_2 \to 0$$

On déduit l'exactitude des suites:

$$0 \to M \to B^*/l^* \to P_1 \to 0$$

$$0 \to 0 \to B^*/l^* \to P_2 \to 0$$

et donc la propriété (ii) est démontrée.
Supposons (ii). La proposition précédente impose alors que $l(P_2)^\pi/l(M)^\pi$ est une extension transcendante pure. Son degré de transcendance est clairement fini. De plus, d'après 4.4.2, $l(P_2)^\pi/l^\pi$ est aussi transcendante pure. La propriété (i) est donc établie, avec $L = l(P_2)^\pi$. $\square$

Nous en déduisons le corollaire suivant, qui nous sera très utile dans la suite:

Corollaire 4.4.6. ***Modules de permutation et extensions transcendantes pures 2***
Soit M un $\mathbb{Z}[\pi]$-module de type fini, libre en tant que groupe abélien. On suppose que , pour tout sous-groupe ρ de π, on a $H^1(\rho, M) = 0$. Les propositions suivantes sont alors équivalentes:

(i) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(ii) Il existe des modules de permutation P_1 et P_2 de type fini tels que

$$M \oplus P_1 \cong P_2$$

Preuve. Supposons (i). Alors, d'après le théorème précédent, on peut trouver des modules de permutation P_1 et P_2 de type fini rendant exacte la suite $0 \to M \to P_2 \to P_1 \to 0$. D'après les caractérisations des facteurs directs de permutation (4.3.3), cette suite est scindée, d'où la propriété (ii).
L'implication $(ii) \Rightarrow (i)$ découle immédiatement du théorème précédent. □

4.5 Construction du module F_ρ et liens avec les extensions transcendantes pures

On suppose maintenant que π est abélien. Dans cette section, nous allons définir un foncteur de la catégorie des π-modules dans la catégorie des $\mathbb{Z}(\rho)$-modules sans torsion, et nous verrons comment l'étude de ce foncteur permet de dire si une certaine extension est transcendante pure ou pas.
On définit ce foncteur par $F_{\pi,\rho}(M) = (M \otimes_\pi \mathbb{Z}(\rho))/\{\text{éléments d'ordre additif fini}\}$, où M est un π-module et ρ est un groupe quotient cyclique de π. Ce foncteur est bien défini, car le morphisme d'anneaux surjectif $\mathbb{Z}[\pi] \to \mathbb{Z}(\rho)$ nous permet de considérer chaque $\mathbb{Z}(\rho)$-module comme un π-module.

Proposition 4.5.1. ***"Indépendance par rapport au choix de π"***
Soient $S(\pi)$ l'ensemble des quotients cycliques de π et π' un groupe quotient de π. Alors il y a une inclusion naturelle $S(\pi') \subset S(\pi)$. En plus, pour tout π'-module M on a:
i) Si $\rho \in S(\pi')$, alors $F_{\pi,\rho}(M) \cong F_{\pi',\rho}(M)$ en tant que $\mathbb{Z}(\rho)$-modules;
ii) Si $\rho \in S(\pi)$ mais $\rho \notin S(\pi')$, alors $F_{\pi,\rho}(M) = 0$.

Preuve. Déjà, l'inclusion est claire (elle est induite par le morphisme surjectif $\pi \to \pi'$).

Montrons l'assertion i). On a l'isomorphisme $M \otimes_\pi \mathbb{Z}[\pi'] \cong M$, donc $M \otimes_\pi \mathbb{Z}(\rho) = M \otimes_\pi \mathbb{Z}[\pi'] \otimes_\pi \mathbb{Z}(\rho) = M \otimes_{\pi'} \mathbb{Z}(\rho)$.
Montrons l'assertion ii). L'hypothèse $\rho \notin S(\pi')$ montre l'existence d'un élément $\sigma \in \pi$ qui a pour l'image 1 dans π' et dont l'image σ^* dans ρ est différente de 1. L'action de σ sur M est alors triviale, donc $(\sigma^* - 1) \cdot (M \otimes_\pi \mathbb{Z}(\rho)) = 0$, où $\sigma^* - 1$ est un élément non nul de $\mathbb{Z}(\rho)$. Mais alors, si τ est un générateur de ρ et $\sigma^* = \tau^d$ avec $0 < d < |\rho|$, comme les polynômes $\phi_{|\rho|}(X)$ et $X^d - 1$ $(d < |\rho|)$ sont premiers entre eux, il suit que $\sigma^* - 1$ divise un entier non nul dans $\mathbb{Z}(\rho)$ par Bézout. Mais alors $M \otimes_\pi \mathbb{Z}(\rho)$ est un groupe de torsion, et donc $F_{\pi,\rho}(M) = 0$. □

On écrit dorénavant F_ρ au lien de $F_{\pi,\rho}$ par abus de langage.

Proposition 4.5.2. ***Une certaine compatibilité avec l'inclusion***
Soient N un π-module et $M \subset N$ un sous-π-module de N tel que N/M soit un groupe de torsion. Alors $F_\rho(M)$ est isomorphe à l'image de M sous l'application naturelle $N \to F_\rho(N)$, pour tout groupe quotient cyclique ρ de π.

Preuve. Soit J le noyau du morphisme $\mathbb{Z}[\pi] \to \mathbb{Z}(\rho)$. Ceci induit, pour tout π-module P, une surjection $P \to F_\rho(P)$ de noyau $\{p \in P | \exists k \in \mathbb{Z}, k \neq 0, k \cdot p \in J \cdot P\}$. Il suffit alors de voir que $\{m \in M | \exists k \in \mathbb{Z}, k \neq 0, k \cdot m \in J \cdot M\} = M \cap \{n \in N | \exists k \in \mathbb{Z}, k \neq 0, k \cdot n \in J \cdot N\}$. Mais ceci est vrai car N/M est de torsion. □

Proposition 4.5.3. ***Cas d'un module de permutation***
Si N est un π-module de permutation, alors $F_\rho(N)$ est $\mathbb{Z}(\rho)$-libre pour tout ρ groupe quotient cyclique de π.

Preuve. Le module N est un π-module de permutation, donc il suffit de traiter le cas $N = \mathbb{Z}[\pi']$ avec π' un groupe quotient de π car le foncteur que nous avons défini est compatible avec la somme directe. Mais alors d'après la proposition 4.5.1, $F_\rho(N) \cong \mathbb{Z}(\rho)$ ou $F_\rho(N) = 0$. D'où la proposition. □

Théorème 4.5.4. ***F_ρ et isomorphismes 1***
Soit π un groupe cyclique. Soit M un π-module projectif de type fini. Alors $l(M)^\pi$ et $l(\underset{\rho}{\oplus} F_\rho(M))^\pi$ sont isomorphes sur l^π, où ρ parcourt l'ensemble des quotients cycliques de π.

Preuve. Cette preuve est assez longue et délicate. Fixons d'abord les notations pour cette preuve. Soit π un groupe cyclique d'ordre m et de générateur τ. On note $E(m)$ l'ensemble des diviseurs positifs de m. On note π_d l'unique groupe quotient de π d'ordre d pour $d \in E(m)$. On note aussi, pour $C \subset E(m)$, $\phi_C = \prod_{d \in C} \phi_d$.
Si M est un π-module, alors on note, pour tout $C \subset E(m)$, $M_C = M/\phi_C(\tau)M$.
On introduit aussi un graphe qui sera étudié dans lemme 3 et dont l'ensemble

des sommets est l'ensemble des relations d'équivalence sur $E(m)$: si $G(m)$ est l'ensemble des relations d'équivalence sur $E(m)$ et u un élément de $G(m)$ dont l'ensemble de ses classes d'équivalence non nulles est noté $[u]$, alors deux sommets u et v sont les extrémités d'une arête si la condition suivante est vérifiée: il existe $d \in E(m)$ et $D \in [u]$ tels que $E(d) \subset D$, $E(d) \neq D$ et $[v] = \{E(d), D-E(d), C | C \in [u], C \neq D\}$. L'ensemble des arêtes sera noté $S(m)$, et on montrera dans le lemme 3 que ce graphe est connexe.
Lemme 1: Soit M un $\mathbb{Z}[\pi]$-module projectif, et soit $d \in E(m)$. Alors $M_{E(d)}$ est un $\mathbb{Z}[\pi]$-module, facteur direct de permutation.
Preuve du lemme 1: $M_{E(d)} \cong M/(\tau^d - 1)M \cong M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}[\pi]/(\tau^d - 1) \cong M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}[\pi_d]$. M étant projectif, cet isomorphisme impose que $M_{E(d)}$ est un $\mathbb{Z}[\pi_d]$-module projectif, et donc un $\mathbb{Z}[\pi]$-module, facteur direct de permutation.

Lemme 2: Soient M un π-module projectif, et C, C' deux sous-ensembles disjoints de $E(m)$. Alors on a une suite exacte de π-modules:

$$0 \to M_C \to M_{C \cup C'} \to M_{C'} \to 0$$

Preuve du lemme 2: Comme tout passe à la somme directe, il suffit de traiter le cas où $M = \mathbb{Z}[\pi]$. On vérifie l'exactitude de la suite pour les applications suivantes: celle de $M_{C \cup C'}$ vers $M_{C'}$ est la projection naturelle, et celle de M_C vers $M_{C \cup C'}$ est induite par la multiplication par $\phi_{C'}(\tau)$.

Lemme 3: Le graphe $(G(m), S(m))$ est connexe.
Un mot avant de faire la preuve de ce lemme: on ne prend pas en compte l'orientation des chemins.
Preuve du lemme 3:
On note $i(m)$ (resp. $w(m)$) la relation d'équivalence sur $E(m)$ telle que $[i(m)] = \{\{d\} | d \in E(m)\}$ (resp. $[w(m)] = \{E(m)\}$). Il suffit de voir qu'il existe un chemin de u vers $i(m)$ pour tout $u \in G(m)$. On va faire une récurrence (forte) sur m. On note aussi $n(u) = |E(m)| - |[u]|$. Pour m fixé, on fait une récurrence sur $n(u)$.
Récurrence sur m: Si $m = 1$ il n'y a rien à démontrer. Le passage de $\leq m$ à $m+1$ se fait par une récurrence sur $n(u)$.
Récurrence sur $n(u)$: Si $n(u) = 0$, alors $u = i(m)$ et on a gagné. On suppose donc $n(u) > 0$, et soit e le plus petit élément de $E(m)$ tel qu'il existe $D \in [u]$ avec $|D| > 1$ (non trivial) et $e \in D$. Il suffit donc de montrer qu'on peut isoler e dans D. Comme $u \neq i(m)$, on a $e < m$. On peut donc appliquer l'hypothèse de récurrence sur m, qui donne un chemin de $i(e)$ à $w(e)$ dans le graphe $(G(e), S(e))$. On va noter ce chemin $(v_j)_{0 \leq j \leq b}$, et on va modifier ce chemin dans la suite. Pour $0 \leq j \leq b$, on note $D_j \in [v_j]$ la classe qui contient e, i.e. $e \in D_j$. On définit alors un chemin de longueur $2b+1$ qui permet de

séparer e des autres éléments de D. Pour $0 \leq j \leq b$, on définit $u_j \in G(m)$ par $[u_j] = \{C \in [u] | C \cap E(e) = \emptyset\} \cup \{D \cup D_j\} \cup ([v_j] - \{D_j\})$. Pour $b+1 \leq j \leq 2b+1$, on définit $u_j \in G(m)$ par $[u_j] = \{C \in [u] | C \cap E(e) = \emptyset\} \cup \{D - \{e\}\} \cup [v_{2b+1-j}]$. On vérifie bien qu'il s'agit d'un chemin sur le graphe, comme on peut s'en convaincre à partir d'une figure: On a par ailleurs $[u_{2b+1}] = \{D - \{e\}, \{e\}\} \cup \{[u] - \{D\}\}$. On a donc réussi à isoler e dans la classe D, il suit que $n(u_{2b+1}) = n(u) - 1$. L'hypothèse de récurrence fournit alors un chemin de u_{2b+1} à $i(m)$. On peut donc relier u à $i(m)$.
On a ainsi bien montré la connexité du graphe (dans le sens d'un graphe non-orienté).

<u>Lemme 4:</u> (Un invariant du graphe) Si $u, v \in G(m)$, alors $l(M(u))^\pi \cong l(M(v))^\pi$ sur l^π, où $M(s) = \underset{C \in [s]}{\oplus} M_C$ pour $s \in G(m)$.
<u>Preuve du lemme 4:</u> Déjà remarquons que le lemme précédent nous permet de simplifier la situation: il suffit de faire cette preuve dans le cas de deux extrémités d'une arête du graphe. On peut alors appliquer le lemme 2 pour avoir une suite exacte de π-modules:

$$0 \to M_{D-E(d)} \to M_D \to M_{E(d)} \to 0$$

Cette suite exacte donne lieu alors, en ajoutant un facteur $N = \underset{C \in [u], C \neq D}{\oplus} M_C$, la suite exacte suivante:

$$0 \to N \oplus M_{D-E(d)} \to N \oplus M_D \to M_{E(d)} \to 0$$

de modules $\mathbb{Z}$-libres car M est projectif. En appliquant les lemmes 1 (de cette démonstration) et 4.4.3, on a un isomorphisme de corps entre $l(N \oplus M_{D-E(d)} \oplus M_{E(d)})^\pi$ et $l(N \oplus M_D)^\pi$ sur l^π. Mais ceci est tout simplement un isomorphisme $l(M(u))^\pi \cong l(M(v))^\pi$ sur l^π, puisque u et v sont les extrémités d'une même arête du graphe.
Finalement on est en mesure de démontrer le théorème:

<u>Preuve du théorème:</u> reprenons les notations $i(m)$ et $w(m)$ du lemme 3. Alors en appliquant le lemme 4 à $u = i(m)$, $v = w(m)$, on a $M(i(m)) = \underset{d|m}{\oplus} M/(\phi_d(\tau)M) \cong \underset{\rho}{\oplus} F_\rho(M)$ et $M(w(m)) = M$, ce qui donne l'isomorphisme entre $l(M)^\pi$ et $l(\underset{\rho}{\oplus} F_\rho(M))^\pi$ sur l^π. D'où le théorème. $\square$

Nous en déduisons le corollaire suivant:

Corollaire 4.5.5. ***F_ρ et isomorphismes 2***
Soit π un groupe abélien fini. Soit M un $\mathbb{Z}[\pi]$-module de type fini de la forme

$$M = \bigoplus_{\pi'} M_{\pi'}$$

où $M_{\pi'}$ est un $\mathbb{Z}[\pi']$-module projectif, π' décrivant les quotients cycliques de π. On a alors le l^π-isomorphisme de corps:

$$l(M)^\pi \cong l\left(\bigoplus_\rho F_\rho(M)\right)^\pi$$

ρ décrivant les quotients cycliques de π.

Preuve. Soit π' un quotient cyclique de π. Notons $\pi' = \pi/\pi''$. Le théorème précédent appliqué au groupe cyclique π', au module $M_{\pi'}$ et au corps $l^{\pi''}$ permet d'obtenir le l^π-isomorphisme de corps:

$$l(M_{\pi'})^\pi \cong l\left(\bigoplus_{\rho'} F_{\rho'}(M_{\pi'})\right)^\pi$$

où la somme est prise sur les quotients cycliques de π'. La proposition 4.5.1 permet alors d'écrire:

$$l(M_{\pi'})^\pi \cong l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)^\pi$$

où la somme est prise sur les quotients cycliques de π.
Montrons que cela implique que $l(M_{\pi'}) \cong l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$. Pour ce faire, la bonne notion à introduire est celle des extensions linéairement disjointes. Cependant, afin de ne pas introduire de nouvelles notions qui ne serviront que dans cette preuve, nous allons donner une démonstration “ à la main ”.
Étudions d'abord $l(M_{\pi'})^\pi$. En appliquant le théorème de l'élément primitif, soit l_0 tel que $1, l_0, ..., l_0^{p-1}$ soit une base de l sur l^π, où p est l'ordre de π. Montrons que, dans le corps $l(M_{\pi'})$, $1, l_0, ..., l_0^{p-1}$ sont libres sur $l(M_{\pi'})^\pi$. Soient $a_1, ..., a_p \in l(M_{\pi'})^\pi$ tels que

$$\sum_{i=1}^{p} a_i l_0^{i-1} = 0$$

On a alors, pour tout $\sigma \in \pi$,

$$\sum_{i=1}^{p} a_i \sigma(l_0)^{i-1} = 0$$

Donc, si $\sigma_1, ..., \sigma_p$ sont les éléments de π et si $V(\sigma_1(l_0), ..., \sigma_p(l_0))$ est la matrice de Van der Monde associée à $\sigma_1(l_0), ..., \sigma_p(l_0)$, alors:

$$V(\sigma_1(l_0), ..., \sigma_p(l_0))^t(a_1, ..., a_p) = 0$$

On en déduit que $a_1 = ... = a_p = 0$, d'où la liberté de $1, l_0, ..., l_0^{p-1}$ sur $l(M_{\pi'})^\pi$.
On déduit immédiatement que l'application l^π-linéaire $l(M_{\pi'})^\pi \otimes_{l^\pi} l \to l(M_{\pi'})$ définie par $a \otimes b \to ab$ est injective. Munissons $l(M_{\pi'})^\pi \otimes_{l^\pi} l$ d'une structure d'anneau par $(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$. L'application linéaire précédente est alors un morphisme d'anneaux injectif, dont l'image est

$$l(M_{\pi'})^\pi l = \left\{ \sum a_i b_i, a_i \in l(M_{\pi'})^\pi, b_i \in l \right\}$$

où les somes prises sont toutes finies. On en déduit que $l(M_{\pi'})^\pi l$ est un $l(M_{\pi'})^\pi$-espace vectoriel de dimension p, inclus dans $l(M_{\pi'})$, qui est aussi un $l(M_{\pi'})^\pi$-espace vectoriel de dimension p. Par conséquent, $l(M_{\pi'})^\pi l = l(M_{\pi'})$. On en déduit que $l(M_{\pi'})^\pi \otimes_{l^\pi} l$ est un corps l-isomorphe à $l(M_{\pi'})$.
De manière analogue, $l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)^\pi \otimes_{l^\pi} l$ est muni d'une structure de corps l-isomorphe à $l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$. Nous en déduisons un l-isomorphisme entre les corps $l(M) \cong l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$, qui commute avec l'action de π. On en déduit un isomorphisme

$$l(M) \cong \left(\bigoplus_\rho F_\rho(M) \right)$$

qui commute avec l'action de π, d'où le résultat.

□

Le résultat suivant jouera un rôle important dans la suite:

Théorème 4.5.6. ***Lien entre F_ρ et les extensions transcendantes pures***
Soit π un groupe abélien fini. Soit M un $\mathbb{Z}[\pi]$-module de la forme:

$$M = \bigoplus_{\pi'} M_{\pi'}$$

où $M_{\pi'}$ est un $\mathbb{Z}[\pi']$-module projectif, π' décrivant les quotients cycliques de π. Il y a alors équivalence entre les propriétés suivantes:

(i) Le corps $l(M)^\pi$ est une extension transcendante pure de l^π.

(ii) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(iii) Pour tout quotient cyclique ρ de π, $F_\rho(M)$ est un $\mathbb{Z}(\rho)$-module libre.

Preuve. Supposons (ii). Le module M est un facteur direct de permutation sur $\mathbb{Z}[\pi]$, donc d'après 4.3.2, nous pouvons appliquer 4.4.6. Il existe donc des $\mathbb{Z}[\pi]$-modules de permutation de type fini N_1 et N_2 tels que $M \oplus N_1 \cong N_2$. D'après 4.5.3, pour tout quotient cyclique ρ de π, $F_\rho(N_1)$ et $F_\rho(N_2)$ sont des $\mathbb{Z}(\rho)$-modules libres tels que $F_\rho(M) \oplus F_\rho(N_1) \cong F_\rho(N_2)$. Comme $\mathbb{Z}(\rho)$ est un anneau de Dedekind, d'après le théorème de structure des modules de type fini sur un anneau de Dedekind, cela impose que $F_\rho(M)$ est un $\mathbb{Z}(\rho)$-module libre, d'où (iii).
Supposons maintenant (iii). Soit $r(\pi')$ le rang de $M_{\pi'}$ sur $\mathbb{Z}[\pi']$. Posons

$$N = \bigoplus_{\pi'} \mathbb{Z}[\pi']^{r(\pi')}$$

Soit ρ un quotient cyclique de π. Par hypothèse, $F_\rho(M)$ est libre. Soit $\mathcal{G}$ l'ensemble des quotients cycliques π' de π tels que ρ est un quotient de π'. Alors le rang de $F_\rho(M)$ est:

$$R = \sum_{\pi' \in \mathcal{G}} r(\pi')$$

D'autre part, il est clair que $F_\rho(N)$ est libre de rang R. Donc $F_\rho(M)$ et $F_\rho(N)$ sont des $\mathbb{Z}(\rho)$-modules isomorphes. Par conséquent,

$$\bigoplus_{\rho} F_\rho(M) \cong \bigoplus_{\rho} F_\rho(N)$$

Avec 4.5.5, on déduit les l^π-isomorphismes

$$l(M)^\pi \cong l\left(\bigoplus_{\rho} F_\rho(M)\right)^\pi \cong l\left(\bigoplus_{\rho} F_\rho(N)\right)^\pi \cong l(N)^\pi$$

Or, d'après 4.4.2, $l(N)^\pi$ est une extension transcendante pure de l^π, d'où (i). $\square$

4.6 Étude des modules I_q et J_q

Soit p un nombre premier et posons $q = p^s$, où $s > 0$. On se donne un corps l, de caractéristique distincte de p, et contenant une racine primitive q-ième de l'unité, notée ζ_q. On considère aussi un groupe abélien fini π d'automorphismes de l. On note alors $k = l^\pi$. L'extension $l|k$ est alors finie galoisienne de groupe de Galois π. Soient $\pi(q) = Gal(l|k(\zeta_q))$ et $\rho(q) = Gal(k(\zeta_q)/k)$. La théorie de Galois impose alors que $\rho(q) = \pi/\pi(q)$. L'application $\pi \to (\mathbb{Z}/q\mathbb{Z})^*, \sigma \mapsto t$ telle que $\sigma(\zeta_q) = \zeta_q^t$ est un morphisme de groupes dont le noyau est $\pi(q)$. Elle se factorise donc en un morphisme de groupes injectif $\varphi_q : \rho(q) \to (\mathbb{Z}/q\mathbb{Z})^*$. Ceci permet de munir $\mathbb{Z}/q\mathbb{Z}$

d'une structure de $\mathbb{Z}[\rho(q)]$-module, et donc aussi d'une structure de $\mathbb{Z}[\pi]$-module.

Supposons dans un premier temps que $\rho(q)$ n'est pas cyclique. On sait que, dès que p est impair ou $s < 3$, $\mathbb{Z}/q\mathbb{Z}$ est cyclique. On en déduit que nécessairement $p = 2$ et $s \geq 3$. Notons $C(q) = (\mathbb{Z}/q\mathbb{Z}) - \{0\}$, et considérons $\mathbb{Z}^{C(q)}$ le $\mathbb{Z}[\rho(q)]$-module de permutation de $\mathbb{Z}$-base $(e_c)_{c \in C(q)}$ indexée par $C(q)$ tel que, pour $\sigma \in \rho(q)$ et $c \in C(q)$, $\sigma(e_c) = e_{\sigma c}$. Soit $i_q : \mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z}$ le morphisme de $\mathbb{Z}[\rho(q)]$-modules tel que $i_q(e_c) = c$, pour $c \in C(q)$. Soit $I_q = Ker(i_q)$. On a alors la suite exacte:

$$0 \to I_q \to \mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Proposition 4.6.1. ***Cohomologie de*** I_q
Supposons $\rho(q)$ non cyclique.

(i) Pour tout sous-groupe ρ de π, $H^1(\rho, I_q) = 0$.

(ii) Il existe un sous-groupe ρ de π tel que $\widehat{H}^{-1}(\rho, I_q) \neq 0$.

Preuve.

(i) Soit ρ un sous-groupe de π. Écrivons la suite exacte de cohomologie:

$$0 \to I_q^\rho \to (\mathbb{Z}^{C(q)})^\rho \to (\mathbb{Z}/q\mathbb{Z})^\rho \to H^1(\rho, I_q) \to 0$$

car $\mathbb{Z}^{C(q)}$ est un module de permutation. La flèche $(\mathbb{Z}^{C(q)})^\rho \to (\mathbb{Z}/q\mathbb{Z})^\rho$ étant clairement surjective, on a bien $H^1(\rho, I_q) = 0$.

(ii) Montrons d'abord qu'il existe ρ_0 sous-groupe de $\rho(q)$ tel que $\widehat{H}^{-1}(\rho_0, I_q) \neq 0$. Par hypothèse, $\rho(q)$ n'est pas cyclique. De plus, il s'injecte dans $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$. Par conséquent, on peut trouver ρ_0 un sous-groupe de $\rho(q)$ tel que $\varphi_q(\rho_0) = \{1, -1, u+1, u-1\} \cong (\mathbb{Z}/2\mathbb{Z})^2$, où $u = q/2$.
Soit $C = \{1, u-1, u, u+1, -1\} \subseteq \mathbb{Z}/q\mathbb{Z}$. Tout comme nous avons muni $\mathbb{Z}^{C(q)}$ d'une structure de $\mathbb{Z}[\rho(q)]$-module, on peut munir $\mathbb{Z}^C$ d'une structure de $\mathbb{Z}[\rho_0]$-module. En considérant la restriction de $\mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z}$ à $\mathbb{Z}^C$, on obtient la suite exacte:

$$0 \to \mathbb{Z}^C \cap I_q \to \mathbb{Z}^C \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Posons $M = \mathbb{Z}^C \cap I_q$. Montrons que $H^1(\rho_1, M) = 0$, pour ρ_1 l'un des cinq sous-groupe de $\rho_0 \cong (\mathbb{Z}/2\mathbb{Z})^2$. D'après la suite exacte de cohomologie, il suffit de montrer que la flèche $f_{\rho_1} : (\mathbb{Z}^C)^{\rho_1} \to \mathbb{Z}/q\mathbb{Z}^{\rho_1}$ est surjective.
Si $\rho_1 = 1$, il est clair que f_{ρ_1} est surjective.
Si $\rho_1 = \rho_0$ ou $\rho_1 = \varphi_q^{-1}(\{1, -1\})$ ou $\rho_1 = \varphi_q^{-1}(\{1, u-1\})$, alors $\mathbb{Z}/q\mathbb{Z}^{\rho_1} = \{0, u\}$ et $e_u \in (\mathbb{Z}^C)^{\rho_1}$, donc f_{ρ_1} est surjective.

Finalement, si $\rho_1 = \varphi_q^{-1}(\{1, u+1\})$, alors $\mathbb{Z}/q\mathbb{Z}^{\rho_1} = \{0, 2, 4, ..., q-2\}$. Comme $(u+2)/2$ est impair, il est inversible dans $\mathbb{Z}/q\mathbb{Z}$. Soit donc $\lambda \in \mathbb{N}$ tel que $\lambda(u+2) \equiv 2 \pmod q$. Alors l'image de $k\lambda(e_1 + e_{u+1}) \in (\mathbb{Z}^C)^{\rho_1}$ par f_{ρ_1} est $2k$, d'où la surjectivité de f_{ρ_1}.
Ainsi, nous avons montré que, dans tous les cas, $H^1(\rho_1, I_q) = 0$.
Montrons à présent que $\widehat{H}^{-1}(\rho_0, M) \neq 0$. Considérons:

$$x = (1 - u/2)e_1 + (u/2)e_{-1} - e_{1+u}$$

Il est clair que $x \in M$, et on remarque que $\sum_{\sigma \in \rho_1} \sigma x = 0$. Montrons donc que x n'est pas dans $I_{\rho_0}M$, où I_{ρ_0} est l'idéal de $\mathbb{Z}[\rho_0]$ engendré par les $\sigma - 1$ pour $\sigma \in \rho_0$. Soit $\alpha = \sum_{c \in C} \alpha_c e_c$ un élément de M. Alors q divise $\sum_{c \in C} c\alpha_c$, et donc u divise $\alpha_1 - \alpha_{u-1} + \alpha_{u+1} + \alpha_{-1}$. Or, on remarque que les composantes selon e_{u-1} et e_{-1} de:
*$(\phi_q^{-1}(u-1) - \phi_q^{-1}(1))\alpha$ sont $\alpha_1 - \alpha_{u-1}$ et $\alpha_{u+1} - \alpha_{-1}$ respectivement.
*$(\phi_q^{-1}(u+1) - \phi_q^{-1}(1))\alpha$ sont $\alpha_{-1} - \alpha_{u-1}$ et $\alpha_{u-1} - \alpha_{-1}$ respectivement.
*$(\phi_q^{-1}(-1) - \phi_q^{-1}(1))\alpha$ sont $\alpha_{u+1} - \alpha_{u-1}$ et $\alpha_1 - \alpha_{-1}$ respectivement.
Dans les 3 cas, la somme des coefficients de e_{u-1} et e_{-1} est donc multiple de u. On en déduit par linéarité que, pour tout élément de $I_{\rho_0}M$, la somme des coefficients de e_{u-1} et de e_{-1} est multiple de u. Or, pour x, cette somme vaut $u/2$, donc x n'appartient pas à $I_{\rho_0}M$. Ainsi, $\widehat{H}^{-1}(\rho_0, M) \neq 0$.
En composant la flèche $I_q \to \mathbb{Z}^{C(q)}$ avec la projection $\mathbb{Z}^{C(q)} \to \mathbb{Z}^{C(q)-C}$, on obtient une application $I_q \to \mathbb{Z}^{C(q)-C}$ rendant exacte la suite de $\mathbb{Z}[\rho_0]$-modules:

$$0 \to M \to I_q \to \mathbb{Z}^{C(q)-C} \to 0$$

Comme pour tout sous-groupe ρ_1 de ρ_0 on a $H^1(\rho_1, M) = 0$ et comme $\mathbb{Z}^{C(q)-C}$ est un facteur direct de permutation, d'après 4.3.3 la suite précédente est scindée. Donc $I_q = M \oplus \mathbb{Z}^{C(q)-C}$ et donc $\widehat{H}^{-1}(\rho_0, I_q) \neq 0$. Finalement, si l'on note ρ l'image réciproque de ρ_0 par la projection $\pi \to \rho(q)$, on obtient immédiatement que $\widehat{H}^{-1}(\rho, I_q) \neq 0$.

□

À partir d'ici, et jusqu'à la fin de cette partie, nous supposerons $\rho(q)$ cyclique. Notons J_q le noyau du morphisme $\mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z}$ induit par φ_q, de telle sorte que la suite suivante de $\mathbb{Z}[\rho(q)]$-modules est exacte:

$$0 \to J_q \to \mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Nous allons étudier le module J_q.

Proposition 4.6.2. ***Projectivité de*** J_q
Supposons $\rho(q)$ cyclique. Supposons de plus que 4 ne divise pas q ou que $\varphi_q(\rho(q))$ n'est pas égal à $\{1, -1\}$. Alors J_q est un $\mathbb{Z}[\rho(q)]$-module projectif.

Preuve. Notons $\rho = \varphi_q(\rho(q))$ et ρ_1 l'image réciproque de ρ par $\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$. Notons aussi n l'ordre de ρ. Alors l'ordre de ρ_1 est np. Montrons par l'absurde que ρ_1 est cyclique.
Suposons donc que ρ_1 ne soit pas cyclique. Par conséquent, $(\mathbb{Z}/pq\mathbb{Z})^*$ n'est pas cyclique, et donc pq est une puissance de 2 au moins égale à 8. Donc $p = 2$ et 4 divise q. On a alors $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-1}\mathbb{Z}$, et donc, comme ρ_1 n'est pas cyclique, nécessairement $-1 \in \rho_1$, d'où $-1 \in \rho$. Ainsi, ρ est un sous-groupe cyclique de $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$ contenant -1. On en déduit que $\rho = \{1, -1\}$: c'est absurde! Donc ρ_1 est cyclique.
Soit $t \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/pq\mathbb{Z}$ engendre ρ_1. L'odre de ρ_1 étant strictement plus grand que n, pq ne divise pas $t^n - 1$. Or la classe de t dans $\mathbb{Z}/q\mathbb{Z}$ engendre ρ, donc q divise $t^n - 1$. On peut donc écrire $t^n - 1 = aq$ avec $a \wedge q = 1$.
On se donne alors $\tau \in \rho(q)$ tel que $\phi_q(\tau) = t \pmod q$. Alors τ engendre $\rho(q)$ et J_q est l'idéal de $\mathbb{Z}[\rho(q)]$ engendré par $\tau - t$ et a: pour le voir, il suffit de remarquer que les $(\tau - t)^k$ pour $0 \leq k \leq n-1$ forment une base du groupe abélien libre $\mathbb{Z}[\rho(q)]$. Notons M l'idéal engendré par $\tau - t$ et a. Comme $a \wedge q = 1$, on a $J_q + M = \mathbb{Z}[\rho(q)]$, et donc $J_q M = J_q \cap M$, d'où la suite exacte de $\mathbb{Z}[\rho(q)]$-modules:

$$0 \to J_q M \to J_q \oplus M \to \mathbb{Z}[\rho(q)] \to 0$$

où l'application $J_q \oplus M \to \mathbb{Z}[\rho(q)]$ est donnée par $(j, m) \mapsto j - m$. Cette suite est scindée puisque $\mathbb{Z}[\rho(q)]$ est projectif. Donc $J_q \oplus M = J_q M \oplus \mathbb{Z}[\rho(q)]$.
Remarquons que l'idéal $J_q M$ est engendré par $(\tau - t)^2$, $a(\tau - t)$, $q(\tau - t)$ et aq. Comme $aq = t^n - \tau^n$ et $a \wedge q = 1$, on a $J_q M = (\tau - t)\mathbb{Z}[\rho(q)]$, qui est un $\mathbb{Z}[\rho(q)]$-module libre. Par conséquent, $J_q \oplus M$ est libre, et donc J_q est projectif. □

Pour la preuve de la proposition suivante, nous aurons besoin du petit lemme suivant:

Lemme 4.6.3. ***Idéaux d'indice une puissance de 2***
Soit I un idéal de $\mathbb{Z}[\zeta_{2^r}]$ d'indice $2^{r'}$. Alors $I = (1 - \zeta_{2^r})^{r'}$.

Preuve. L'anneau $\mathbb{Z}[\zeta_{2^r}]$ est un anneau de Dedekind. Soit $\mathfrak{p}$ un idéal premier (et donc maximal) contenant I. L'idéal $N_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}}(\mathfrak{p})$ est l'indice de $\mathfrak{p}$ dans $\mathbb{Z}[\zeta_{2^r}]$, c'est à dire une puissance de 2. C'est en plus un nombre premier: c'est donc 2. On en déduit que $\mathfrak{p}$ est d'indice 2, et donc $2 \in \mathfrak{p}$. En remarquant que $\Phi_{2^r}(1) = 2 = \prod_{1 \leq a \leq 2^r, a \wedge 2 = 1}(1 - \zeta_{2^r}^a)$, il existe a_0 tel que $1 \leq a_0 \leq 2^r$, a_0 impair et $1 - \zeta_{2^r}^{a_0} \in \mathfrak{p}$. Comme $1 - \zeta_{2^r}^{a_0}$ et $1 - \zeta_{2^r}$ sont associés, $1 - \zeta_{2^r} \in \mathfrak{p}$. Comme $(1 - \zeta_{2^r})$ est maximal, c'est $\mathfrak{p}$. En tenant compte de 2.1.7, il existe r'' tel que $I = (1 - \zeta_{2^r})^{r''}$. En calculant la norme de I, on obtient alors que $r'' = r'$. □

Nous sommes à présent en mesure d'établir le résultat suivant:

Proposition 4.6.4. ***Lien entre J_q et les extensions transcendantes pures***
Supposons $\rho(q)$ cyclique. Supposons de plus que $p = 2$. Alors $l(J_q)^\pi$ est une extension transcendante pure de l^π.

Preuve. Quitte à remplacer l par $l^{\pi(q)}$, on peut supposer $\pi = \rho(q)$.
Supposons d'abord que 4 ne divise pas q ou que $\varphi_q(\rho(q)) \neq \{-1, 1\}$. Alors, d'après 4.6.2, J_q est un $\mathbb{Z}[\pi]$-module projectif. Donc, d'après 4.5.6, il suffit de voir que $F_\rho(J_q)$ est cyclique pour tout quotient ρ de π. Soit donc ρ un tel quotient, et notons 2^r son ordre. Comme $\mathbb{Z}[\pi]/J_q$ est un groupe de torsion, d'après 4.5.2, $F_\rho(J_q)$ est un sous-module de $F_\rho(\mathbb{Z}[\pi]) \cong \mathbb{Z}(\rho) \cong \mathbb{Z}[\zeta_{2^r}]$ d'indice une puissance de 2. D'après le lemme précédent, $F_\rho(J_q)$ est libre, d'où le résultat.
Supposons maintenant que 4 divise q et que $\varphi_q(\rho(q)) = \{-1, 1\}$. Notons $\rho(q) = \{1, \tau\}$, avec $\varphi_q(\tau) = -1$. Notons $x = 1 + \tau$ et $y = \frac{1}{2}q(1 - \tau)$. Une vérification immédiate montre que $J_q = \mathbb{Z}x \oplus \mathbb{Z}y$, et on a $\tau \cdot x = x$ et $\tau \cdot y = -y$. Donc $l(J_q) = l(x, y)$, où $\tau(x) = x$ et $\tau(y) = y^{-1}$. Soit $\alpha \in l$ tel que $\tau(\alpha) \neq \alpha$, et posons $z = \frac{\alpha y + \tau(\alpha)}{y+1}$. On a alors $\tau(z) = z$, et donc $l(x, y)^\pi = l^\pi(x, z)$, avec x et z algébriquement indépendants sur l^π. □

Pour $m \in \mathbb{Z}$, notons $ord(m)$ la valuation p-adique de p dans m. Nous aurons besoin dans la suite du lemme arithmétique suivant:

Lemme 4.6.5. ***Un lemme d'arithmétique élémentaire***
Supposons p impair. Soit $t \in \mathbb{Z}$ non divisible par p. Soit f l'ordre de sa classe modulo p dans $(\mathbb{Z}/p\mathbb{Z})^*$. Alors:

(i) $ord(\phi_f(t)) = ord(t^f - 1) > 0$,
$ord(\phi_{fp^i}(t)) = 1$ *pour* $i > 0$,
$ord(\phi_d(t)) = 0$ *pour d ne s'écrivant pas sous la forme fp^i pour $i \geq 0$.*

(ii) $ord(t^m - 1) = 0$ *si $m > 0$ n'est pas multiple de f,*
$ord(t^m - 1) = ord(t^f - 1) + ord(m)$ *si $m > 0$ est multiple de f.*

Preuve. Soit $m > 0$.
Si f ne divise pas m, alors $ord(t^m - 1) = 0$, et comme $\phi_m(t) \mid t^m - 1$, $ord(\phi_m(t)) = 0$.
Supposons à présent que f divise m. Écrivons $m = fp^i n$, avec n non multiple de p. Notons $r = fp^i$.
Supposons d'abord $n > 1$. Avec la formule du binôme,

$$\frac{t^m - 1}{t^r - 1} = \frac{((t^r - 1) + 1)^n}{t^r - 1} = \sum_{0 \leq i \leq n-1} C_n^{i+1}(t^r - 1)^i \equiv n(mod p)$$

donc $ord(t^m - 1) = ord(t^r - 1)$. De plus, comme $\phi_m(t) | \frac{t^m - 1}{t^r - 1}$, $ord(\phi_m(t)) = 0$.
On est donc maintenant ramenés à étudier le cas où $n = 1$. Supposons que $i > 0$.

Notons $s = fp^{i-1}$. Encore avec la formule du binôme, on a:

$$\frac{t^m - 1}{t^s - 1} = \frac{((t^s - 1) + 1)^p}{t^s - 1} = \sum_{0 \leq i \leq p-1} C_p^{i+1}(t^s - 1)^i \equiv p(mod p^2)$$

donc $ord(t^m - 1) = ord(t^s - 1) + 1$. De plus,

$$\frac{t^m - 1}{t^s - 1} = \prod_{d|m, d\nmid s} \phi_d(t)$$

et donc, comme le seul d tel que $f \mid d \mid m$ mais $d \nmid s$ est m, on a $ord(\phi_m(t)) = 1$. Finalement, une récurrence simple donne que $ord(t^m - 1) = ord(t^f - 1) + ord(m)$, et on a terminé. □

Si K est une extension cyclique de k contenue dans l, alors $Gal(K|k)$ est un quotient cyclique de π. Nous noterons F_K au lieu de $F_{Gal(K|k)}$. Nous pouvons maintenant montrer la proposition suivante:

Proposition 4.6.6. ***Calculs de*** $F_K(J_q)$
Supposons p impair. Soit τ un générateur de $\rho(q)$, et soit $t \in \mathbb{Z}$ tel que $\tau(\zeta_q) = \zeta_q^t$. Soit f l'ordre de $t \mod p$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, et soit r tel que $p^r = q \wedge (t^f - 1)$. On a alors:

(a) Tout corps intermédiaire $k \subseteq K \subseteq k(\zeta_q)$ est uniquement déterminé par le degré $[K : k]$. De plus, le groupe $\rho_K = Gal(K|k)$ est cyclique, engendré par l'image τ_K de τ dans ρ_K.

(b) (i) Si $K = k(\zeta_p)$, alors $K = k(\zeta_{p^i})$ pour tout $1 \leq i \leq r$, $[K : k] = f$, et $F_K(J_q)$ est isomorphe à l'idéal $(p, \tau_k - t)^r$ en tant que $\mathbb{Z}(\rho_K)$-module.

(ii) Si $K = k(\zeta_{p^i})$ pour $r < i \leq s$, alors $[K : k] = fp^{i-r}$, et $F_K(J_q)$ est isomorphe à l'idéal $(p, \tau_K - t)$ en tant que $\mathbb{Z}(\rho_K)$-module.

(iii) Pour tous les autres corps intermédiaires $k \subseteq K \subseteq k(\zeta_q)$, $F_K(J_q)$ est isomorphe à $\mathbb{Z}(\rho_K)$ en tant que $\mathbb{Z}(\rho_K)$-module.

Preuve.

(a) Immédiat d'après la théorie de Galois et en tenant compte du fait que $k(\zeta_q)|k$ est cyclique.

(b) Soit $1 \leq i \leq s$. La théorie de Galois impose que $[k(\zeta_{p^i}) : k]$ est le plus petit entier strictement positif m tel que $\tau^m(\zeta_{p^i}) = \zeta_{p^i}$, c'est-à-dire tel que p^i divise $t^m - 1$. Avec le lemme précédent, on déduit que $[k(\zeta_{p^i}) : k] = f$ si $1 \leq i \leq r$, $[k(\zeta_{p^i}) : k] = fp^{i-r}$ sinon. En combinant avec (a), cela permet d'établir que

si $K = k(\zeta_p)$, alors $K = k(\zeta_p^i)$ pour $1 \leq i \leq r$.
Soit K un corps intermédiaire entre k et $k(\zeta_q)$. Soit $d = [K : k]$. On a clairement $d|fp^{s-r}$. Rappelons que la suite $0 \to J_q \to \mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z} \to 0$ est exacte. En tensorisant par $\mathbb{Z}(\rho_K)$ au-dessus de $\mathbb{Z}[\rho(q)]$, on obtient la suite exacte de $\mathbb{Z}(\rho_K)$-modules suivante:

$$J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to 0$$

D'après 4.6.2, J_q est projectif, donc $J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) = F_K(J_q)$. De plus, $F_K(\mathbb{Z}[\rho(q)]) = \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \cong \mathbb{Z}(\rho_K)$. Comme $\mathbb{Z}[\rho(q)]/J_q$ est un groupe de torsion, la proposition 4.5.2 impose que la flèche

$$J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K)$$

est injective, d'où l'exactitude de la suite:

$$0 \to J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to 0$$

Comme $\mathbb{Z}(\rho_K) = \mathbb{Z}[\rho(q)]/\phi_d(\tau)\mathbb{Z}[\rho(q)]$, on a:

$$\mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \cong (\mathbb{Z}/q\mathbb{Z})/\phi_d(\tau)(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q\mathbb{Z} + \phi_d(t)\mathbb{Z})$$

On en déduit la suite exacte:

$$0 \to F_K(J_q) \to \mathbb{Z}(\rho_K) \to \mathbb{Z}/(q\mathbb{Z} + \phi_d(t)\mathbb{Z}) \to 0$$

Dans le cas (iii), d'après le lemme précédent, $q \wedge \phi_d(t) = 1$, et donc $F_K(J_q) \cong \mathbb{Z}(\rho_K)$. Dans le cas (ii), encore d'après le lemme précédent, $q \wedge \phi_d(t) = p$, donc $F_K(J_q)$ est d'indice p dans $\mathbb{Z}(\rho_K)$. Comme il contient $(p, \tau_K - t)$ qui est d'indice au plus p, $F_K(J_q) \cong (p, \tau_K - t)$. Dans le cas (i), $q \wedge \phi_d(t) = p^r$, donc $F_K(J_q)$ est d'indice p^r dans $\mathbb{Z}(\rho_K)$. Comme il contient $(p, \tau_K - t)^r$ qui est d'indice au plus p^r, $F_K(J_q) \cong (p, \tau_K - t)^r$.

□

Nous pouvons finalement énoncer la proposition suivante, qui permet de relier le module $F_K(J_q)$ à l'idéal $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$:

Corollaire 4.6.7. ***Lien entre*** $F_K(J_q)$ ***et l'idéal*** $\mathfrak{a}(\mathbb{Z}/q\mathbb{Z})$
Supposons $p \neq 2$. Soit K un corps intermédaire $k \subset K \subset l$ tel que $\rho_K = Gal(K|k)$ est cyclique. Alors on a les isomorphismes de $\mathbb{Z}(\rho_K)$-modules suivants:

(i) Si $K \subseteq k(\zeta_q)$, $F_K(J_q) \cong \mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$.

(ii) Si $K \nsubseteq k(\zeta_q)$, $F_K(J_q) = 0$.

Preuve. Il s'agit ici de revenir à la définition de $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ et d'utiliser la proposition précédente. On reprend les notations de la proposition précédente.
Supposons que $K \subseteq k(\zeta_q)$. En reprenant les notations de la partie 4.2, on a

$$\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = \prod_{(a,b)\in T} \mathfrak{a}_K(a^b)^{m(\mathbb{Z}/q\mathbb{Z},a,b)}$$

- Si $K = k(\zeta_p)$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *si $1 \leq b \leq r$, $\mathfrak{a}_K(p^b) = (\tau_K - t, p)$ et $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 1$.
  *si $r < b \leq s$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = (p, \tau - t)^r \cong F_K(J_q)$.

- Si $K = k(\zeta_{p^i})$ pour $r < i \leq s$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *$\mathfrak{a}_K(p^i) = (\tau_K - t, p)$ et $m(\mathbb{Z}/q\mathbb{Z}, p, i) = 1$.
  *si $b \leq s$ et $b \neq i$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = (p, \tau - t) \cong F_K(J_q)$.

- Pour tous les autres $K \subseteq k(\zeta_q)$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *si $1 \leq b \leq s$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}(\rho_K) \cong F_K(J_q)$.

Par conséquent, pour terminer la preuve, il ne reste plus qu'à voir que, si $K \nsubseteq k(\zeta_q)$, alors $F_K(J_q) = 0$. Dans ce cas, J_q est un $\mathbb{Z}[\rho(q)]$-module, mais $Gal(K|k)$ n'est pas un quotient de $\rho(q)$. Donc, en vertu de 4.5.1, $F_K(J_q) = 0$. □

4.7 Un lemme pour se ramener au cas où $car(k)$ ne divise pas l'ordre de G

Dans cette partie, nous allons montrer un lemme qui nous permettra de nous ramener à un cas où la caractéristique de k ne divise pas l'ordre de G. Pour ce faire, nous devons d'abord établir quelques lemmes préliminaires.

Lemme 4.7.1. ***Existence d'un générateur***
Soit P un groupe fini qui agit sur un corps K par automorphismes. Supposons que

P agit aussi sur l'anneau $K(X)$ par $\sigma(X) = X + \lambda_\sigma$ pour $\sigma \in P$, où $\lambda_\sigma \in K$. Alors il existe $Q \in K[X]^P$ tel que $K(K(X)^P) = K(Q)$.

Preuve. Montrons d'abord que le corps des fractions L de $K[X]^P$ est $K(X)^P$. Soit $R/S \in K(X)^P$, avec $R, S \in K[X]$. Montrons que $R/S \in L$ par récurence sur $degR + degS$. Si $degR = 0$ ou si $degS = 0$, le résultat est évident. Supposons donc $degR > 0$ et $degS > 0$. On suppose de plus que R et S sont premiers entre eux et que $degR \geq degS$. Pour $\sigma \in P$, $\sigma(R)$ et $\sigma(S)$ sont premiers entre eux et $\sigma(R)/\sigma(S) = R/S$, donc il existe $\chi(\sigma) \in K^*$ tel que $\sigma(R) = \chi(\sigma)R$ et $\sigma(S) = \chi(\sigma)S$. Il est alors clair que χ est un caractère $P \to K^*$. Écrivons la division euclidienne de R par S: $R = SU + V$, avec $degV < degR$. Alors, pour $\sigma \in P$, on a $\chi(\sigma)R = \chi(\sigma)S\sigma(U) + \sigma(V)$, et donc par unicité du quotient et du reste, $\sigma(U) = U$. Par hypothèse de récurrence, $V/S \in L$ et on conclut alors que $R/S = U + V/S \in L$. Le corps des fractions de $K[X]^P$ est donc bien $K(X)^P$.
Nous avons ainsi montré que, si $K[X]^P \subseteq K$, alors $K(X)^P \subseteq K$. Le lemme est donc évident lorsque $K[X]^P \subseteq K$. Supposons donc que $K[X]^P \nsubseteq K$. Soit alors $Q \in K[X]^P - K$ de degré minimal. Montrons à présent que $K[X]^P = K^P[Q]$. Soit $R \in K[X]^P$. Montrons que $R \in K^P[Q]$ par récurrence sur $degR$. Écrivons la division euclidienne de R par Q: $R = QU + V$, $degV < degQ$. Pour $\sigma \in P$, $R = Q\sigma(U) + \sigma(V)$. Donc $\sigma(U) = U$ et $\sigma(V) = V$. Par minimalité du degré de Q, $V \in K^P$. Par hypothèse de récurrence, $U \in K^P[Q]$. Par conséquent, $R = QU + V \in K^P[Q]$. Donc $K[X]^P = K^P[Q]$. □

Le lemme que nous venons de montrer ne servira que dans la preuve du lemme suivant, qui lui jouera un rôle important dans la suite:

Lemme 4.7.2. ***Existence de d générateurs***
Soit une suite de corps $K_0 \subseteq K_1 \subseteq ... \subseteq K_d$, tous de caractéristique $p \neq 0$, et tels que, pour tout i, il existe $x_i \in K_i$ tel que $K_i = K_{i-1}(x_i)$. Soit P un p-groupe fini de K_0-automorphismes de corps de K_d tel que, pour tout $1 \leq i \leq d$ et tout $\sigma \in P$, $\sigma(x_i) - x_i \in K_{i-1}$. Alors il existe $y_1, ..., y_d$ dans K_d tels que $K_d^P = K_0(y_1, ..., y_d)$.

Preuve. On procède par récurrence sur d. Pour $d = 0$, l'énoncé est trivial. Soit $d > 0$. Supposons d'abord que x_d est transcendant sur K_{d-1}. Par hypothèse de récurrence, $K_{d-1}^P = K_0(y_1, ..., y_{d-1})$ avec $y_i \in K_{d-1}$. D'après le lemme précédent, on peut trouver $y_d \in K_d^P$ tel que $K_{d-1}(K_d^P) = K_{d-1}(y_d)$. Alors $K_d^P = (K_{d-1}(K_d^P))^P = K_{d-1}(y_d)^P = K_{d-1}^P(y_d) = K_0(y_1, ..., y_d)$.
Supposons maintenant que x_d est algébrique sur K_{d-1}. Soit Q son polynôme minimal. Alors $K_d \cong K_{d-1}[X]/(Q)$. Pour $\sigma \in P$, soit $\lambda_\sigma \in K_{d-1}$ tel que $\sigma(x_d) - x_d = \lambda_\sigma$. On peut alors faire agir P sur $K_{d-1}(X)$ par $\sigma(X) = X + \lambda_\sigma$. Comme avant, on trouve $y_1, ..., y_{d-1}, y'_d \in K_{d-1}(X)$ tels que $K_{d-1}(X)^P = K_0(y_1, ..., y_{d-1}, y'_d)$. Soit alors y_d la classe de y'_d dans K_d. Alors $K_d^P = K_0(y_1, ..., y_d)$. □

Finalement, nous aurons aussi besoin du petit lemme suivant:

Lemme 4.7.3. ***Existence d'un point fixe***
Soient K un corps de caractéristique $p \neq 0$ et P un p-groupe fini. Considérons M un $K[P]$-module non nul. Alors $M^P \neq 0$.

Preuve. Soit $m \in M$, non nul. Soit le sous-groupe $N = \sum_{g \in P}(gm)\mathbb{Z}$. Le groupe P agit sur N, qui est un $\mathbb{F}_p$-espace vectoriel non nul de dimension finie. Comme P est un p-groupe, $Card(N^P) \equiv Card(N) \pmod p$, donc p divise $Card(N^P)$. Par conséquent, N^P n'est pas trivial, donc $M^P \neq 0$. □

Supposons que k est de caractéristique non nulle. Notons $car(k) = p$. À l'aide de la classification des groupes abéliens de type fini, nous pouvons écrire $G = P \times H$ où P est un p-Sylow de G. Nous pouvons alors énoncer la proposition suivante:

Proposition 4.7.4. ***Un lemme pour éviter les problèmes de caractéristique***
Le corps k_G est k-isomorphe à une extension transcendante pure de k_H.

Preuve. Considérons V le sous-k-espace vectoriel de $k(V) = k(\{x_g, g \in G\})$ engendré par les x_g, pour $g \in G$. L'espace vectoriel V, vu comme un $k[G]$-module, est isomorphe à $k[G]$. On regarde le sous-espace W fixe par P (i.e. $W = V^P$), c'est un $k[H]$-module isomorphe à $k[H]$. On peut ainsi reformuler l'énoncé à montrer: $k(V)^G$ est une extension transcendante pure de $k(W)^H$, où $k(W)$ désigne le corps engendré par k et W dans $k(V)$. La codimension de W dans V est égale à $d = |G| - |H|$.
On note U le $k(W)$-espace vectoriel engendré par V dans $k(V)$, alors $dim_{k(W)}U = d+1$, $1 \in U$, et H agit de façon sémi-linéaire sur U. On note $T = U^H$. Alors par le lemme 4.4.1, T est un $k(W)^H$-espace vectoriel de dimension $d+1$ contenant 1. Remarquons que T est un $k(W)^H[P]$-module car $\sigma T = T$ pour tout $\sigma \in P$. On note $Y_0 = k(W)^H.1$ et on veut trouver une suite $(Y_i)_{0 \leq i \leq d}$ de $k(W)^H[P]$-sous-modules de T telle que les $k(W)^H(Y_i)$ vérifient les conditions du lemme 4.7.2. Pour ce faire, on construit successivement les Y_i de telle sorte que $Y_{i-1} \subseteq Y_i$ et Y_i/Y_{i-1} est un $k(W)^H$-espace vectoriel de dimension 1 sur lequel P agit trivialement: il suffit d'appliquer le lemme précédent à $M = T/Y_{i-1}$ pour trouver Y_i. On a $Y_d = T$ pour des raisons de dimension.
Soit $u_i \in Y_{i-1}$ tel que $Y_i = Y_{i-1} + k(W)^H u_i$ pour $1 \leq i \leq d$. On note ensuite K_i le corps engendré par $k(W)^H$ et Y_i, pour $0 \leq i \leq d$. On a $K_0 = k(W)^H$, et montrons que $K_d = k(V)^H$. En effet, remarquons d'abord que $K_d = k(W)^H(T) = k(W)^H(U^H)$, donc $K_d \subseteq k(V)^H$. Avec 4.4.1, soit $(b_0, ..., b_d)$ une base du $k(W)$-espace vectoriel U fixée par H. Alors $(b_0, ..., b_d)$ est une base du $k(W)^H$-espace vectoriel U^H d'où $K_d = k(W)^H(b_0, ..., b_d)$. On a aussi $k(V) = k(W)(U) =$

$k(W)(b_0, ..., b_d)$. On a donc le diagramme:

$$\begin{tikzcd}
 & k(V) & \\
K_d \arrow[ur] & & k(W) \arrow[ul] \\
 & k(W)^H \arrow[ul] \arrow[ur, "Galoisienne, |H|"'] &
\end{tikzcd}$$

Avec le théorème de l'élément primitif, prenons z tel que $k(W) = k(W)^H(z)$. Alors $k(V) = K_d(z)$ et donc $[K(V) : K_d] \leq |H|$. Comme $[k(V) : k(V)^H] = |H|$, on a bien $K_d = k(V)^H$. Par le lemme 4.7.2, $K_d^P = K_0(z_1, \ldots, z_d)$, pour certains $z_1, \ldots, z_d \in K_d$. Or $k(V)^G = (k(V)^H)^P = k(W)^H(z_1, \ldots, z_d)$. En plus, le degré de transcendance de $k(V)^G$ (resp. $k(W)^H$) sur k est le même que celui de $k(V)$ (resp. $k(W)$) sur k, donc le degré de transcendance de $k(V)^G$ sur $k(W)^H$ est égal à $|G| - |H| = d$. Or $K_d^P = K_0(z_1, \ldots, z_d)$, donc $z_1, \ldots, z_d$ sont algébriquement indépendants, et on a montré que $k(V)^G$ est une extension transcendante pure de $k(W)^H$, d'où le théorème. □

4.8 Preuve du théorème de Lenstra

On écrit $G = P \times H$ comme dans la section précédente. On note e l'exposant de H et on considère le corps $l = k(\zeta_e)$ ainsi que le groupe de Galois $\pi = Gal(l/k)$. Par la réduction au-dessus, on s'intéresse d'abord au groupe H.
On considère alors le groupe dual $D = Hom(H, l^*)$ de H, qui est lui aussi un groupe abélien isomorphe à H. On voit D comme un π-module en définissant l'action par $(\sigma d)(g) = \sigma(d(g))$ pour $\sigma \in \pi$, $d \in P$ et $g \in H$. On définit ensuite un module de permutation $\mathbb{Z}^D$ qui en tant que groupe abélien libre est engendré par les éléments $(e_d)_{d \in D}$ sur $\mathbb{Z}$ et tel que $\sigma e_d = e_{\sigma d}$, pour $\sigma \in \pi$ et $d \in D$. On a alors une suite exacte $0 \to J \to \mathbb{Z}^D \to D \to 0$, où $J = Ker(\mathbb{Z}^D \underset{e_d \mapsto d}{\longrightarrow} D)$.

Proposition 4.8.1. ***Un premier isomorphisme***
On a $k_H \cong l(J)^\pi$ sur $k = l^\pi$.

Preuve. On définit $l(x) = l(\{x_g | g \in H\})$ et $k(x) = k(\{x_g | g \in H\})$. La méthode consiste à montrer que $l_H \cong l(J)$, puis descendre à k.
On s'intéresse donc à $l_H = l(x)^H$. On note, pour tout $d \in D$, l'expression $y_d = (\sum_{g \in H} d(g)^{-1} \cdot x_g) \in l(x)$. Cette transformation est inversible, donc $l(x) = l(\{y_d | d \in D\})$, et on vérifie facilement que l'action de H sur $l(\{y_d\})$ est donnée par $g(y_d) = d(g) \cdot y_d$ ($\forall g \in H$, $d \in D$). On note $F \subset l(x)^*$ le sous-groupe multiplicatif engendré

par les $(y_d)_{d\in D}$. Alors F est libre et de rang $|D| = |H|$. On définit le morphisme $\phi : F \to D$ qui envoie y_d sur d, et on vérifie la relation: $g(y) = \phi(y)(g) \cdot y$ pour tout $y \in F$ et $g \in H$.
On a $l(ker(\phi)) \subset l_H \subset l(x) = l(F)$. En effet, si $y \in ker(\phi)$, alors $g(y) = y$ pour tout $y \in H$, i.e. $y \in l_H$. En plus, comme l'indice de $ker(\phi)$ dans F est égal à $|D|$, et alors $[l(F) : l(ker(\phi))] \leq |D|$ (en effet, considérons une base de $l(F)$ sur $l(ker(\phi))$ contenue dans une $\mathbb{Z}$-base de F; si son cardinal est plus grand que $|D|$, alors il existe deux élément qui sont dans la même classe, ce qui n'est pas possible). Mais on a aussi $[l(F) : l_H] = |D|$ par la théorie de Galois, ce qui montre que $l(ker(\phi)) = l_H$. Comme en plus une $\mathbb{Z}$-base de $ker(\phi)$ est algébriquement indépendante sur l, $l(ker(\phi))$ est le corps des fractions de $l[ker(\phi)]$.
On a décrit l_H, et maintenant on peut s'intéresser à k. L'action de π sur l induit une action sur $l(x) \cong l \otimes_k k(x)$. On vérifie que l'action de π et l'action de H sur $l(x)$ commutent. On en déduit que $k_H = (l(x)^\pi)^H = (l(x)^H)^\pi = (l_H)^\pi$. Un calcul montre que $\sigma(y_d) = y_{\sigma d}$ pour $\sigma \in \pi$ et $d \in D$, ce qui montre que $F \cong \mathbb{Z}^D$ en tant que sous-π-module de $l(x)^*$. Comme l'application $\phi : F \to D$ est π-linéaire, on a $ker(\phi) \cong J$, et alors on a $l_H = l(ker(\phi)) \cong l(J)$ sur l. Cet isomorphisme est bien compatible avec l'action de π, donc il induit un isomorphisme $k_H = (l_H)^\pi \cong l(J)^\pi$ sur $k = l^\pi$, et c'est bien ce que l'on cherchait à montrer. □

Il est temps de faire intervenir les modules I_q et J_q définis avant. On écrit l'isomorphisme de groupes

$$H \cong \underset{q}{\oplus}(\mathbb{Z}/q\mathbb{Z})^{n(q)}$$

où q décrit les puissances (distinctes de 1) des nombres premiers. Distinguons des cas selon la parité de q et la cyclicité de $\rho(q)$: définissons les π-modules I_1, I_2, I_3 par

$$I_1 = \bigoplus_{q \ impair} J_q^{n(q)}$$

$$I_2 = \bigoplus_{\rho(q) \ non \ cyclique} I_q^{n(q)}$$

$$I_3 = \bigoplus_{q \ pair, \ \rho(q) \ cyclique} J_q^{n(q)}$$

On note $I = I_1 \oplus I_2$. Dans la suite, nous trouverons des conditions pour que $I = I_1$.

Proposition 4.8.2. ***Un deuxième isomorphisme***
$l(J)^\pi$ est l^π-isomorphe à une extension transcendante pure de $l(I)^\pi$.

Preuve. On décompose $H \cong D = \underset{q}{\oplus}(\mathbb{Z}/q\mathbb{Z})^{n(q)}$, chaque composante étant munie d'une struture de π-module définie dans la partie 4.6. On adoptera les notations

et résultats déjà introduits dans la partie 4.6.
On dit qu'un ensemble E est un π-ensemble si π agit sur E comme un groupe de permutations (on n'exige pas que cette action soit fidèle). Soit q une puissance d'un nombre premier. Distinguons alors les deux cas suivants:
• Cas 1: $\rho(q)$ est non cyclique.
Considérons une application injective $\mathbb{Z}/q\mathbb{Z} \to D$ qui identifie $\mathbb{Z}/q\mathbb{Z}$ à un facteur de D. Elle est π-linéaire, elle induit donc une injection de π-ensembles $C(q) \subset \mathbb{Z}/q\mathbb{Z} \to D$, et on peut alors définir une application π-linéaire $\mathbb{Z}^{C(q)} \to \mathbb{Z}^D$. On a donc le diagramme suivant, et on vérifie facilement qu'il est commutatif:

$$\begin{tikzcd}
0 \arrow[r] & I_q \arrow[r] & \mathbb{Z}^{C(q)} \arrow[r] \arrow[d] & \mathbb{Z}/q\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J \arrow[r] & \mathbb{Z}^D \arrow[r] & D \arrow[r] & 0
\end{tikzcd}$$

• Cas 2: $\rho(q)$ est cyclique.
Considérons une application injective $\mathbb{Z}/q\mathbb{Z} \to D$ qui identifie $\mathbb{Z}/q\mathbb{Z}$ à un facteur de D. Elle est π-linéaire, elle induit donc une injection de π-ensembles $\rho(q) \underset{\varphi_q}{\to} (\mathbb{Z}/q\mathbb{Z})^* \subset \mathbb{Z}/q\mathbb{Z} \to D$, et on peut alors définir une application π-linéaire $\mathbb{Z}^{C(q)} \to \mathbb{Z}^D$. On a donc le diagramme suivant, et on vérifie facilement qu'il est commutatif:

$$\begin{tikzcd}
0 \arrow[r] & J_q \arrow[r] & \mathbb{Z}[\rho(q)] \arrow[r, "\varphi_q"] \arrow[d] & \mathbb{Z}/q\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J \arrow[r] & \mathbb{Z}^D \arrow[r] & D \arrow[r] & 0
\end{tikzcd}$$

• Finalement, en combinant ces deux diagrammes, on obtient le diagramme commutatif suivant:

$$\begin{tikzcd}
0 \arrow[r] & I_1 \oplus I_2 \oplus I_3 \arrow[r] & \mathbb{Z}^E \arrow[r] \arrow[d] & \bigoplus_q (\mathbb{Z}/q\mathbb{Z})^{n(q)} \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & J \arrow[r] & \mathbb{Z}^D \arrow[r] & D \arrow[r] & 0
\end{tikzcd}$$

E désigne ici un π-ensemble qui est en fait une réunion disjointe de $C(q)$ et $\rho(q)$ avec certaines multiplicités. On veut voir E comme un sous-π-ensemble de D, il faut donc vérifier que les images de $C(q)$ et $\rho(q)$ ne superposent pas dans D. C'est effectivment le cas car $0 \notin C(q) \subset \mathbb{Z}/q\mathbb{Z}$ et $0 \notin \varphi_q[\rho(q)] \subset \mathbb{Z}/q\mathbb{Z}$. Ainsi l'injection $\mathbb{Z}^E \to \mathbb{Z}^D$ admet un co-noyau N qui est un module de permutation sur π. On obtient alors facilement une suite exacte de π-modules:

$$0 \to I \oplus I_3 \to J \to N \to 0$$

où N est un module de permutation. On applique le lemme 4.4.4, et $l(J)^\pi$ est donc isomorphe à une extension transcendante pure de $l(I \oplus I_3)^\pi$. Mais $l(I \oplus I_3)^\pi$ est une extension transcendante pure de $l(I)^\pi$ d'après le lemme 4.6.4. D'où la proposition. □

Proposition 4.8.3. ***Une extension transcendante pure***
k_G est k-isomorphe à une extension transcendante pure de $l(I)^\pi$.

Preuve. Immédiat à l'aide de 4.7.4, 4.8.1 et 4.8.2. □

Proposition 4.8.4. ***Cohomologie de I***
Pour tout sous-groupe $\pi' \subset \pi$ on a $H^1(\pi', I) = 0$.

Preuve. La preuve suit immédiatement des lemmes 4.6.1, 4.6.2 et de la définition de I. □

Proposition 4.8.5. ***Lien entre $F_K(I_1)$ et $\mathfrak{a}_K(G)$***
Soit K un corps intermédiaire entre k et l (i.e. $k \subset K \subset l$) tel que $\rho_K = Gal(K/k)$ est cyclique. Alors $F_K(I_1)$ est $\mathbb{Z}(\rho_K)$-libre ssi l'idéal $\mathfrak{a}_K(G)$ de $\mathbb{Z}(\rho_K)$ est principal.

Preuve. Pour obtenir ce résultat, on utilisera essentiellement un lemme sur les anneaux de Dedekind, facilement obtenu en utilisant par exemple la classification des modules sur un anneau de Dedekind.
Soient $\alpha_1, \ldots, \alpha_n$ des idéaux non nuls d'un anneau de Dedekind, alors leur somme directe est libre (sur cet anneau de Dedekind) ssi leur produit est un idéal principal. En effet, il suffit de voir que $\alpha_1 \oplus \cdots \oplus \alpha_n$ est isomorphe à la somme directe d'un module libre de rang $n-1$ et de $\alpha_1 ... \alpha_n$ d'après le lemme 2.1.10. À l'aide de la classification des modules de type fini sur un anneau de Dedekind, on déduit que $\alpha_1 \oplus \cdots \oplus \alpha_n$ est libre si, et seulement si, $\alpha_1 ... \alpha_n$ est libre, i.e principal.
Le reste de cette démonstration suit du lemme 4.6.7 qui met en relation entre F_K et $\mathfrak{a}_K$. En effet, $F_K(I_1)$ est somme directe de certains $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ par le lemme 4.6.7, et $\mathfrak{a}_K(A)$ est, par définition, le produit de ces mêmes $\mathbb{Z}(\rho_K)$-idéaux. Comme $\mathbb{Z}(\rho_K)$ est un anneau de Dedekind, la proposition découle immédiatement. □

Maintenant on est en mesure de reformuler la condition (i) dans l'énoncé du théorème principal.

Proposition 4.8.6. ***Équivalents de (i) du théorème de Lenstra***
Les assertions suivantes sont équivalentes:
(a) Le corps $l(I_1)^\pi$ est une extension transcendante pure de l^π.
(b) Il existe une extension transcendante pure L de $l(I_1)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.
(c) La condition (i) du théorème de Lenstra est vérifiée.

Preuve. D'après le lemme 4.6.2, les hypothèses pour pouvoir appliquer le lemme 4.5.6 à $I_1 = M$ sont satisfaites. Il suffit donc de voir que 4.5.6(iii) est équivalente à (c). Or cela est une conséquence immédiate de 4.8.5. □

Maintenant il ne reste qu'à combiner tous les résultats pour démontrer le théorème de Lenstra. Pour nous débarrasser de I_2, nous nous intéresserons à $\widehat{H}^{-1}$.

Preuve. **Preuve du théorème de Lenstra**
Supposons d'abord que les conditions du théorème soient satisfaites. Alors $I = I_1$, et alors k_G est isomorphe à une extension transcendante pure de $l(I)^\pi$ sur l^π par la proposition 4.8.3, mais $l(I)^\pi$ est une extension transcendante pure de l^π par la proposition précédente. Donc k_G est une extension transcendante pure de k.
Réciproquement, si k_G est une extension transcendante pure de l^π, alors d'après 4.8.3 il existe une extension transcendante pure L de $l(I)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π en vertu de l'isomorphisme $k_G \cong l^\pi$ sur l^π. Nous pouvons appliquer le lemme 4.4.6 au I grâce lemme 4.8.4, ce qui montre l'existence de deux π-modules de permutation N_1 et N_2 (de type fini) tels que $I \oplus N_1 \cong N_2$. L'étude de la cohomologie $\widehat{H}^{-1}$ faite dans les lemmes 4.3.2 et 4.6.1 permet d'établir que $n(q) = 0$ dès que $\rho(q)$ n'est pas cyclique, ce qui montre la condition (ii) du théorème. On a donc $I \cong I_1$, et la proposition précédente nous permet de conclure que (i) est aussi satisfaite. □

De la preuve du théorème de Lenstra découle l'intéressante remarque suivante:

Remarque 4.8.7. *Soit G un groupe abélien fini. Si k_G admet une extension transcendante pure de degré de transcendance fini et qui est aussi transcendante pure sur k, alors $k_G|k$ est transcendante pure.*

5 Quelques conséquences lorsque le groupe est cyclique

Dans cette partie, on supposera que le groupe G est cyclique. Le théorème de la partie précédente se réécrit alors de la manière suivante:

Théorème 5.0.8. ***Théorème de Lenstra dans le cas cyclique***
Soit n l'ordre de G. Notons V l'ensemble des $k(\zeta_{p^s})$ avec p premier distinct de $car(k)$, s entier strictement positif, et $p^s|n$. Alors $k_G|k$ est transcendante pure si, et seulement si, pour tout $K \in V$, les conditions suivantes sont vérifiées:

(i) L'extension $K|k$ est cyclique.

(ii) Si σ_K est un générateur de $Gal(K|k)$, l'idéal $I_{k,K} = \prod(p, \zeta_{[K:k]} - t_p)$ de $\mathbb{Z}[\zeta_{[K:k]}]$ est principal, où le produit est pris sur les couples (p, s) tels que p premier distinct de $car(k)$, s entier strictement positif, $p^s|n$ et $K = k(\zeta_{p^s})$ et où t_p est tel que $\sigma_K(\zeta_p) = \zeta_p^{t_p}$.

Nous en déduisons le corollaire:

Corollaire 5.0.9. ***Les cas*** $k = \mathbb{R}$ ***et*** $k = \mathbb{C}$
Supposons que $k = \mathbb{R}$ ou $\mathbb{C}$. Alors $k_G|k$ est transcendante pure.

Preuve. Si $k = \mathbb{C}$, $V = \{\mathbb{C}\}$, donc pour tout $K \in V$, $K|\mathbb{C}$ est cyclique et $\mathbb{Z}[\zeta_{[K:\mathbb{C}]}] = \mathbb{Z}$ est un anneau principal, d'où le résultat.
Si $k = \mathbb{R}$, $V = \{\mathbb{R}, \mathbb{C}\}$, donc pour tout $K \in V$, $K|\mathbb{R}$ est cyclique et $\mathbb{Z}[\zeta_{[K:\mathbb{C}]}] = \mathbb{Z}$ est un anneau principal, d'où le résultat. □

Remarque 5.0.10. *On peut montrer directement ce résultat. Se référer à [Len80] (partie 2).*

Nous allons à partir de maintenant étudier le cas du corps des rationnels:

Corollaire 5.0.11. ***Le cas*** $n = 8$
$\mathbb{Q}(x_1, ..., x_8)^{\mathbb{Z}/8\mathbb{Z}}$ *n'est pas une extension transcendante pure de $\mathbb{Q}$.*

Preuve. Dans le cas $n = 8$ et $k = \mathbb{Q}$, $\mathbb{Q}(\zeta_8)$ est dans V. Mais $Gal(\mathbb{Q}(\zeta_8)|\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ n'est pas cyclique. Donc $\mathbb{Q}_G|\mathbb{Q}$ n'est pas transcendante pure. □

Remarque 5.0.12. *De même, lorsque $k = \mathbb{Q}$, dès que n est multiple de 8, $\mathbb{Q}_G|\mathbb{Q}$ n'est pas transcendante pure.*

Le théorème suivant permet de ramener l'étude d'une extension de corps à l'étude des idéaux dans un anneau de Dedekind:

Théorème 5.0.13. ***Le cas rationnel***
Soit n l'ordre de G. Les trois propositions suivantes sont équivalentes:

(i) $\mathbb{Q}_G|\mathbb{Q}$ est trancendante pure.

(ii) Pour tout corps k, $k_G|k$ est transcendante pure.

(iii) n n'est pas multiple de 8 et pour tout nombre premier p et tout entier strictement positif s tel que n est multiple de p^s mais pas de p^{s+1}, l'anneau $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ a un idéal principal de norme p.

Preuve. Supposons (i). Avec la remarque 5.0.12, il est clair que n n'est pas multiple de 8. De plus, l'idéal $I_{\mathbb{Q},\mathbb{Q}(\zeta_{p^s})} = (p, \zeta_{(p-1)p^{s-1}} - t_p)$ de $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ est principal de norme p, d'où (iii).
Supposons (iii). Soient p et s comme décrits dans (iii). Soit $K = k(\zeta_{p^r})$ pour $r \leq s$. On sait que 8 ne divise pas n, donc $Gal(K|k)$ s'injecte dans le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$. Donc $K|k$ est une extension cyclique. Soit $\mathfrak{p}$ un idéal principal de $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ de norme p. Il est clair que $[K : k]$ divise $(p-1)p^{s-1}$, et donc, en prenant la norme de $\mathfrak{p}$ par rapport à $\mathbb{Z}[\zeta_{[K:k]}]$, on obtient un idéal principal $\mathfrak{q}$ de $\mathbb{Z}[\zeta_{[K:k]}]$ de norme p. Comme tous les idéaux de norme p de $\mathbb{Z}[\zeta_{[K:k]}]$ sont conjugués par l'action du groupe de Galois, ils sont tous principaux, donc $I_{k,K}$ est un produit d'idéaux principaux, donc principal. Donc, d'après le théorème 5.0.8, la propriété (ii) est prouvée. □

Remarque 5.0.14. *C'est ici que l'on voit clairement le lien entre le théorème de Lenstra et le contre-exemple de Swan. En effet, dans la propriété "47 est un nombre magique" (3.3.2), Swan prouve que $\mathbb{Z}[\zeta_{46}]$ ne contient pas d'idéal principal de norme 47. Il prouve donc exactement que le (iii) du théorème précédent n'est pas vérifié lorsque $n = 47$.*

Nous pouvons maintenant déduire:

Corollaire 5.0.15. ***Une simplification***
Soit n l'ordre de G. Écrivons sa décomposition en produit de facteurs premiers: $n = \prod_p p^{s_p}$. Alors $\mathbb{Q}_G|\mathbb{Q}$ est transcendante pure si, et seulement si, pour tout nombre premier p, $\mathbb{Q}_{(\mathbb{Z}/p^{s_p}\mathbb{Z})}|\mathbb{Q}$ l'est.

Preuve. Il suffit d'appliquer l'équivalence $(i) \Leftrightarrow (iii)$ du théorème précédent. □

Il suffit donc de s'intéresser au cas où l'ordre de G est une puissance d'un nombre premier.

Corollaire 5.0.16. ***Une condition suffisante pour que l'extension soit transcendante pure***
Supposons que l'ordre de G divise $2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71$ pour un certain entier naturel m. Alors $k_G|k$ est transcendante pure.

Preuve. En tenant compte des résultats précédents, il suffit de voir que pour $p^s = 2, 3^m, 4, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 49, 61, 67, 71$, il existe $\alpha \in \mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ de norme p. On vérifie par le calcul que les α suivants conviennent, avec $\zeta = \zeta_{(p-1)p^{s-1}}$:

p^s	α
2	2
3^m	$1-\zeta^2$
4	2
5	$\zeta^2+\zeta-1$
7	$\zeta^3-\zeta-1$
11	$\zeta^3+\zeta^2-1$
13	$\zeta^4-\zeta-1$
17	$\zeta^3-\zeta^2-1$
19	$\zeta^4+\zeta+1$
23	$\zeta^5-\zeta^3+1$
25	$\zeta^5-\zeta^3+1$
29	$\zeta^5-\zeta^2+1$
31	$\zeta^3+\zeta+1$
37	$\zeta^5+\zeta^2+1$
41	$\zeta^8-\zeta^5+1$
43	$\zeta^6+\zeta-1$
49	$\zeta^4-\zeta-1$
61	$\zeta^6-\zeta-1$
67	$\zeta^6+\zeta+1$
71	$\zeta^7-\zeta^3+1$

Par exemple, pour $p^s = 5$, la norme de $\zeta^2+\zeta-1$ est le déterminant de $\begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix}$ c'est-à-dire 5. □

Le corollaire suivant permet de traiter le cas où l'ordre de G est une puissance d'un nombre premier sans être un nombre premier:

Corollaire 5.0.17. ***Une condition nécessaire et suffisante dans un cas particulier***
Soient p un nombre premier et $s \geq 2$ un entier. Soit $G = \mathbb{Z}/p^s\mathbb{Z}$. Alors $\mathbb{Q}_G|\mathbb{Q}$ est transcendante pure si, et seulement si,

$$p^s \in \left\{2^2, 3^m, 5^2, 7^2 : m \geq 2\right\}$$

Preuve. La réciproque a déjà été montrée. La propriété directe découle immédiatement du lemme suivant et de 5.0.13. □

Lemme 5.0.18. ***Éléments de norme*** p

(i) Soit $p \geq 5$ un nombre premier. Alors $\mathbb{Z}[\zeta_{(p-1)p^2}]$ n'a pas d'élément de norme p.

(ii) Soit $p \geq 11$ un nombre premier. Alors $\mathbb{Z}[\zeta_{(p-1)p}]$ n'a pas d'élément de norme p.

Nous admettrons ce lemme dont la démonstration est indépendante de ce qui a été fait jusqu'ici. Elle se trouve dans [Len80] (lemme 5).
À ce stade, afin de résoudre le problème de Noether dans le cas d'un groupe cyclique, il ne nous reste plus qu'à étudier le cas où $G = \mathbb{Z}/p\mathbb{Z}$ avec p premier. Nous savons que la réponse est affirmative lorsque p est 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71. Avec le contre-exemple de Swan, nous savons aussi que la réponse est négative lorsque $p = 47$. En fait, la preuve de Swan marche aussi de la même manière pour $p = 113$ et pour $p = 233$, ce qui prouve que pour ces nombres premiers le problème de Noether admet aussi une réponse négative. Il y a aussi des nombres premiers pour lesquels le problème est toujours ouvert: c'est par exemple le cas de 53, 59 ou 73. Essayons d'expliquer pourquoi dans ces cas-là, malgré les résultats de Swan et de Lenstra, le problème reste ouvert. D'une part, le raisonnement de Swan tombe en défaut pour ces trois valeurs. En effet, à l'exception de la proposition 3.3.2, toute la preuve de Swan reste valable pour 53, 59 et 73 au lieu de 47. Mais ces trois nombres-là ne sont pas magiques comme 47. Pour 53, on a $\mathbb{Q}(\sqrt{13}) \subset \mathbb{Q}(\zeta_{52})$, et donc par le raisonnement de Swan, il faut résoudre l'équation $x^2 - 13y^2 = 4 \cdot 53$ dans les entiers avec $x \equiv y(mod 2)$. Mais $(678, 188)$ est bien solution de cette équation et donc on n'arrive pas à une contradiction comme dans le cas 47. De même, pour 59 et 73, on obtient les équations $x^2 - 29y^2 = 4 \cdot 59$ et $x^2 + 3y^2 = 4 \cdot 73$, qui ont pour solutions respectives $(56, 10)$ et $(10, 8)$. D'autre part, le théorème de Lenstra permet de se ramener à la recherche d'un idéal principal de norme 53, 59 et 73 respectivement dans $\mathbb{Z}[\zeta_{52}]$, $\mathbb{Z}[\zeta_{58}]$ et $\mathbb{Z}[\zeta_{72}]$, mais ce nouveau problème n'est pas simple. Même si le problème reste toujours ouvert, on peut au moins se demander s'il y a beaucoup de nombres premiers pour lesquels $\mathbb{Q}_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de $\mathbb{Q}$. Dans [Len74] (corollaire 7.6), Lenstra a montré le théorème suivant:

Théorème 5.0.19. ***Il y a peu de nombres premiers pour lesquels l'extension est transcendante pure***
Pour $x \in \mathbb{R}$, soit $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x, et soit $\pi^*(x)$ le nombre de nombres premiers $p \leq x$ tels que $\mathbb{Q}_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de $\mathbb{Q}$. Alors

$$\frac{\pi^*(x)}{\pi(x)} \to 0$$

Plus précisément,

$$\frac{\pi^*(x)}{\pi(x)} = O((\log\log\log x)^{-1/2})$$

Pour clore cette partie, nous pouvons faire la jolie petite remarque suivante:

Remarque 5.0.20. ***Le cas*** $k = \mathbb{F}_2$
Prenons $k = \mathbb{F}_2$. Si p est un nombre premier de Mersenne ou de Fermat, alors $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k.

Preuve. Soit $p = 2^q - 1$ un nombre premier de Mersenne. Alors $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2] = q$. Comme $Gal(\mathbb{F}_{2^q}|\mathbb{F}_2)$ est cyclique engendré par le morphisme de Frobenius, on a $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (p, \zeta_q - 2)$. Or $\phi_q(2) = 2^p - 1 \in (\zeta_q - 2)$, donc $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (\zeta_q - 2)$ est principal. Donc $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k, pour $k = \mathbb{F}_2$.
Soit maintenant $p = 2^{2^n} + 1$ un nombre premier de Fermat. Alors $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2] = [\mathbb{F}_2(\zeta_{2^{2^{n+1}}-1}) : \mathbb{F}_2] = 2^{n+1}$. Comme $Gal(\mathbb{F}_{2^{2^{n+1}}}|\mathbb{F}_2)$ est cyclique engendré par le morphisme de Frobenius, on a $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (p, \zeta_{2^{n+1}} - 2)$. Or $\phi_{2^{n+1}}(2) = 2^{2^n} + 1 \in (\zeta_{2^{n+1}} - 2)$, donc $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (\zeta_{2^{n+1}} - 2)$ est principal. Donc $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k, pour $k = \mathbb{F}_2$. $\square$

Références

[Art55] Emil Artin. The orders of the linear groups. *Comm. Pure Appl. Math.*, 8:355–365, 1955.

[CF667] *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London, 1967.

[EM73] Shizuo Endô and Takehiko Miyata. Invariants of finite abelian groups. *J. Math. Soc. Japan*, 25:7–26, 1973.

[Fis15] E. Fischer. Die isomorphie der invariantenkörper der endlichen abelschen gruppen linearer transformationen. *Nachr. Königl. Ges. Wiss., Göttingen*, 1915.

[Ker75] Michel Kervaire. Fractions rationnelles invariantes (d'après H. W. Lenstra). In *Séminaire Bourbaki, Vol. 1973/1974, 26ème année, Exp. No. 445*, pages 170–189. Lecture Notes in Math., Vol. 431. Springer, Berlin, 1975.

[Kun56] Hideo Kuniyoshi. Certain subfields of rational function fields. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 241–243, Tokyo, 1956. Science Council of Japan.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Len74] H. W. Lenstra, Jr. Rational functions invariant under a finite abelian group. *Invent. Math.*, 25:299–325, 1974.

[Len80] H. W. Lenstra, Jr. Rational functions invariant under a cyclic group. In *Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979)*, volume 54 of *Queen's Papers in Pure and Appl. Math.*, pages 91–99, Kingston, Ont., 1980. Queen's Univ.

[Mar71] Jacques Martinet. Un contre-exemple à une conjecture d'E. Noether d'après R. Swan. In *Séminaire Bourbaki, Vol. 1969/1970, 22ème année, Exp. No. 372*, pages 145–154. Lecture Notes in Math., Vol. 180. Springer, Berlin, 1971.

[Mas55] Katsuhiko Masuda. On a problem of Chevalley. *Nagoya Math. J.*, 8:59–63, 1955.

[Mas68] Katsuhiko Masuda. Application of the theory of the group of classes of projective modules to the existance problem of independent parameters of invariant. *J. Math. Soc. Japan*, 20:223–232, 1968.

[Mat64] Ryuuki Matsuda. On purely-transcendency of certain fields. *Tôhoku Math. J. (2)*, 16:189–202, 1964.

[Mil08] J.S. Milne. Class field theory, 2008.

[Miy71] Takehiko Miyata. Invariants of Certain Groups. *I. Nagaya Math.*, 41:69–73, 1971.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Swa69] Richard G. Swan. Invariant rational functions and a problem of Steenrod. *Invent. Math.*, 7:148–158, 1969.