Étude de la répartition des automorphismes de Frobenius dans les groupes de Galois

Alexandre Bailleul
Sous la direction de Florent Jouve

Institut de Mathématiques de Bordeaux

Vendredi 27 novembre 2020

Organisation de l'exposé

1. Biais de Tchebychev : cadre historique
2. Le cas des corps de nombres
3. Le cas des corps de fonctions
4. Versions explicites du théorème de Kronecker-Weyl

Organisation de l'exposé

Le biais de Tchebychev

Tchebychev (lettre à Fuss, 1853).

« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

Le biais de Tchebychev

Tchebychev (lettre à Fuss, 1853).

« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

Autrement dit, on aurait $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand, où

$$\pi(x;q,a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

Le biais de Tchebychev

Tchebychev (lettre à Fuss, 1853).

« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

Autrement dit, on aurait $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand, où

$$\pi(x;q,a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

Tchebychev (lettre à Fuss, 1853).

« [...] à mesure que c s'approche de zéro, la valeur de la série $e^{-3c} - e^{-5c} + e^{-7c} + e^{-11c} - e^{-13c} - e^{-17c} + e^{-19c} + e^{-23c} + \dots$ s'approche de $+\infty$. »

Le biais de Tchebychev

Quelques problèmes :

Le biais de Tchebychev

Quelques problèmes :

- D'après le théorème des nombres premiers en progressions arithmétiques, $\pi(x;4,3) \underset{x\to+\infty}{\sim} \pi(x;4,1) \underset{x\to+\infty}{\sim} \frac{1}{2}\operatorname{Li}(x)$, où $\operatorname{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}$, et les termes d'erreur connus (et attendus) ont la même taille.

Le biais de Tchebychev

Quelques problèmes :

- D'après le théorème des nombres premiers en progressions arithmétiques, $\pi(x;4,3) \underset{x\to+\infty}{\sim} \pi(x;4,1) \underset{x\to+\infty}{\sim} \frac{1}{2}\operatorname{Li}(x)$, où $\operatorname{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}$, et les termes d'erreur connus (et attendus) ont la même taille.

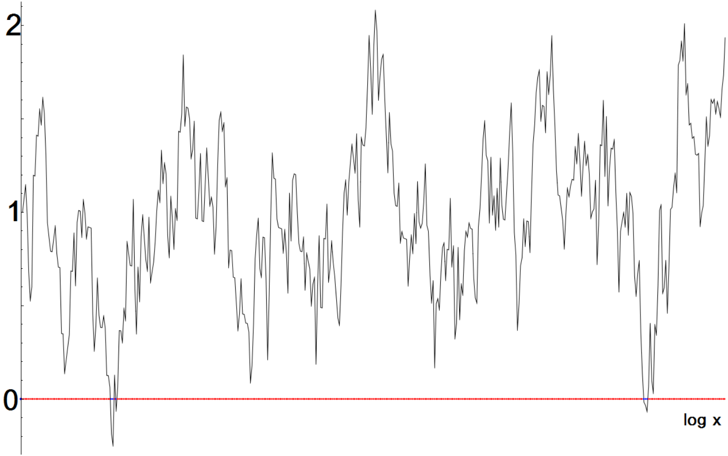
- On sait que $\pi(x;4,3) > \pi(x;4,1)$ et $\pi(x;4,3) < \pi(x;4,1)$ se produisent pour des x arbitrairement grands : $\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}(x^{1/2}\log\log\log x)$ (Littlewood, 1914).

Le biais de Tchebychev

Quelques problèmes :

- D'après le théorème des nombres premiers en progressions arithmétiques, $\pi(x;4,3) \underset{x\to+\infty}{\sim} \pi(x;4,1) \underset{x\to+\infty}{\sim} \frac{1}{2}\,\mathrm{Li}(x)$, où $\mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}$, et les termes d'erreur connus (et attendus) ont la même taille.
- On sait que $\pi(x;4,3) > \pi(x;4,1)$ et $\pi(x;4,3) < \pi(x;4,1)$ se produisent pour des x arbitrairement grands : $\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}(x^{1/2}\log\log\log x)$ (Littlewood, 1914).
- $\sum_p (-1)^{\frac{p+1}{2}} e^{-pc} \underset{c\to 0}{\longrightarrow} +\infty \Leftrightarrow$ Hypothèse de Riemann pour $L(s,\chi_4)$ (Hardy-Littlewood 1916, Landau 1918).

Le biais de Tchebychev



$$\frac{\pi(x;4,3)-\pi(x;4,1)}{\sqrt{x}/\log x}, 10^4 \leq x \leq 10^8$$

(Daniel Fiorilli)

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, qui est en tête le plus souvent ?

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{|\mathcal{P}_{4;3,1} \cap [2,X]|}{X} = 1.$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{|\mathcal{P}_{4;3,1} \cap [2,X]|}{X} = 1.$$

- **Kaczorowski, 1995 :** Si $L(s,\chi_4)$ vérifie GRH (hypothèse de Riemann généralisée), alors

$$\underline{d}(\mathcal{P}_{4;3,1}) < 0,9594595\ldots$$

et

$$\overline{d}(\mathcal{P}_{4;3,1}) > 0,999989360\ldots$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3$ mod 4 et les premiers $p \equiv 1$ mod 4, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{|\mathcal{P}_{4;3,1} \cap [2,X]|}{X} = 1.$$

- **Kaczorowski, 1995 :** Si $L(s,\chi_4)$ vérifie GRH (hypothèse de Riemann généralisée), alors

$$\underline{d}(\mathcal{P}_{4;3,1}) < 0,9594595\dots$$

et

$$\overline{d}(\mathcal{P}_{4;3,1}) > 0,999989360\dots$$

- **Rubinstein-Sarnak, 1994 :** Si $L(s,\chi_4)$ vérifie GRH et LI (indépendance linéaire),

$$\delta(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{1}{\log X} \int_2^X \mathbf{1}_{\mathcal{P}_{4;3,1}}(t) \frac{\mathrm{d}t}{t}$$

existe et $\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\dots$

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s, \chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.
- **Théorème central limite** :

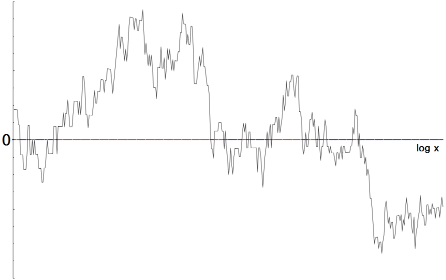
$$\max_{a,b \text{ premiers avec } q} \left|\delta(\mathcal{P}_{q;a,b}) - \frac{1}{2}\right| \underset{q\to+\infty}{\longrightarrow} 0.$$

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.
- **Théorème central limite** :

$$\max_{a,b \text{ premiers avec } q} \left| \delta(\mathcal{P}_{q;a,b}) - \frac{1}{2} \right| \underset{q \to +\infty}{\longrightarrow} 0.$$



$$\frac{\pi(x;101,3) - \pi(x;101,1)}{\sqrt{x}/\log x},$$

$$10^4 \leq x \leq 10^8$$

(Daniel Fiorilli)

La méthode de Rubinstein-Sarnak

Elle s'articule en trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

$$\frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x} = \#\sqrt{\{b\}} - \#\sqrt{\{a\}} + \sum_{\chi\in X_q} \overline{\chi(b)-\chi(a)} \sum_{\gamma_\chi} \frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{x}\right),$$

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

La méthode de Rubinstein-Sarnak

Elle s'articule en trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

$$\frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x} = \#\sqrt{\{b\}} - \#\sqrt{\{a\}} + \sum_{\chi\in X_q} \overline{\chi(b)-\chi(a)} \sum_{\gamma_\chi} \frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{x}\right),$$

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

2) Utilisation du **théorème de Kronecker-Weyl** $\Rightarrow$ existence d'une distribution limite $\mu_{q;a,b}$ (mesure de probabilité sur $\mathbb{R}$) pour $x \mapsto \frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x}$.

La méthode de Rubinstein-Sarnak

Elle s'articule en trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

$$\frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x} = \#\sqrt{\{b\}} - \#\sqrt{\{a\}} + \sum_{\chi\in X_q} \overline{\chi(b)-\chi(a)} \sum_{\gamma_\chi} \frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{x}\right),$$

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

2) Utilisation du **théorème de Kronecker-Weyl** $\Rightarrow$ existence d'une distribution limite $\mu_{q;a,b}$ (mesure de probabilité sur $\mathbb{R}$) pour $x \mapsto \frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x}$.

3) Utilisation de l'hypothèse LI pour établir la régularité de $\mu_{q;a,b}$, étudier sa fonction caractéristique et l'existence de $\delta(\mathcal{P}_{q;a,b}) = \mu_{q;a,b}(]0,+\infty[)$.

L'hypothèse LI

Théorème de Kronecker-Weyl : Si $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$ sont linéairement indépendants sur $\mathbb{Q}$ alors $x \mapsto \left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right)$ « se comporte » comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

L'hypothèse LI

Théorème de Kronecker-Weyl : Si $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$ sont linéairement indépendants sur $\mathbb{Q}$ alors $x \mapsto \left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right)$ « se comporte » comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \in X_q, L\left(\frac{1}{2} + i\gamma, \chi\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

L'hypothèse LI

Théorème de Kronecker-Weyl : Si $\gamma_1, \dots, \gamma_n \in \mathbb{R}$ sont linéairement indépendants sur $\mathbb{Q}$ alors $x \mapsto \left(e^{i\gamma_1 x}, \dots, e^{i\gamma_n x}\right)$ « se comporte » comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \in X_q, L\left(\frac{1}{2} + i\gamma, \chi\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

(Par l'équation fonctionnelle, si $L\left(\frac{1}{2} + i\gamma, \chi\right) = 0$ alors $L\left(\frac{1}{2} - i\gamma, \overline{\chi}\right) = 0$)

L'hypothèse LI

Théorème de Kronecker-Weyl : Si $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$ sont linéairement indépendants sur $\mathbb{Q}$ alors $x \mapsto \left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right)$ « se comporte » comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \in X_q, L\left(\frac{1}{2} + i\gamma, \chi\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

(Par l'équation fonctionnelle, si $L\left(\frac{1}{2} + i\gamma, \chi\right) = 0$ alors $L\left(\frac{1}{2} - i\gamma, \overline{\chi}\right) = 0$)

L'hypothèse LI permet de traiter la somme sur les zéros dans la formule explicite comme une somme de variables aléatoires **indépendantes**, uniformes sur $\mathbb{S}^1$.

Organisation de l'exposé

1. Biais de Tchebychev : cadre historique
2. **Le cas des corps de nombres**
3. Le cas des corps de fonctions
4. Versions explicites du théorème de Kronecker-Weyl

Frobenius et Chebotarev

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L, on peut associer une classe de conjugaison $\mathrm{Frob}_{\mathfrak{p}}$ de G.

Frobenius et Chebotarev

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L, on peut associer une classe de conjugaison $\mathrm{Frob}_{\mathfrak{p}}$ de G.

Pour $L = \mathbb{Q}(\zeta_q)$, $K = \mathbb{Q}$, $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ et pour $p \nmid q$, $\mathrm{Frob}_p = a \Leftrightarrow p \equiv a \bmod q$.

Frobenius et Chebotarev

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L, on peut associer une classe de conjugaison $\mathrm{Frob}_{\mathfrak{p}}$ de G.

Pour $L = \mathbb{Q}(\zeta_q)$, $K = \mathbb{Q}$, $G \simeq (\mathbb{Z}/q\mathbb{Z})^{\times}$ et pour $p \nmid q$, $\mathrm{Frob}_p = a \Leftrightarrow p \equiv a \bmod q$.

Si C_1, C_2 sont des classes de conjugaison de G, on note

$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ x \geq 2 \mid \frac{\pi(x; C_1, L/K)}{\# C_1} > \frac{\pi(x; C_2, L/K)}{\# C_2} \right\},$$

où

$$\pi(x; C, L/K) := \#\{\mathfrak{p} \mid N(\mathfrak{p}) \leq x, \mathrm{Frob}_{\mathfrak{p}} = C\} \underset{x \to +\infty}{\sim} \frac{\# C}{\# G} \mathrm{Li}(x) \quad \text{(Chebotarev)}.$$

Fonctions L d'Artin

Si $\chi \in \mathrm{Irr}(G)$, de représentation sous-jacente (ρ, V), sa fonction L d'Artin est

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \det\left(\mathrm{id}_V - \rho(\mathrm{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s}_{|V^{\mathcal{I}_{\mathfrak{p}}}}\right)^{-1}.$$

Fonctions L d'Artin

Si $\chi \in \mathrm{Irr}(G)$, de représentation sous-jacente (ρ, V), sa fonction L d'Artin est

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \det\left(\mathrm{id}_V - \rho(\mathrm{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s}_{|V^{\mathcal{I}_{\mathfrak{p}}}}\right)^{-1}.$$

Théorème (Ng, 2000).

Si les fonctions L d'Artin associées aux caractères irréductibles de G satisfont AC (conjecture d'Artin), GRH et $\tilde{\mathrm{LI}}$, alors $\delta(\mathcal{P}_{L/K;C_1,C_2})$ existe, et en l'absence de zéros en $1/2$, $\delta(\mathcal{P}_{L/K;C_1,C_2}) - 1/2$ est du signe de $\frac{\#\sqrt{C_2}}{\#C_2} - \frac{\#\sqrt{C_1}}{\#C_1}$.

Fonctions L d'Artin

Si $\chi \in \mathrm{Irr}(G)$, de représentation sous-jacente (ρ, V), sa fonction L d'Artin est

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \det\left(\mathrm{id}_V - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s}_{|V^{\mathcal{I}_{\mathfrak{p}}}}\right)^{-1}.$$

Théorème (Ng, 2000).

Si les fonctions L d'Artin associées aux caractères irréductibles de G satisfont AC (conjecture d'Artin), GRH et $\tilde{\mathsf{LI}}$, alors $\delta(\mathcal{P}_{L/K;C_1,C_2})$ existe, et en l'absence de zéros en $1/2$, $\delta(\mathcal{P}_{L/K;C_1,C_2}) - 1/2$ est du signe de $\frac{\#\sqrt{C_2}}{\#C_2} - \frac{\#\sqrt{C_1}}{\#C_1}$.

Ici, $\tilde{\mathsf{LI}}$ signifie que le (multi)-ensemble $\left\{\gamma > 0 \mid \exists \chi \in \mathrm{Irr}(G), L\left(\frac{1}{2} + i\gamma, \chi, L/K\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$ (noter le > 0 au lieu de ≥ 0).

Défauts de $\tilde{\mathsf{LI}}$

Malheureusement $\tilde{\mathsf{LI}}$ est en général fausse : les fonctions L d'Artin admettent des factorisations non triviales à cause de leurs propriétés fonctorielles.

Défauts de $\widetilde{\mathsf{LI}}$

Malheureusement $\widetilde{\mathsf{LI}}$ est en général fausse : les fonctions L d'Artin admettent des factorisations non triviales à cause de leurs propriétés fonctorielles.

Si L/F est galoisienne de groupe de Galois G', avec $F \subset K$ et $\chi \in \mathrm{Irr}(G)$ alors

$$L(s, \chi, L/K) = L\left(s, \mathrm{Ind}_G^{G'} \chi, L/F\right),$$

$$\begin{tikzcd}
L \arrow[d, dash, "G"'] \arrow[dd, dash, bend left, "G'"] \\
K \arrow[d, dash] \\
F
\end{tikzcd}$$

Défauts de $\widetilde{\mathsf{LI}}$

Malheureusement $\widetilde{\mathsf{LI}}$ est en général fausse : les fonctions L d'Artin admettent des factorisations non triviales à cause de leurs propriétés fonctorielles.

Si L/F est galoisienne de groupe de Galois G', avec $F \subset K$ et $\chi \in \mathrm{Irr}(G)$ alors

$$L(s, \chi, L/K) = L\left(s, \mathrm{Ind}_G^{G'} \chi, L/F\right),$$

$$\begin{tikzcd} L \arrow[d, dash, "G"'] \arrow[dd, dash, bend left, "G'"] \\ K \arrow[d, dash] \\ F \end{tikzcd}$$

on décompose

$$\mathrm{Ind}_G^{G'} \chi = \sum_{\lambda \in \mathrm{Irr}(G')} \langle \mathrm{Ind}_G^{G'} \chi, \lambda \rangle \lambda$$

Défauts de $\tilde{\mathsf{LI}}$

Malheureusement $\tilde{\mathsf{LI}}$ est en général fausse : les fonctions L d'Artin admettent des factorisations non triviales à cause de leurs propriétés fonctorielles.

$$\begin{array}{c} L \\ {\scriptstyle G}\big| \\ K \\ \big| \\ F \end{array} \; \Bigg) {\scriptstyle G'}$$

Si L/F est galoisienne de groupe de Galois G', avec $F \subset K$ et $\chi \in \mathrm{Irr}(G)$ alors

$$L(s,\chi,L/K) = L\left(s, \mathrm{Ind}_G^{G'} \chi, L/F\right),$$

on décompose

$$\mathrm{Ind}_G^{G'} \chi = \sum_{\lambda \in \mathrm{Irr}(G')} \langle \mathrm{Ind}_G^{G'} \chi, \lambda \rangle \lambda$$

et on obtient

$$L(s,\chi,L/K) = \prod_{\lambda \in \mathrm{Irr}(G')} L(s,\lambda,L/F)^{\langle \mathrm{Ind}_G^{G'} \chi, \lambda \rangle}.$$

Défauts de $\widetilde{\mathsf{LI}}$

Malheureusement $\widetilde{\mathsf{LI}}$ est en général fausse : les fonctions L d'Artin admettent des factorisations non triviales à cause de leurs propriétés fonctorielles.

Si L/F est galoisienne de groupe de Galois G', avec $F \subset K$ et $\chi \in \mathrm{Irr}(G)$ alors

$$L(s, \chi, L/K) = L\left(s, \mathrm{Ind}_G^{G'} \chi, L/F\right),$$

$$\begin{tikzcd} L \arrow[d, dash, "G"'] \arrow[dd, dash, bend left, "G'"] \\ K \arrow[d, dash] \\ F \end{tikzcd}$$

on décompose

$$\mathrm{Ind}_G^{G'} \chi = \sum_{\lambda \in \mathrm{Irr}(G')} \langle \mathrm{Ind}_G^{G'} \chi, \lambda \rangle \lambda$$

et on obtient

$$L(s, \chi, L/K) = \prod_{\lambda \in \mathrm{Irr}(G')} L(s, \lambda, L/F)^{\langle \mathrm{Ind}_G^{G'} \chi, \lambda \rangle}.$$

Conclusion : $L(s, \chi, L/K)$ peut admettre des zéros multiples, ou des zéros en commun avec des $L(s, \chi', L/K)$, $\chi' \neq \chi$, quand $K \neq \mathbb{Q}$.

L'hypothèse LI

On suppose $L/\mathbb{Q}$ galoisienne, de groupe de Galois G^+.

L'hypothèse LI

On suppose $L/\mathbb{Q}$ galoisienne, de groupe de Galois G^+.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma > 0 \mid \exists \chi \in \mathrm{Irr}(G^+), L\left(\frac{1}{2} + i\gamma, \chi, L/\mathbb{Q}\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

L'hypothèse LI

On suppose $L/\mathbb{Q}$ galoisienne, de groupe de Galois G^+.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma > 0 \mid \exists \chi \in \mathrm{Irr}(G^+), L\left(\frac{1}{2} + i\gamma, \chi, L/\mathbb{Q}\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

Les résultats de Ng restent valable sous l'hypothèse plus faible LI.

L'hypothèse LI

On suppose $L/\mathbb{Q}$ galoisienne, de groupe de Galois G^+.

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma > 0 \mid \exists \chi \in \mathrm{Irr}(G^+), L\left(\frac{1}{2} + i\gamma, \chi, L/\mathbb{Q}\right) = 0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

Les résultats de Ng restent valable sous l'hypothèse plus faible LI.

L'hypothèse n'exclut pas la possibilité de zéros en $1/2$ ($\gamma = 0$).

Formule explicite

Dans la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right),$$

un $\gamma_\chi=0$ contribue à l'espérance.

Formule explicite

Dans la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right),$$

un $\gamma_\chi=0$ contribue à l'espérance.

Peut-on influer sur le biais de Tchebychev à l'aide de zéros en $1/2$?

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre).

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre). Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}).$$

Si $W(\chi) = -1$ alors $L(1/2,\chi,L/K) = 0$!

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre). Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}).$$

Si $W(\chi) = -1$ alors $L(1/2,\chi,L/K) = 0$!

Si $\chi \in \mathrm{Irr}(G)$ est réel, la constante $W(\chi)$ (*root number*) ne peut être que $+1$ ou -1.

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre). Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}).$$

Si $W(\chi) = -1$ alors $L(1/2,\chi,L/K) = 0$!

Si $\chi \in \mathrm{Irr}(G)$ est réel, la constante $W(\chi)$ (*root number*) ne peut être que $+1$ ou -1. Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre). Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}).$$

Si $W(\chi) = -1$ alors $L(1/2,\chi,L/K) = 0$!

Si $\chi \in \mathrm{Irr}(G)$ est réel, la constante $W(\chi)$ (*root number*) ne peut être que $+1$ ou -1. Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

- **Fröhlich-Queyrut, 1973 :** Si χ est orthogonal, $W(\chi) = +1$.

Root number et zéros en $1/2$

Des exemples de fonctions L d'Artin s'annulant en $1/2$ sont connus (Armitage, Serre). Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}).$$

Si $W(\chi) = -1$ alors $L(1/2,\chi,L/K) = 0$!

Si $\chi \in \mathrm{Irr}(G)$ est réel, la constante $W(\chi)$ (*root number*) ne peut être que $+1$ ou -1. Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

- **Fröhlich-Queyrut, 1973 :** Si χ est orthogonal, $W(\chi) = +1$.
- Tous les exemples connus de root numbers -1, et *a fortiori* de zéros en $1/2$ correspondent à des caractères symplectiques.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q})$ se produit si et seulement si $W(\lambda) = -1$, et ça ne peut se produire que si λ est symplectique.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q})$ se produit si et seulement si $W(\lambda) = -1$, et ça ne peut se produire que si λ est symplectique.

Sous LI^+, on veut utiliser des groupes de Galois possédant beaucoup de caractères symplectiques pour avoir une influence non négligeable de zéros en $1/2$.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q})$ se produit si et seulement si $W(\lambda) = -1$, et ça ne peut se produire que si λ est symplectique.

Sous LI^+, on veut utiliser des groupes de Galois possédant beaucoup de caractères symplectiques pour avoir une influence non négligeable de zéros en $1/2$.

Les groupes

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$$

possèdent 2^n éléments, $2^{n-2} + 3$ caractères irréductibles et 2^{n-3} caractères symplectiques.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q})$ se produit si et seulement si $W(\lambda) = -1$, et ça ne peut se produire que si λ est symplectique.

Sous LI^+, on veut utiliser des groupes de Galois possédant beaucoup de caractères symplectiques pour avoir une influence non négligeable de zéros en $1/2$.

Les groupes

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$$

possèdent 2^n éléments, $2^{n-2} + 3$ caractères irréductibles et 2^{n-3} caractères symplectiques. De plus, $-1 := x^{2^{n-2}}$ a $2^{n-1} + 1$ racines carrées et 1 n'en a que 2.

Biais extrêmes opposés

Théorème (B. , 2019).

Sous GRH et LI^+ pour les fonctions L d'Artin qui interviennent, il existe deux familles $(\mathcal{Q}_n^+)_{n\geq 3}$ et $(\mathcal{Q}_n^-)_{n\geq 3}$ d'extensions galoisiennes de $\mathbb{Q}$ telles que $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q}) \simeq \mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q}) \simeq \mathbb{H}_{2^n}$ et

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < 1 - \delta(\mathcal{P}_{\mathcal{Q}_n^+/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right)$$

et

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < \delta(\mathcal{P}_{\mathcal{Q}_n^-;1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

Biais extrêmes opposés

Théorème (B. , 2019).

Sous GRH et LI^+ pour les fonctions L d'Artin qui interviennent, il existe deux familles $(\mathcal{Q}_n^+)_{n\geq 3}$ et $(\mathcal{Q}_n^-)_{n\geq 3}$ d'extensions galoisiennes de $\mathbb{Q}$ telles que $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q}) \simeq \mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q}) \simeq \mathbb{H}_{2^n}$ et

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < 1 - \delta(\mathcal{P}_{\mathcal{Q}_n^+/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right)$$

et

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < \delta(\mathcal{P}_{\mathcal{Q}_n^-;1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

Remarque : Le groupe $\mathcal{D}_{2^{n-1}}$ a la même table de caractères que $\mathbb{H}_{2^n}$, mais uniquement des caractères orthogonaux, donc un tel phénomène ne peut se produire pour de tels groupes de Galois !

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée :

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée : on va construire $(\mathcal{Q}_n^{\pm})_{n\geq 3}$ modérément ramifiés sur $\mathbb{Q}$ telles que $W_{\mathcal{Q}_n^+} = +1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q})$ et $W_{\mathcal{Q}_n^-} = -1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q})$.

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée : on va construire $(\mathcal{Q}_n^{\pm})_{n\geq 3}$ modérément ramifiés sur $\mathbb{Q}$ telles que $W_{\mathcal{Q}_n^+} = +1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q})$ et $W_{\mathcal{Q}_n^-} = -1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q})$.

- La théorie de Fröhlich permet de construire de telles extensions $K/\mathbb{Q}$ à root numbers et ramification prescrits. Le choix de W_K devient alors une propriété « de type Chebotarev » pour un nombre premier qui sera (presque) le seul ramifié dans l'extension.

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée : on va construire $(\mathcal{Q}_n^{\pm})_{n\geq 3}$ modérément ramifiés sur $\mathbb{Q}$ telles que $W_{\mathcal{Q}_n^+} = +1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q})$ et $W_{\mathcal{Q}_n^-} = -1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q})$.

- La théorie de Fröhlich permet de construire de telles extensions $K/\mathbb{Q}$ à root numbers et ramification prescrits. Le choix de W_K devient alors une propriété « de type Chebotarev » pour un nombre premier qui sera (presque) le seul ramifié dans l'extension. Une borne sur le plus petit premier dans le théorème de Chebotarev permet ainsi de contrôler la taille du discriminant des extensions construites.

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée : on va construire $(\mathcal{Q}_n^{\pm})_{n\geq 3}$ modérément ramifiés sur $\mathbb{Q}$ telles que $W_{\mathcal{Q}_n^+} = +1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q})$ et $W_{\mathcal{Q}_n^-} = -1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q})$.

- La théorie de Fröhlich permet de construire de telles extensions $K/\mathbb{Q}$ à root numbers et ramification prescrits. Le choix de W_K devient alors une propriété « de type Chebotarev » pour un nombre premier qui sera (presque) le seul ramifié dans l'extension. Une borne sur le plus petit premier dans le théorème de Chebotarev permet ainsi de contrôler la taille du discriminant des extensions construites.

- Avec des estimations convenables, on contrôle la variance grâce au discriminant, et les espérances explosent vers $+\infty$ le long de $(\mathcal{Q}_n^+)_{n\geq 3}$ et vers $-\infty$ le long de $(\mathcal{Q}_n^-)_{n\geq 3}$.

Idée de démonstration

- La théorie des modules galoisiens de Fröhlich montre que $W(\chi)$ est le même pour tout caractère symplectique dans le cas d'une extension quaternionienne modérément ramifiée : on va construire $(\mathcal{Q}_n^{\pm})_{n\geq 3}$ modérément ramifiés sur $\mathbb{Q}$ telles que $W_{\mathcal{Q}_n^+} = +1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q})$ et $W_{\mathcal{Q}_n^-} = -1$ pour tout caractère symplectique de $\mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q})$.

- La théorie de Fröhlich permet de construire de telles extensions $K/\mathbb{Q}$ à root numbers et ramification prescrits. Le choix de W_K devient alors une propriété « de type Chebotarev » pour un nombre premier qui sera (presque) le seul ramifié dans l'extension. Une borne sur le plus petit premier dans le théorème de Chebotarev permet ainsi de contrôler la taille du discriminant des extensions construites.

- Avec des estimations convenables, on contrôle la variance grâce au discriminant, et les espérances explosent vers $+\infty$ le long de $(\mathcal{Q}_n^+)_{n\geq 3}$ et vers $-\infty$ le long de $(\mathcal{Q}_n^-)_{n\geq 3}$. Des inégalités de grandes déviations de Fiorilli-Jouve permettent de conclure (**NB :** quand le corps de base n'est pas $\mathbb{Q}$, celles-ci ne suffisent plus).

Organisation de l'exposé

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K ($\Leftrightarrow$ corps des fonctions d'une courbe projective irréductible lisse sur $\mathbb{F}_q$).

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K ($\Leftrightarrow$ corps des fonctions d'une courbe projective irréductible lisse sur $\mathbb{F}_q$).

On dispose d'une théorie de la ramification en tout point semblable à celle pour les corps de nombres (corps globaux).

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K ($\Leftrightarrow$ corps des fonctions d'une courbe projective irréductible lisse sur $\mathbb{F}_q$).

On dispose d'une théorie de la ramification en tout point semblable à celle pour les corps de nombres (corps globaux). Ici, on s'intéresse à la répartition des diviseurs premiers de K ($\Leftrightarrow$ orbites galoisiennes de points fermés de la courbe).

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K ($\Leftrightarrow$ corps des fonctions d'une courbe projective irréductible lisse sur $\mathbb{F}_q$).

On dispose d'une théorie de la ramification en tout point semblable à celle pour les corps de nombres (corps globaux). Ici, on s'intéresse à la répartition des diviseurs premiers de K ($\Leftrightarrow$ orbites galoisiennes de points fermés de la courbe).

Si L/K est une extension galoisienne, on peut associer à (presque) tout diviseur premier P de K une classe de conjugaison Frob_P de $\mathrm{Gal}(L/K)$.

Extensions de corps de fonctions

Un **corps de fonctions** sur $\mathbb{F}_q$ tout corps K finiment engendré et de degré de transcendance 1 sur $\mathbb{F}_q$, tel que $\mathbb{F}_q$ soit algébriquement clos dans K ($\Leftrightarrow$ corps des fonctions d'une courbe projective irréductible lisse sur $\mathbb{F}_q$).

On dispose d'une théorie de la ramification en tout point semblable à celle pour les corps de nombres (corps globaux). Ici, on s'intéresse à la répartition des diviseurs premiers de K ($\Leftrightarrow$ orbites galoisiennes de points fermés de la courbe).

Si L/K est une extension galoisienne, on peut associer à (presque) tout diviseur premier P de K une classe de conjugaison Frob_P de $\mathrm{Gal}(L/K)$. On peut ainsi retrouver des congruences de polynômes irréductibles sur $\mathbb{F}_q$.

Hypothèse de Riemann pour les courbes

Soit L/K une extension galoisienne géométrique (*i.e.* L est aussi un corps de fonctions sur $\mathbb{F}_q$) de groupe de Galois G.

Hypothèse de Riemann pour les courbes

Soit L/K une extension galoisienne géométrique (*i.e.* L est aussi un corps de fonctions sur $\mathbb{F}_q$) de groupe de Galois G.

Théorème (Weil).

On a $\zeta_K(s) = L(s, \chi_0, L/K)$ est une fraction rationnelle en la variable $u := q^{-s}$: $\zeta_K(s) = \frac{P(u)}{(1-qu)(1-u)}$ avec $P \in \mathbb{Z}[X]$. Pour tout $\chi \in \mathrm{Irr}(G) \setminus \{\chi_0\}$, $L(s, \chi, L/K)$ est un **polynôme** à coefficients entiers en u : $L(s, \chi, L/K) = \prod_{j=1}^{M_\chi}(1 - \gamma(j, \chi)u)$. Les (inverses des) racines ont pour module $q^{1/2}$ ($\Leftrightarrow$ les zéros ont pour partie réelle $1/2$).

Courses dans les corps de fonctions

Soit C_1, C_2 des classes de conjugaison de G. On pose

$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ X \geq 2 \mid \frac{\pi(X; C_1, L/K)}{\# C_1} > \frac{\pi(X; C_2, L/K)}{\# C_2} \right\}$$

où

$$\pi(X; C, L/K) := \#\{P \text{ diviseur premier de } K \mid N(P) = X, \mathrm{Frob}_P = C\}.$$

Courses dans les corps de fonctions

Soit C_1, C_2 des classes de conjugaison de G. On pose

$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ X \geq 2 \mid \frac{\pi(X; C_1, L/K)}{\# C_1} > \frac{\pi(X; C_2, L/K)}{\# C_2} \right\}$$

où

$$\pi(X; C, L/K) := \#\{P \text{ diviseur premier de } K \mid N(P) = X, \mathrm{Frob}_P = C\}.$$

Théorème (Cha-Im, 2011).

Si L/K satisfait LI alors

$$d_{\text{nat}}(\mathcal{P}_{L/K;C_1,C_2}) := \lim_{X \to +\infty} \frac{\#(\mathcal{P}_{L/K;C_1C_2} \cap [2, X])}{X}$$

existe.

Courses dans les corps de fonctions

Soit C_1, C_2 des classes de conjugaison de G. On pose

$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ X \geq 2 \mid \frac{\pi(X; C_1, L/K)}{\# C_1} > \frac{\pi(X; C_2, L/K)}{\# C_2} \right\}$$

où

$$\pi(X; C, L/K) := \#\{P \text{ diviseur premier de } K \mid N(P) = X, \mathrm{Frob}_P = C\}.$$

Théorème (Cha-Im, 2011).

Si L/K satisfait LI alors

$$d_{\mathrm{nat}}(\mathcal{P}_{L/K;C_1,C_2}) := \lim_{X \to +\infty} \frac{\#(\mathcal{P}_{L/K;C_1C_2} \cap [2, X])}{X}$$

existe.

Ici LI signifie que, en écrivant $\gamma(j, \chi) = \sqrt{q} e^{i\theta(j,\chi)}$, que $\{\theta(j, \chi) \mid \chi \in \mathrm{Irr}(G) \setminus \{\chi_0\}, 1 \leq j \leq M_\chi/2\} \cup \{\pi\}$ est linéairement indépendant sur $\mathbb{Q}$.

Courses dans les corps de fonctions

Soit C_1, C_2 des classes de conjugaison de G. On pose

$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ X \geq 2 \mid \frac{\pi(X; C_1, L/K)}{\# C_1} > \frac{\pi(X; C_2, L/K)}{\# C_2} \right\}$$

où

$$\pi(X; C, L/K) := \#\{P \text{ diviseur premier de } K \mid N(P) = X, \mathrm{Frob}_P = C\}.$$

Théorème (Cha-Im, 2011).

Si L/K satisfait LI alors

$$d_{\mathrm{nat}}(\mathcal{P}_{L/K;C_1,C_2}) := \lim_{X \to +\infty} \frac{\#(\mathcal{P}_{L/K;C_1C_2} \cap [2, X])}{X}$$

existe.

Ici LI signifie que, en écrivant $\gamma(j,\chi) = \sqrt{q} e^{i\theta(j,\chi)}$, que $\{\theta(j,\chi) \mid \chi \in \mathrm{Irr}(G) \setminus \{\chi_0\}, 1 \leq j \leq M_\chi/2\} \cup \{\pi\}$ est linéairement indépendant sur $\mathbb{Q}$.

Remarque importante : On connaît des contre-exemples !

Un théorème central limite

Théorème (B. , 2020).

Soit $K = \mathbb{F}_q(x)$, $n \geq 3$ tel que $q \equiv 1 \bmod n$. Soit $(f_d)_{d>n}$ une famille d'éléments sans facteur carré de $\mathbb{F}_q[x]$ telle que pour tout $d > n$, $\deg f_d = d$ et L_d/K satisfasse LI, où $L_d = \mathbb{F}_q(x, y)$ et $y^n = f_d(x)$. Alors

$$\max_{C_1, C_2 \in \mathrm{Gal}(L_d/K)} \left| d_{\text{nat}}(\mathcal{P}_{L_d/K;C_1,C_2}) - \frac{1}{2} \right| \asymp_n \frac{1}{\sqrt{d}}.$$

Idée de démonstration

- Une formule explicite et LI permet de calculer la fonction caractéristique de la distribution limite μ de $\frac{\pi(X;C_1,L/K)}{\#C_1} - \frac{\pi(X;C_2,L/K)}{\#C_2}$.

Idée de démonstration

- Une formule explicite et LI permet de calculer la fonction caractéristique de la distribution limite μ de $\frac{\pi(X;C_1,L/K)}{\#C_1} - \frac{\pi(X;C_2,L/K)}{\#C_2}$.
- On utilise une inégalité de Berry-Esseen pour borner l'écart $\left|d_{\mathrm{nat}}(\mathcal{P}_{L_d/K;C_1,C_2}) - \frac{1}{2}\right|$ par $V^{-1/2}$, où V est la variance de μ.

Idée de démonstration

- Une formule explicite et LI permet de calculer la fonction caractéristique de la distribution limite μ de $\frac{\pi(X;C_1,L/K)}{\#C_1} - \frac{\pi(X;C_2,L/K)}{\#C_2}$.
- On utilise une inégalité de Berry-Esseen pour borner l'écart $\left|d_{\text{nat}}(\mathcal{P}_{L_d/K;C_1,C_2}) - \frac{1}{2}\right|$ par $V^{-1/2}$, où V est la variance de μ.
- L'étude de la ramification (qui est modérée) et la formule de Riemann-Hurwitz montre que $V \asymp_n g_{L_d}$ (**genre** de L_d).

Idée de démonstration

- Une formule explicite et LI permet de calculer la fonction caractéristique de la distribution limite μ de $\frac{\pi(X;C_1,L/K)}{\#C_1} - \frac{\pi(X;C_2,L/K)}{\#C_2}$.

- On utilise une inégalité de Berry-Esseen pour borner l'écart $\left|d_{\text{nat}}(\mathcal{P}_{L_d/K;C_1,C_2}) - \frac{1}{2}\right|$ par $V^{-1/2}$, où V est la variance de μ.

- L'étude de la ramification (qui est modérée) et la formule de Riemann-Hurwitz montre que $V \asymp_n g_{L_d}$ (**genre** de L_d). Comme L_D/K est superelliptique, $g_{L_D} \asymp_n d$.

Organisation de l'exposé

1. Biais de Tchebychev : cadre historique
2. Le cas des corps de nombres
3. Le cas des corps de fonctions
4. **Versions explicites du théorème de Kronecker-Weyl**

Le théorème de Kronecker-Weyl

Théorème (Kronecker-Weyl continu).

Soit $\theta_1, \ldots, \theta_r \in \mathbb{R}$. Le sous-groupe à un paramètre

$$\Gamma_\theta := \left\{ \left(e^{i\theta_1 y}, \ldots, e^{i\theta_r y} \right) \mid y \in \mathbb{R} \right\}$$

de $\mathbb{T}^r$ est équiréparti dans un sous-tore de $\mathbb{T}^r$, *i.e.* il existe un sous-groupe connexe fermé H de $\mathbb{T}^r$ tel que pour toute fonction continue $f : \mathbb{T}^r \to \mathbb{C}$,

$$\frac{1}{X} \int_0^X f\left(e^{i\theta_1 y}, \ldots, e^{i\theta_r y} \right) dy \underset{X \to +\infty}{\longrightarrow} \int_H f \, \mathrm{d}\mu_H$$

où μ_H est la mesure de Haar normalisée de H.
De plus, $\dim H = \dim \mathrm{Vect}_{\mathbb{Q}}(\theta_1, \ldots, \theta_r)$.

Le théorème de Kronecker-Weyl

Théorème (Kronecker-Weyl continu).

Soit $\theta_1, \ldots, \theta_r \in \mathbb{R}$. Le sous-groupe à un paramètre

$$\Gamma_\theta := \left\{ \left(e^{i\theta_1 y}, \ldots, e^{i\theta_r y} \right) \mid y \in \mathbb{R} \right\}$$

de $\mathbb{T}^r$ est équiréparti dans un sous-tore de $\mathbb{T}^r$, *i.e.* il existe un sous-groupe connexe fermé H de $\mathbb{T}^r$ tel que pour toute fonction continue $f : \mathbb{T}^r \to \mathbb{C}$,

$$\frac{1}{X} \int_0^X f\left(e^{i\theta_1 y}, \ldots, e^{i\theta_r y} \right) \, dy \underset{X \to +\infty}{\longrightarrow} \int_H f \, \mathrm{d}\mu_H$$

où μ_H est la mesure de Haar normalisée de H.
De plus, $\dim H = \dim \mathrm{Vect}_{\mathbb{Q}}(\theta_1, \ldots, \theta_r)$.

Preuve : Dualité de Pontryagin, formule sommatoire de Poisson et densité des caractères dans $\mathcal{C}^0(\mathbb{T}^r, \mathbb{C})$.

Le théorème de Kronecker-Weyl

Théorème (Kronecker-Weyl discret).

Soit $\theta_1, \ldots, \theta_r \in \mathbb{R}$. Le sous-groupe à un paramètre discret

$$\Gamma_\theta := \left\{ \left(e^{i\theta_1 n}, \ldots, e^{i\theta_r n} \right) \mid n \in \mathbb{Z} \right\}$$

de $\mathbb{T}^r$ est équiréparti dans son adhérence, *i.e.* il existe un sous-groupe fermé H de $\mathbb{T}^r$ tel que pour toute fonction continue $f : \mathbb{T}^r \to \mathbb{C}$,

$$\frac{1}{X} \sum_{n \leq X} f\left(e^{i\theta_1 n}, \ldots, e^{i\theta_r n} \right) \underset{X \to +\infty}{\longrightarrow} \int_H f \, \mathrm{d}\mu_H$$

où μ_H est la mesure de Haar normalisée de H. Si $\pi \notin \mathrm{Vect}_{\mathbb{Q}}(\theta_1, \ldots, \theta_r)$ alors H est connexe.

Preuve : Mêmes ingrédients.

Le théorème de Kronecker-Weyl

Théorème (Kronecker-Weyl discret).

Soit $\theta_1, \ldots, \theta_r \in \mathbb{R}$. Le sous-groupe à un paramètre discret

$$\Gamma_\theta := \left\{ \left(e^{i\theta_1 n}, \ldots, e^{i\theta_r n} \right) \mid n \in \mathbb{Z} \right\}$$

de $\mathbb{T}^r$ est équiréparti dans son adhérence, *i.e.* il existe un sous-groupe fermé H de $\mathbb{T}^r$ tel que pour toute fonction continue $f : \mathbb{T}^r \to \mathbb{C}$,

$$\frac{1}{X} \sum_{n \leq X} f\left(e^{i\theta_1 n}, \ldots, e^{i\theta_r n} \right) \underset{X \to +\infty}{\longrightarrow} \int_H f \, \mathrm{d}\mu_H$$

où μ_H est la mesure de Haar normalisée de H. Si $\pi \notin \mathrm{Vect}_{\mathbb{Q}}(\theta_1, \ldots, \theta_r)$ alors H est connexe.

Preuve : Mêmes ingrédients.

Le nombre π joue un rôle particulier ici : si $\theta_i \in \pi\mathbb{Q}$, une des composantes de Γ_θ est discrète.

Versions explicites

Théorème (B. , 2020).

Soit $\theta_1, \dots, \theta_r \in \mathbb{R}$, $\theta_1 \notin \pi\mathbb{Q}$ tels que $(2\pi, \theta_1, \dots, \theta_m)$ soit une base de $\mathrm{Vect}_{\mathbb{Q}}(2\pi, \theta_1, \dots, \theta_r)$. On note $\theta_j = 2\pi c_j + \sum_{k=1}^{m} b_{k,j}\theta_k$, d le PPCM des dénominateurs des $c_j, b_{k,j}$ et $h_{k,j} = db_{k,j} \in \mathbb{Z}$. Alors

$$\overline{\Gamma_\theta} = \bigcup_{a=0}^{d-1} \nu_\theta^a H_\theta,$$

où $\nu_\theta := \left(e^{i\theta_1}, \dots, e^{i\theta_r}\right)$ et

$$H_\theta := \left\{ \left(z_1^d, \dots, z_m^d, \dots, \prod_{k=1}^{m} z_k^{h_{k,j}}, \dots \right) \mid (z_1, \dots, z_m) \in \mathbb{T}^m \right\}.$$

Si la base est choisie de sorte que d est minimal, alors $\overline{\Gamma_\theta}$ a exactement d composantes connexes.

Application

Comment utiliser cette version explicite du théorème de Kronecker-Weyl discret ?

Application

Comment utiliser cette version explicite du théorème de Kronecker-Weyl discret ?

Les formules explicites sur les corps de fonctions sont de la forme

$$\begin{aligned}\frac{X}{q^{X/2}}\frac{\#G}{\#C}\pi(X;C,L/K) &= A + a_0\cos(\pi X) + \sum_{k=1}^{n}\left(a_k e^{i\theta_k X} + \overline{a_k}e^{-i\theta_k X}\right) + o(1)\\ &= f\left(e^{i\pi X}, e^{i\theta_1 X}, \dots, e^{i\theta_r X}\right) + o(1)\end{aligned}$$

quand $X \to +\infty$, avec $A, a_0, \dots, a_n \in \mathbb{R}$ et $f \in \mathbb{C}(X_0, X_1, \dots, X_r)$.

Application

Comment utiliser cette version explicite du théorème de Kronecker-Weyl discret ?

Les formules explicites sur les corps de fonctions sont de la forme

$$\begin{aligned}\frac{X}{q^{X/2}}\frac{\#G}{\#C}\pi(X;C,L/K) &= A + a_0\cos(\pi X) + \sum_{k=1}^{n}\left(a_k e^{i\theta_k X} + \overline{a_k}e^{-i\theta_k X}\right) + o(1)\\ &= f\left(e^{i\pi X}, e^{i\theta_1 X}, \ldots, e^{i\theta_r X}\right) + o(1)\end{aligned}$$

quand $X \to +\infty$, avec $A, a_0, \ldots, a_n \in \mathbb{R}$ et $f \in \mathbb{C}(X_0, X_1, \ldots, X_r)$.

Le théorème permet par exemple d'étudier la densité des n tels que $F_1(n) > F_2(n)$, où $F_i = f_i\left(e^{i\pi X}, e^{i\theta_1 X}, \ldots, e^{i\theta_r X}\right) + o(1)$ quand $X \to +\infty$.

Application

Théorème (B. , 2020).

Soit $\theta_1, \ldots, \theta_r \in \mathbb{R}$, $\theta_1 \notin \pi\mathbb{Q}$ et $f_1, f_2 \in \mathbb{C}(X_1, \ldots, X_r)$ à valeurs réelles et sans pôle sur $\mathbb{T}^r$. Soit $F_j(t) = f_j\left(e^{i\theta_1 t}, \ldots, e^{i\theta_r t}\right) + o(1)$ quand $t \to +\infty$.
Alors

$$\frac{1}{d}\sum_{a=0}^{d-1}\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > f_2(\nu_\theta^a Z_\theta)) \leq \underline{d_{\text{nat}}}(F_1 > F_2)$$

$$\leq \overline{d_{\text{nat}}}(F_1 > F_2) \leq \frac{1}{d}\sum_{a=0}^{d-1}\mathbb{P}(f_1(\nu_\theta^a Z_\theta) \geq f_2(\nu_\theta^a Z_\theta)).$$

De plus, si pour tout $0 \leq a \leq d-1$, il existe $n \equiv a \bmod d$ tel que $F_1(n) \neq F_2(n)$, alors $d_{\text{nat}}(F_1 > F_2)$ existe et

$$d_{\text{nat}}(F_1 > F_2) = \frac{1}{d}\sum_{a=0}^{d-1}\mathbb{P}(f_1(\nu_\theta^a Z_\theta) > f_2(\nu_\theta^a Z_\theta)).$$

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2+t)\alpha^3 - 1 = 0$.

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2+t)\alpha^3 - 1 = 0$. On a $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$, avec $\mathrm{Irr}(\mathfrak{S}_3) = \{\chi_0, \chi_1, \chi_2\}$. Notons $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ et $C_3 = \{(1\,2\,3), (1\,3\,2)\}$.

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2 + t)\alpha^3 - 1 = 0$. On a $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$, avec $\mathrm{Irr}(\mathfrak{S}_3) = \{\chi_0, \chi_1, \chi_2\}$. Notons $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ et $C_3 = \{(1\,2\,3), (1\,3\,2)\}$.

On a

$$L(s, \chi_1, L/K) = 1 + 4u + 7u^2 = (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),$$

$$L(s, \chi_2, L/K) = 1 + u + 7u^2 = (1 - \gamma_2 u)(1 - \overline{\gamma_2} u),$$

$$\gamma_1 = -2 + i\sqrt{3}$$

et

$$\gamma_2 = \frac{-1 + 3i\sqrt{3}}{2}.$$

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2+t)\alpha^3 - 1 = 0$. On a $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$, avec $\mathrm{Irr}(\mathfrak{S}_3) = \{\chi_0, \chi_1, \chi_2\}$. Notons $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2),(1\,3),(2\,3)\}$ et $C_3 = \{(1\,2\,3),(1\,3\,2)\}$.

On a

$$L(s,\chi_1,L/K) = 1 + 4u + 7u^2 = (1-\gamma_1 u)(1-\overline{\gamma_1}u),$$
$$L(s,\chi_2,L/K) = 1 + u + 7u^2 = (1-\gamma_2 u)(1-\overline{\gamma_2}u),$$
$$\gamma_1 = -2 + i\sqrt{3}$$

et

$$\gamma_2 = \frac{-1+3i\sqrt{3}}{2}.$$

Alors $\theta_1 = \arctan\left(-\frac{\sqrt{3}}{2}\right)$, $\theta_2 = \arctan(-3\sqrt{3}) \notin \pi\mathbb{Q}$ et $\theta_1 + \theta_2 = \frac{4\pi}{3}$ (!).

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2+t)\alpha^3 - 1 = 0$. On a $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$, avec $\mathrm{Irr}(\mathfrak{S}_3) = \{\chi_0, \chi_1, \chi_2\}$. Notons $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ et $C_3 = \{(1\,2\,3), (1\,3\,2)\}$.

On a

$$L(s, \chi_1, L/K) = 1 + 4u + 7u^2 = (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),$$
$$L(s, \chi_2, L/K) = 1 + u + 7u^2 = (1 - \gamma_2 u)(1 - \overline{\gamma_2} u),$$
$$\gamma_1 = -2 + i\sqrt{3}$$

et

$$\gamma_2 = \frac{-1 + 3i\sqrt{3}}{2}.$$

Alors $\theta_1 = \arctan\left(-\frac{\sqrt{3}}{2}\right)$, $\theta_2 = \arctan(-3\sqrt{3}) \notin \pi\mathbb{Q}$ et $\theta_1 + \theta_2 = \frac{4\pi}{3}$ (!).

Des vérifications numériques montrent que pour toute permutation $\sigma \in \mathfrak{S}_3$, la densité $d_{\text{nat}}\left(\mathcal{P}_{L/K;C_{\sigma(1)},C_{\sigma(2)},C_{\sigma(3)}}\right)$ existe,

Un exemple de Cha-Im

Soit $K = \mathbb{F}_7(t)$ et $L = K(\alpha)$ où $\alpha^6 - (t^2+t)\alpha^3 - 1 = 0$. On a $G = \mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$, avec $\mathrm{Irr}(\mathfrak{S}_3) = \{\chi_0, \chi_1, \chi_2\}$. Notons $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\,2), (1\,3), (2\,3)\}$ et $C_3 = \{(1\,2\,3), (1\,3\,2)\}$.

On a

$$L(s, \chi_1, L/K) = 1 + 4u + 7u^2 = (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),$$

$$L(s, \chi_2, L/K) = 1 + u + 7u^2 = (1 - \gamma_2 u)(1 - \overline{\gamma_2} u),$$

$$\gamma_1 = -2 + i\sqrt{3}$$

et

$$\gamma_2 = \frac{-1 + 3i\sqrt{3}}{2}.$$

Alors $\theta_1 = \arctan\left(-\frac{\sqrt{3}}{2}\right)$, $\theta_2 = \arctan(-3\sqrt{3}) \notin \pi\mathbb{Q}$ et $\theta_1 + \theta_2 = \frac{4\pi}{3}$ (!).

Des vérifications numériques montrent que pour toute permutation $\sigma \in \mathfrak{S}_3$, la densité $d_{\mathrm{nat}}\left(\mathcal{P}_{L/K;C_{\sigma(1)},C_{\sigma(2)},C_{\sigma(3)}}\right)$ existe, et aussi $0 < d_{\mathrm{nat}}\left(\mathcal{P}_{L/K;C_{\sigma(1)},C_{\sigma(2)},C_{\sigma(3)}}\right) < 1$.

Merci de votre attention.