# Dénombrement des extensions d'une algèbre centrale simple sur un corps de nombres

Béranger Seguin, Université de Paderborn (Allemagne)
Tous les résultats sont obtenus avec Fabian Gundlach
**arXiv:** 2405.17286

Journées Galoisiennes, Caen
16 décembre 2024

# Une question classique : le dénombrement des extensions de corps

# Une question classique : le dénombrement des extensions de corps

$K$ un corps de nombres, $n \geq 2$.

$\mathcal{N}_n(K, X)$ = nombre d'extensions $L|K$ avec $[L : K] = n$ et $\|\mathrm{Disc}(L|K)\| \leq X$

# Une question classique : le dénombrement des extensions de corps

$K$ un corps de nombres, $n \geq 2$.

$\mathcal{N}_n(K, X)$ = nombre d'extensions $L|K$ avec $[L : K] = n$ et $\|\mathrm{Disc}(L|K)\| \leq X$

**Conjecture**

$\mathcal{N}_n(K, X) \sim C \cdot X$ pour un réel $C > 0$

# Une question classique : le dénombrement des extensions de corps

$K$ un corps de nombres, $n \geq 2$.

$\mathcal{N}_n(K, X)$ = nombre d'extensions $L|K$ avec $[L : K] = n$ et $\|\mathrm{Disc}(L|K)\| \leq X$

**Conjecture**

$\mathcal{N}_n(K, X) \sim C \cdot X$ pour un réel $C > 0$

Connu pour :

- $n = 2$ (trivial sur $\mathbb{Q}$, Datskovsky-Wright '88)
- $n = 3$ (Davenport-Heilbronn '69, Datskovsky-Wright '88)
- $n = 4, 5$ (Bhargava '05-'10, Bhargava-Shankar-Wang '15)

# Une question classique : le dénombrement des extensions de corps

$K$ un corps de nombres, $n \geq 2$.

$\mathcal{N}_n(K, X)$ = nombre d'extensions $L|K$ avec $[L : K] = n$ et $\|\mathrm{Disc}(L|K)\| \leq X$

**Conjecture**

$\mathcal{N}_n(K, X) \sim C \cdot X$ pour un réel $C > 0$

Connu pour :

- $n = 2$ (trivial sur $\mathbb{Q}$, Datskovsky-Wright '88)
- $n = 3$ (Davenport-Heilbronn '69, Datskovsky-Wright '88)
- $n = 4, 5$ (Bhargava '05-'10, Bhargava-Shankar-Wang '15)

Pour $n$ général, on est loin :

$$\mathcal{N}_n(\mathbb{Q}, X) = O(X^{c(\log n)^2}). \qquad \text{(Lemke Oliver-Thorne '20)}$$

# Variantes de la question

# Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)

## Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)
- Fixer le groupe de Galois $G = \mathrm{Aut}(L|K)$ :
  - pour $G$ abélien : Wright '89

## Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)
- Fixer le groupe de Galois $G = \mathrm{Aut}(L|K)$ :
  - pour $G$ abélien : Wright '89
  - en général : conjecture de Malle '02 (problème inverse de Galois "quantitatif")

## Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)
- Fixer le groupe de Galois $G = \mathrm{Aut}(L|K)$ :
  - pour $G$ abélien : Wright '89
  - en général : conjecture de Malle '02 (problème inverse de Galois "quantitatif")
- Autres corps de base $K$ :
  - $\mathbb{F}_q(T)$ (cas modéré) : borne supérieure par Ellenberg-Tran-Westerland '23

## Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)
- Fixer le groupe de Galois $G = \mathrm{Aut}(L|K)$ :
  - pour $G$ abélien : Wright '89
  - en général : conjecture de Malle '02 (problème inverse de Galois "quantitatif")
- Autres corps de base $K$ :
  - $\mathbb{F}_q(T)$ (cas modéré) : borne supérieure par Ellenberg-Tran-Westerland '23
  - cas local avec ramification sauvage : Serre '78 (formule de masse), Lagemann '10, Klüners-Müller '20, Potthast '24, Gundlach '24

## Variantes de la question

- Autres invariants à la place du discriminant (ex: produit des premiers ramifiés)
- Fixer le groupe de Galois $G = \mathrm{Aut}(L|K)$ :
  - pour $G$ abélien : Wright '89
  - en général : conjecture de Malle '02 (problème inverse de Galois "quantitatif")
- Autres corps de base $K$ :
  - $\mathbb{F}_q(T)$ (cas modéré) : borne supérieure par Ellenberg-Tran-Westerland '23
  - cas local avec ramification sauvage : Serre '78 (formule de masse), Lagemann '10, Klüners-Müller '20, Potthast '24, Gundlach '24

**Programme du jour**

Résoudre des questions analogues pour les corps non-commutatifs.

(cf. travaux de Deschamps-Legrand sur le problème inverse de Galois non-commutatif)

# Théorie de Galois non-commutative

# Théorie de Galois non-commutative

Une extension $L|K$ de corps non-commutatifs est *galoisienne* si $K = L^{\mathrm{Aut}(L|K)}$.

# Théorie de Galois non-commutative

Une extension $L|K$ de corps non-commutatifs est *galoisienne* si $K = L^{\mathrm{Aut}(L|K)}$.

On a une correspondance de Galois, etc.

# Théorie de Galois non-commutative

Une extension $L|K$ de corps non-commutatifs est *galoisienne* si $K = L^{\mathrm{Aut}(L|K)}$.

On a une correspondance de Galois, etc.

Deux types opposés d'extensions en lesquels toute extension se décompose :

- $L|K$ est *intérieure* si tout automorphisme de $L|K$ provient de la conjugaison par un élément de $L^\times$.
  **Propriété :** $L|K$ est galoisienne et intérieure $\iff$ $Z(L) \subseteq Z(K)$.

# Théorie de Galois non-commutative

Une extension $L|K$ de corps non-commutatifs est *galoisienne* si $K = L^{\mathrm{Aut}(L|K)}$.

On a une correspondance de Galois, etc.

Deux types opposés d'extensions en lesquels toute extension se décompose :

- $L|K$ est *intérieure* si tout automorphisme de $L|K$ provient de la conjugaison par un élément de $L^\times$.
  **Propriété :** $L|K$ est galoisienne et intérieure $\iff$ $Z(L) \subseteq Z(K)$.
- $L|K$ est *extérieure* si tout élément de $L$ qui commute avec tout élément de $K$ est dans le centre de $L$
  $$\mathrm{Cent}_L(K) = Z(L)$$
  (autrement dit, tous les automorphismes intérieurs sont triviaux)

# Théorie de Galois non-commutative

Une extension $L|K$ de corps non-commutatifs est *galoisienne* si $K = L^{\mathrm{Aut}(L|K)}$.

On a une correspondance de Galois, etc.

Deux types opposés d'extensions en lesquels toute extension se décompose :

- $L|K$ est *intérieure* si tout automorphisme de $L|K$ provient de la conjugaison par un élément de $L^\times$.
  **Propriété :** $L|K$ est galoisienne et intérieure $\iff$ $Z(L) \subseteq Z(K)$.
- $L|K$ est *extérieure* si tout élément de $L$ qui commute avec tout élément de $K$ est dans le centre de $L$
  $$\mathrm{Cent}_L(K) = Z(L)$$
  (autrement dit, tous les automorphismes intérieurs sont triviaux)

Plus généralement : *algèbres simples* au lieu des corps non-commutatifs.

# Paramétrisation des $\mathbb{Q}$-algèbres simples

## Théorème (groupe de Brauer d'un corps de nombres)

Une algèbre simple $K$ de dimension finie sur $\mathbb{Q}$ est déterminée par :

- un corps de nombres $F$ (son centre)
- un entier $m \geq 1$ (tel que $\dim_F K = m^2$)
- pour chaque place $v$ de $F$, un élément $\kappa_v$ de $\mathbb{Z}/m\mathbb{Z}$

# Paramétrisation des $\mathbb{Q}$-algèbres simples

## Théorème (groupe de Brauer d'un corps de nombres)

Une algèbre simple $K$ de dimension finie sur $\mathbb{Q}$ est déterminée par :

- un corps de nombres $F$ (son centre)
- un entier $m \geq 1$ (tel que $\dim_F K = m^2$)
- pour chaque place $v$ de $F$, un élément $\kappa_v$ de $\mathbb{Z}/m\mathbb{Z}$

tels que :

- $\kappa_v = 0$ pour presque tout $v$, dont toutes les places complexes
- $\kappa_v \in \{0, \frac{m}{2}\}$ si $v$ est une place réelle
- $\sum_v \kappa_v = 0$

## Théorème (groupe de Brauer d'un corps de nombres)

Une algèbre simple $K$ de dimension finie sur $\mathbb{Q}$ est déterminée par :

- un corps de nombres $F$ (son centre)
- un entier $m \geq 1$ (tel que $\dim_F K = m^2$)
- pour chaque place $v$ de $F$, un élément $\kappa_v$ de $\mathbb{Z}/m\mathbb{Z}$

tels que :

- $\kappa_v = 0$ pour presque tout $v$, dont toutes les places complexes
- $\kappa_v \in \{0, \frac{m}{2}\}$ si $v$ est une place réelle
- $\sum_v \kappa_v = 0$

$K$ est un corps non-commutatif $\iff$ les éléments $\kappa_v$ engendrent $\mathbb{Z}/m\mathbb{Z}$

## Première question : les extensions galoisiennes intérieures

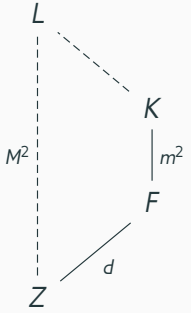
On fixe une $\mathbb{Q}$-algèbre simple $K$. On note comme précédemment $F = Z(K)$, $\dim_F K = m^2$ et $\kappa_v \in \mathbb{Z}/m\mathbb{Z}$ les invariants locaux de $K$.

# Première question : les extensions galoisiennes intérieures

On fixe une $\mathbb{Q}$-algèbre simple $K$. On note comme précédemment $F = Z(K)$, $\dim_F K = m^2$ et $\kappa_v \in \mathbb{Z}/m\mathbb{Z}$ les invariants locaux de $K$.

On fixe:

- un sous-corps $Z \subseteq F$ et un entier $M$
- $d = [F : Z]$ et $j = \frac{M}{dm}$

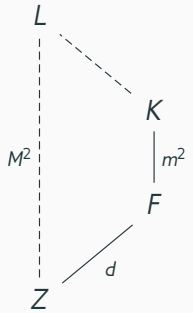


# Première question : les extensions galoisiennes intérieures

On fixe une $\mathbb{Q}$-algèbre simple $K$. On note comme précédemment $F = Z(K)$, $\dim_F K = m^2$ et $\kappa_v \in \mathbb{Z}/m\mathbb{Z}$ les invariants locaux de $K$.

On fixe:

- un sous-corps $Z \subseteq F$ et un entier $M$
- $d = [F : Z]$ et $j = \frac{M}{dm}$




**Question**

Combien y a-t-il d'extensions $L|K$ telles que $Z(L) = Z$, $\dim_Z L = M^2$, et $\mathrm{Disc}(L|Z) \leq X$, pour $X$ "grand" ?

($j$ doit être entier pour qu'une telle extension existe)

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$

$\iff$ choisir un ensemble fini $S$ de places de $\mathbb{Q}$

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$
$\iff$ choisir un ensemble fini $S$ de places de $\mathbb{Q}$

- "$\sum \lambda(v) = 0$" dit que $|S|$ est pair. On choisit plutôt $S' = \{p \text{ premier} \in S\}$
  $\rightsquigarrow$ la parité de $|S'|$ détermine si $\infty \in S$ ou non.

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$
$\iff$ choisir un ensemble fini $S$ de places de $\mathbb{Q}$

- "$\sum \lambda(v) = 0$" dit que $|S|$ est pair. On choisit plutôt $S' = \{p \text{ premier} \in S\}$
  $\rightsquigarrow$ la parité de $|S'|$ détermine si $\infty \in S$ ou non.
- Le discriminant est $\prod_{p \in S'} p^2$.

# Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$
$\iff$ choisir un ensemble fini $S$ de places de $\mathbb{Q}$

- "$\sum \lambda(v) = 0$" dit que $|S|$ est pair. On choisit plutôt $S' = \{p \text{ premier} \in S\}$
  $\rightsquigarrow$ la parité de $|S'|$ détermine si $\infty \in S$ ou non.
- Le discriminant est $\prod_{p \in S'} p^2$.

$\rightsquigarrow$ les discriminants des algèbres de quaternions sur $\mathbb{Q}$ sont exactement les carrés d'entiers sans facteurs carrés, et ceux-ci déterminent uniquement l'algèbre associée.

## Exemple-jouet : compter les algèbres de quaternions sur $\mathbb{Q}$

Le cas $K = F = Z = \mathbb{Q}$ et $M = 2$ ($\rightsquigarrow m = d = 1$, $\kappa_v = 0$, $j = 2$, $G = \mathbb{Z}/2\mathbb{Z}$)

en chaque place $v$ de $\mathbb{Q}$, choisir un invariant $\lambda(v) \in \{0, 1\}$
$\iff$ choisir un ensemble fini $S$ de places de $\mathbb{Q}$

- "$\sum \lambda(v) = 0$" dit que $|S|$ est pair. On choisit plutôt $S' = \{p \text{ premier} \in S\}$
  $\rightsquigarrow$ la parité de $|S'|$ détermine si $\infty \in S$ ou non.
- Le discriminant est $\prod_{p \in S'} p^2$.

$\rightsquigarrow$ les discriminants des algèbres de quaternions sur $\mathbb{Q}$ sont exactement les carrés d'entiers sans facteurs carrés, et ceux-ci déterminent uniquement l'algèbre associée.

$\rightsquigarrow$ autant d'algèbres de quaternions sur $\mathbb{Q}$ de discriminant $\leq X$ que d'entiers sans facteurs carrés inférieurs à $\sqrt{X}$, c'est-à-dire :

$$\sim \frac{6}{\pi^2}\sqrt{X}$$

# Reformulation combinatoire, 1/2

On note $\lambda$ une fonction qui associe à chaque place $v$ de $Z$ un élément $\lambda(v) \in \mathbb{Z}/M\mathbb{Z}$. On la suppose nulle presque partout, etc.

C'est notre "inconnue" : $\lambda(v)$ représente l'invariant local de $L$ en $v$.

**But :** compter les fonctions $\lambda$ correspondant aux extensions qu'on veut compter.

# Reformulation combinatoire, 1/2

On note $\lambda$ une fonction qui associe à chaque place $v$ de $Z$ un élément $\lambda(v) \in \mathbb{Z}/M\mathbb{Z}$. On la suppose nulle presque partout, etc.

C'est notre "inconnue" : $\lambda(v)$ représente l'invariant local de $L$ en $v$.

**But :** compter les fonctions $\lambda$ correspondant aux extensions qu'on veut compter.

La condition $\mathrm{Disc}(L|Z) \leq X$ se reformule :

$$\prod_{p \text{ premier de } Z} \|p\|^{M(M-\gcd(M,\lambda(p)))} \leq X.$$

# Reformulation combinatoire, 1/2

On note $\lambda$ une fonction qui associe à chaque place $v$ de $Z$ un élément $\lambda(v) \in \mathbb{Z}/M\mathbb{Z}$. On la suppose nulle presque partout, etc.

C'est notre "inconnue" : $\lambda(v)$ représente l'invariant local de $L$ en $v$.

**But :** compter les fonctions $\lambda$ correspondant aux extensions qu'on veut compter.

La condition $\mathrm{Disc}(L|Z) \leq X$ se reformule :

$$\prod_{p \text{ premier de } Z} \|p\|^{M(M-\gcd(M,\lambda(p)))} \leq X.$$

Reste à s'assurer que $L$ est bien une extension de $K$, i.e., que $K$ se plonge dans $L$...

# Reformulation combinatoire, 2/2

La condition que $L$ soit une extension de $K$ se reformule :

$$dm \mid d_w \lambda(v) - \underbrace{dj\kappa_w}_{\text{nul pour presque tous les } v}$$

pour chaque place $v$ de $Z$ et chaque place $w$ de $F$ au-dessus de $v$, où $d_w = [F_w : Z_v]$.

# Reformulation combinatoire, 2/2

La condition que $L$ soit une extension de $K$ se reformule :

$$dm \mid d_w \lambda(v) - \underbrace{d j \kappa_w}_{\text{nul pour presque tous les } v}$$

pour chaque place $v$ de $Z$ et chaque place $w$ de $F$ au-dessus de $v$, où $d_w = [F_w : Z_v]$.

Pour presque tous les $v$ (on ignore les autres), la contrainte sur $\lambda(v)$ est qu'il soit divisible par $\frac{dm}{d_w}$ pour tout $w|v$.

# Reformulation combinatoire, 2/2

La condition que $L$ soit une extension de $K$ se reformule :

$$dm \mid d_w \lambda(v) - \underbrace{dj\kappa_w}_{\text{nul pour presque tous les } v}$$

pour chaque place $v$ de $Z$ et chaque place $w$ de $F$ au-dessus de $v$, où $d_w = [F_w : Z_v]$.

Pour presque tous les $v$ (on ignore les autres), la contrainte sur $\lambda(v)$ est qu'il soit divisible par $\frac{dm}{d_w}$ pour tout $w|v$ , i.e., divisible par $\frac{dm}{\gcd_{w|v} d_w}$.

On a une reformulation combinatoire du problème. Comment compter ?

# Un outil puissant : les théorèmes taubériens

# Un outil puissant : les théorèmes taubériens

Soit un ensemble $O$ d'objets et, pour chaque objet $o \in O$, un invariant $d(o)$ de cet objet. Supposons qu'on veuille compter les objets $o \in O$ tels que $d(o) \leq X$.

# Un outil puissant : les théorèmes taubériens

Soit un ensemble $O$ d'objets et, pour chaque objet $o \in O$, un invariant $d(o)$ de cet objet. Supposons qu'on veuille compter les objets $o \in O$ tels que $d(o) \leq X$.

Le **théorème taubérien de Delange** permet d'obtenir des résultats de la forme

$$|\{o \in O \mid d(o) \leq X\}| \sim C \cdot X^{1/a} \cdot (\log X)^{b-1}$$

# Un outil puissant : les théorèmes taubériens

Soit un ensemble $O$ d'objets et, pour chaque objet $o \in O$, un invariant $d(o)$ de cet objet. Supposons qu'on veuille compter les objets $o \in O$ tels que $d(o) \leq X$.

Le **théorème taubérien de Delange** permet d'obtenir des résultats de la forme

$$|\{o \in O \mid d(o) \leq X\}| \sim C \cdot X^{1/a} \cdot (\log X)^{b-1}$$

en montrant que la fonction de la variable complexe :

$$f(s) = \sum_{o \in O} d(o)^{-s}$$

a, pour pôle le plus "à droite", un unique pôle d'ordre $b$ en $s = a$.

# La série de Dirichlet

Suivant la méthode, on pose:

$$f(s) = \sum_{\lambda} \prod_{p \text{ premier de } Z} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les fonctions $\lambda$ satisfaisant les conditions vues précédemment.

# La série de Dirichlet

Suivant la méthode, on pose:

$$f(s) = \sum_{\lambda} \prod_{p \text{ premier de } Z} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les fonctions $\lambda$ satisfaisant les conditions vues précédemment.

**Caractères de** $\mathbb{Z}/M\mathbb{Z}$**:** on peut ignorer la condition $\sum_v \lambda(v) = 0$ (il y a équidistribution de la somme modulo $M \rightsquigarrow$ on trouvera $M$ fois trop de fonctions $\lambda$).

# La série de Dirichlet

Suivant la méthode, on pose:

$$f(s) = \sum_{\lambda} \prod_{p \text{ premier de } Z} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les fonctions $\lambda$ satisfaisant les conditions vues précédemment.

**Caractères de $\mathbb{Z}/M\mathbb{Z}$:** on peut ignorer la condition $\sum_v \lambda(v) = 0$ (il y a équidistribution de la somme modulo $M \rightsquigarrow$ on trouvera $M$ fois trop de fonctions $\lambda$).

Toutes les autres conditions sont **locales**. On écrit:

$$f(s) \approx \prod_{p \text{ premier de } Z} \underbrace{\sum_{\lambda(p)} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}}_{\text{noté } f_p(s)}$$

où la somme porte sur les $\lambda(p) \in \mathbb{Z}/M\mathbb{Z}$ satisfaisant les contraintes locales en $p$.

# Analyse locale des facteurs de la série de Dirichlet 1/2

Soit un premier $p$ de $Z$ "générique" (non-ramifié dans $F$, et $\kappa_q = 0$ pour tout $q|p$).

On étudie le facteur :

$$f_p(s) = \sum_{\lambda(p)} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les $\lambda(p) \in \mathbb{Z}/M\mathbb{Z}$ divisibles par $\frac{dm}{\gcd_{q|p} d_q}$.

# Analyse locale des facteurs de la série de Dirichlet 1/2

Soit un premier $p$ de $Z$ "générique" (non-ramifié dans $F$, et $\kappa_q = 0$ pour tout $q|p$).

On étudie le facteur :

$$f_p(s) = \sum_{\lambda(p)} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les $\lambda(p) \in \mathbb{Z}/M\mathbb{Z}$ divisibles par $\frac{dm}{\gcd_{q|p} d_q}$.

On regroupe les termes selon $g = \gcd(M, \lambda(p))$ :

$$f_p(s) = \sum_{\frac{dm}{\gcd_{q|p} d_q} | g | M} \varphi\left(\frac{M}{g}\right) \cdot \|p\|^{-sM(M-g)}$$

# Analyse locale des facteurs de la série de Dirichlet 1/2

Soit un premier $p$ de $Z$ "générique" (non-ramifié dans $F$, et $\kappa_q = 0$ pour tout $q|p$).

On étudie le facteur :

$$f_p(s) = \sum_{\lambda(p)} \|p\|^{-sM(M-\gcd(M,\lambda(p)))}$$

où la somme porte sur les $\lambda(p) \in \mathbb{Z}/M\mathbb{Z}$ divisibles par $\frac{dm}{\gcd_{q|p} d_q}$.

On regroupe les termes selon $g = \gcd(M, \lambda(p))$ :

$$f_p(s) = \sum_{\frac{dm}{\gcd_{q|p} d_q} | g | M} \varphi\left(\frac{M}{g}\right) \cdot \|p\|^{-sM(M-g)}$$

On fait le changement de variable $g' = \frac{M}{g}$, et on isole le terme $g' = 1$ :

$$f_p(s) = 1 + \sum_{1 < g' \mid j \cdot \gcd_{q|p} d_q} \varphi(g') \cdot \|p\|^{-sM(M-\frac{M}{g'})}.$$

# Analyse locale des facteurs de la série de Dirichlet 2/2

Nous sommes arrivés à l'expression suivante, qu'on cherche à estimer :

$$f_p(s) = 1 + \sum_{1 < g' \mid j \cdot \gcd_{q \mid p} d_q} \varphi(g') \cdot \|p\|^{-sM\left(M - \frac{M}{g'}\right)}.$$

# Analyse locale des facteurs de la série de Dirichlet 2/2

Nous sommes arrivés à l'expression suivante, qu'on cherche à estimer :

$$f_p(s) = 1 + \sum_{1 < g' \mid j \cdot \gcd_{q \mid p} d_q} \varphi(g') \cdot \|p\|^{-sM(M - \frac{M}{g'})}.$$

Le terme principal après 1 provient du plus petit $g'$ dans la somme, c'est-à-dire le plus petit diviseur premier $\alpha(p)$ de $j \cdot \gcd_{q \mid p} d_q$ (s'il existe !) :

$$f_p(s) \approx 1 + (\alpha(p) - 1) \cdot \|p\|^{-sM(M - \frac{M}{\alpha(p)})}.$$

# Analyse locale des facteurs de la série de Dirichlet 2/2

Nous sommes arrivés à l'expression suivante, qu'on cherche à estimer :

$$f_p(s) = 1 + \sum_{1 < g' \mid j \cdot \gcd_{q \mid p} d_q} \varphi(g') \cdot \|p\|^{-sM(M - \frac{M}{g'})}.$$

Le terme principal après 1 provient du plus petit $g'$ dans la somme, c'est-à-dire le plus petit diviseur premier $\alpha(p)$ de $j \cdot \gcd_{q \mid p} d_q$ (s'il existe !) :

$$f_p(s) \approx 1 + (\alpha(p) - 1) \cdot \|p\|^{-sM(M - \frac{M}{\alpha(p)})}.$$

**Question**

Quelle est la distribution, pour divers premiers $p$, de la valeur de l'entier $\alpha(p)$ ?

## Interprétation de $\alpha(p)$

Soit $\widehat{F}$ la clôture galoisienne de $F|Z$, et $G = \mathrm{Gal}(\widehat{F}|Z)$.

$G$ agit transitivement sur les $d = [F : Z]$ plongements $F \hookrightarrow \widehat{F}$
$\rightsquigarrow G \subseteq \mathfrak{S}_d$

## Interprétation de $\alpha(p)$

Soit $\widehat{F}$ la clôture galoisienne de $F|Z$, et $G = \mathrm{Gal}(\widehat{F}|Z)$.

$G$ agit transitivement sur les $d = [F : Z]$ plongements $F \hookrightarrow \widehat{F}$
$\rightsquigarrow G \subseteq \mathfrak{S}_d$

Si $\sigma$ est une permutation, on note $\mathrm{cycgcd}(\sigma)$ le pgcd des tailles de ses cycles.

# Interprétation de $\alpha(p)$

Soit $\widehat{F}$ la clôture galoisienne de $F|Z$, et $G = \mathrm{Gal}(\widehat{F}|Z)$.

$G$ agit transitivement sur les $d = [F : Z]$ plongements $F \hookrightarrow \widehat{F}$
$\rightsquigarrow G \subseteq \mathfrak{S}_d$

Si $\sigma$ est une permutation, on note $\mathrm{cycgcd}(\sigma)$ le pgcd des tailles de ses cycles.

**Fait**

$\mathrm{gcd}_{q|p}\, d_q = \mathrm{cycgcd}(\mathrm{Frob}(p))$

## Interprétation de $\alpha(p)$

Soit $\widehat{F}$ la clôture galoisienne de $F|Z$, et $G = \mathrm{Gal}(\widehat{F}|Z)$.

$G$ agit transitivement sur les $d = [F : Z]$ plongements $F \hookrightarrow \widehat{F}$
$\rightsquigarrow G \subseteq \mathfrak{S}_d$

Si $\sigma$ est une permutation, on note $\mathrm{cycgcd}(\sigma)$ le pgcd des tailles de ses cycles.

**Fait**

$\mathrm{gcd}_{q|p}\, d_q = \mathrm{cycgcd}(\mathrm{Frob}(p))$

La distribution de $\alpha(p)$ ne dépend que de la distribution des éléments $\mathrm{Frob}(p) \in G$, donnés par le **théorème de densité de Chebotarev** !

# Un théorème de Fein, Kantor et Schacher

Un dernier ingrédient :

**Théorème (Fein-Kantor-Schacher '81)**

Si $G \subseteq \mathfrak{S}_d$ est transitif et $d \geq 2$, alors il existe $g \in G$ tel que $\mathrm{cycgcd}(g) \neq 1$.

(leur preuve dépend de la classification des groupes simples finis !)

# Un théorème de Fein, Kantor et Schacher

Un dernier ingrédient :

**Théorème (Fein-Kantor-Schacher '81)**

Si $G \subseteq \mathfrak{S}_d$ est transitif et $d \geq 2$, alors il existe $g \in G$ tel que $\mathrm{cycgcd}(g) \neq 1$.

On peut alors définir :

$u$ = le plus petit nombre premier tel qu'il existe $g \in G$ avec $u \mid j \cdot \mathrm{cycgcd}(g)$

$\beta$ = proportion d'éléments $g \in G$ tels que $u \mid j \cdot \mathrm{cycgcd}(g)$

# Étude de la série de Dirichlet

$u$ = le plus petit nombre premier tel qu'il existe $g \in G$ avec $u \mid j \cdot \mathrm{cycgcd}(g)$

$\beta$ = proportion d'éléments $g \in G$ tels que $u \mid j \cdot \mathrm{cycgcd}(g)$

# Étude de la série de Dirichlet

$u$ = le plus petit nombre premier tel qu'il existe $g \in G$ avec $u \mid j \cdot \mathrm{cycgcd}(g)$

$\beta$ = proportion d'éléments $g \in G$ tels que $u \mid j \cdot \mathrm{cycgcd}(g)$

En un premier $p$ tel que $u \mid j \cdot \mathrm{cycgcd}(\mathrm{Frob}(p))$, on a $\alpha(p) = u$ et donc :

$$f_p(s) \approx 1 + (u-1) \cdot \|p\|^{-sM(M-\frac{M}{u})}.$$

# Étude de la série de Dirichlet

$u$ = le plus petit nombre premier tel qu'il existe $g \in G$ avec $u \mid j \cdot \mathrm{cycgcd}(g)$

$\beta$ = proportion d'éléments $g \in G$ tels que $u \mid j \cdot \mathrm{cycgcd}(g)$

En un premier $p$ tel que $u \mid j \cdot \mathrm{cycgcd}(\mathrm{Frob}(p))$, on a $\alpha(p) = u$ et donc :

$$f_p(s) \approx 1 + (u-1) \cdot \|p\|^{-sM(M-\frac{M}{u})}.$$

Caractères de $G$ + propriétés des fonctions $L \rightsquigarrow$ seuls ces premiers importent.
Par théorème de densité de Chebotarev, leur proportion est $\beta$, d'où l'approximation (en répartissant les termes non nuls sur tous les nombres premiers) :

$$f(s) \approx \prod_p 1 + \beta \cdot (u-1) \cdot \|p\|^{-sM(M-\frac{M}{u})}$$

# Étude de la série de Dirichlet

$u$ = le plus petit nombre premier tel qu'il existe $g \in G$ avec $u \mid j \cdot \mathrm{cycgcd}(g)$

$\beta$ = proportion d'éléments $g \in G$ tels que $u \mid j \cdot \mathrm{cycgcd}(g)$

En un premier $p$ tel que $u \mid j \cdot \mathrm{cycgcd}(\mathrm{Frob}(p))$, on a $\alpha(p) = u$ et donc :

$$f_p(s) \approx 1 + (u-1) \cdot \|p\|^{-sM(M-\frac{M}{u})}.$$

Caractères de $G$ + propriétés des fonctions $L \rightsquigarrow$ seuls ces premiers importent.
Par théorème de densité de Chebotarev, leur proportion est $\beta$, d'où l'approximation (en répartissant les termes non nuls sur tous les nombres premiers) :

$$f(s) \approx \prod_p 1 + \beta \cdot (u-1) \cdot \|p\|^{-sM(M-\frac{M}{u})} \approx \left( \prod_p 1 - \|p\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta}$$

# Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{p} 1 - \|p\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta}$$

# Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{p} 1 - \|p\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta} \approx \zeta_Z \left( sM \left( M - \frac{M}{u} \right) \right)^{(u-1)\beta}$$

# Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{p} 1 - \|p\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta} \approx \zeta_Z\left( sM\left( M - \frac{M}{u} \right) \right)^{(u-1)\beta}$$

Par les propriétés des fonctions zêta de Dedekind, le "pôle" le plus à droite de $f$ se trouve en $\frac{1}{M\left(M-\frac{M}{u}\right)}$ et a "ordre" $(u-1)\beta$ (pas forcément entier !).

# Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{p} 1 - \|p\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta} \approx \zeta_Z\left( sM\left( M - \frac{M}{u} \right) \right)^{(u-1)\beta}$$

Par les propriétés des fonctions zêta de Dedekind, le "pôle" le plus à droite de $f$ se trouve en $\frac{1}{M\left(M-\frac{M}{u}\right)}$ et a "ordre" $(u-1)\beta$ (pas forcément entier !).
Il ne reste qu'à appliquer le théorème taubérien de Delange :

## Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{\mathfrak{p}} 1 - \|\mathfrak{p}\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta} \approx \zeta_Z\left( sM\left( M - \frac{M}{u} \right) \right)^{(u-1)\beta}$$

Par les propriétés des fonctions zêta de Dedekind, le "pôle" le plus à droite de $f$ se trouve en $\frac{1}{M\left(M-\frac{M}{u}\right)}$ et a "ordre" $(u-1)\beta$ (pas forcément entier !).
Il ne reste qu'à appliquer le théorème taubérien de Delange :

**Théorème (Gundlach, S. '24)**

Le nombre d'extensions $L|K$ avec $Z(L) = Z$, $[L : Z] = M^2$ et $\|\mathrm{Disc}(L|Z)\| \leq X$ est équivalent à

$$C \cdot X^{M\left(M-\frac{M}{u}\right)} \cdot (\log X)^{(u-1)\beta-1}$$

pour un réel $C$.

## Résultats asymptotiques

On a obtenu l'approximation :

$$f(s) \approx \left( \prod_{\mathfrak{p}} 1 - \|\mathfrak{p}\|^{-sM(M-\frac{M}{u})} \right)^{-(u-1)\beta} \approx \zeta_Z\left( sM\left( M - \frac{M}{u} \right) \right)^{(u-1)\beta}$$

Par les propriétés des fonctions zêta de Dedekind, le "pôle" le plus à droite de $f$ se trouve en $\frac{1}{M\left(M-\frac{M}{u}\right)}$ et a "ordre" $(u-1)\beta$ (pas forcément entier !).
Il ne reste qu'à appliquer le théorème taubérien de Delange :

**Théorème (Gundlach, S. '24)**

Le nombre d'extensions $L|K$ avec $Z(L) = Z$, $[L : Z] = M^2$ et $\|\mathrm{Disc}(L|Z)\| \leq X$ est équivalent à

$$C \cdot X^{M\left(M-\frac{M}{u}\right)} \cdot (\log X)^{(u-1)\beta-1}$$

pour un réel $C$. Même réponse si on ne compte que les corps non-commutatifs.

## Un mot sur les extensions extérieures

Nous avons aussi regardé les extensions extérieures $L|K$ avec groupe de Galois fixé.

## Un mot sur les extensions extérieures

Nous avons aussi regardé les extensions extérieures $L|K$ avec groupe de Galois fixé.

**Théorème (Deschamps-Legrand)**

Si $L|K$ est une extension extérieure galoisienne de groupe $G$ alors $Z(L)|Z(K)$ est une extension galoisienne de groupe $G$ et

$$L \simeq K \otimes_{Z(K)} Z(L).$$

## Un mot sur les extensions extérieures

Nous avons aussi regardé les extensions extérieures $L|K$ avec groupe de Galois fixé.

**Théorème (Deschamps-Legrand)**

Si $L|K$ est une extension extérieure galoisienne de groupe $G$ alors $Z(L)|Z(K)$ est une extension galoisienne de groupe $G$ et

$$L \simeq K \otimes_{Z(K)} Z(L).$$

Autrement dit, “tout se passe au niveau commutatif” : on sait compter les $G$-extensions $L|K$ chaque fois qu’on sait compter les $G$-extensions de $Z(K)$.

## Un mot sur les extensions extérieures

Nous avons aussi regardé les extensions extérieures $L|K$ avec groupe de Galois fixé.

**Théorème (Deschamps-Legrand)**

Si $L|K$ est une extension extérieure galoisienne de groupe $G$ alors $Z(L)|Z(K)$ est une extension galoisienne de groupe $G$ et

$$L \simeq K \otimes_{Z(K)} Z(L).$$

Autrement dit, “tout se passe au niveau commutatif” : on sait compter les $G$-extensions $L|K$ chaque fois qu’on sait compter les $G$-extensions de $Z(K)$.

Petites subtilités si on ne regarde que les corps non-commutatifs.

## Un mot sur les extensions extérieures

Nous avons aussi regardé les extensions extérieures $L|K$ avec groupe de Galois fixé.

**Théorème (Deschamps-Legrand)**

Si $L|K$ est une extension extérieure galoisienne de groupe $G$ alors $Z(L)|Z(K)$ est une extension galoisienne de groupe $G$ et

$$L \simeq K \otimes_{Z(K)} Z(L).$$

Autrement dit, "tout se passe au niveau commutatif" : on sait compter les $G$-extensions $L|K$ chaque fois qu'on sait compter les $G$-extensions de $Z(K)$.

Petites subtilités si on ne regarde que les corps non-commutatifs.

$\rightsquigarrow$ "en gros" le problème non-commutatif est équivalent à la conjecture de Malle ordinaire.

Merci pour votre attention !

Des questions ?