

Théorème de Chebotarev effectif

Bruno Winckler

CJC 2014, Bordeaux

13 juin 2014

Plan

- 1 Introduction
 - Énoncé du théorème de Chebotarev
 - Fil de la démonstration

Plan

- 1 Introduction
 - Énoncé du théorème de Chebotarev
 - Fil de la démonstration
- 2 Démonstration
 - Transformée de Mellin tronquée
 - Facteurs γ et répartition des zéros
 - Conclusion

Plan

- 1 Introduction
 - Énoncé du théorème de Chebotarev
 - Fil de la démonstration
- 2 Démonstration
 - Transformée de Mellin tronquée
 - Facteurs γ et répartition des zéros
 - Conclusion

Soit L/K une extension galoisienne de corps de nombres, \mathfrak{p} un idéal maximal de \mathcal{O}_K qui ne se ramifie pas dans L , et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de G

qui relève

$$\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \rightarrow & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{N_{K/\mathbb{Q}}(\mathfrak{p})} \end{array} \cdot$$

Soit L/K une extension galoisienne de corps de nombres, \mathfrak{p} un idéal maximal de \mathcal{O}_K qui ne se ramifie pas dans L , et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de G

qui relève
$$\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \rightarrow & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{N_{K/\mathbb{Q}}(\mathfrak{p})} \end{array} .$$

On note $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{ \left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p} \right\}$ et si C est une classe de conjugaison, on pose

$$\pi_C(x) = \left\{ \mathfrak{p} \in \text{Spec}(\mathcal{O}_K) \setminus \{0\}; N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \text{ et } \left(\frac{L/K}{\mathfrak{p}}\right) = C \right\} .$$

Théorème (Théorème de Chebotarev explicite, W.)

Notons $\text{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$. Pour $x \geq \exp(109981n_L(\ln(9d_L^8))^2)$,

$$\left| \pi_C(x) - \frac{|C|}{|G|} \text{Li}(x) \right| \leq \frac{|C|}{|G|} \text{Li}(x^\beta) + 3,37 \cdot 10^{13} \frac{|C|}{|G|} x \exp\left(-\frac{1}{12} \sqrt{\frac{\ln(x)}{n_L}}\right),$$

avec β l'éventuel zéro positif de ζ_L « proche » de 1.

Théorème (Théorème de Chebotarev explicite, W.)

Notons $\text{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$. Pour $x \geq \exp(109981n_L(\ln(9d_L^8))^2)$,

$$\left| \pi_C(x) - \frac{|C|}{|G|} \text{Li}(x) \right| \leq \frac{|C|}{|G|} \text{Li}(x^\beta) + 3,37 \cdot 10^{13} \frac{|C|}{|G|} x \exp\left(-\frac{1}{12} \sqrt{\frac{\ln(x)}{n_L}}\right),$$

avec β l'éventuel zéro positif de ζ_L « proche » de 1.

Théorème (Théorème de Chebotarev explicite avec GRH, W.)

Supposons que GRH est vraie pour ζ_L . Alors, pour tout $x \geq 2$,

$$\left| \pi_C(x) - \frac{|C|}{|G|} \text{Li}(x) \right| \leq \frac{|C|}{|G|} \sqrt{x} [1, 2 \ln(d_L) + 0,6 \ln(x)n_L + \text{reste}].$$

Applications

Applications

Exemple

Soit $P \in \mathcal{O}_K[X]$ un polynôme irréductible sur K , de sorte que $L = K[X]/(P)$. La décomposition en cycles à support disjoints de $\left(\frac{L/K}{\mathfrak{p}}\right) \in G \mapsto \text{Bij}(\{\text{racines de } P\})$ dépend de la factorisation de $P \pmod{\mathfrak{p}}$ pour presque tout \mathfrak{p} , et réciproquement.

Applications

Exemple

Soit $P \in \mathcal{O}_K[X]$ un polynôme irréductible sur K , de sorte que $L = K[X]/(P)$. La décomposition en cycles à support disjoints de $\left(\frac{L/K}{\mathfrak{p}}\right) \in G \mapsto \text{Bij}(\{\text{racines de } P\})$ dépend de la factorisation de $P \pmod{\mathfrak{p}}$ pour presque tout \mathfrak{p} , et réciproquement.

- Si G est connu, le théorème de Chebotarev informe de la fréquence des différentes factorisations de P quand \mathfrak{p} varie.

Applications

Exemple

Soit $P \in \mathcal{O}_K[X]$ un polynôme irréductible sur K , de sorte que $L = K[X]/(P)$. La décomposition en cycles à support disjoints de $\left(\frac{L/K}{\mathfrak{p}}\right) \in G \mapsto \text{Bij}(\{\text{racines de } P\})$ dépend de la factorisation de $P \pmod{\mathfrak{p}}$ pour presque tout \mathfrak{p} , et réciproquement.

- Si G est connu, le théorème de Chebotarev informe de la fréquence des différentes factorisations de P quand \mathfrak{p} varie.
- Sinon, factoriser P modulo les différents \mathfrak{p} , et calculer la fréquence d'apparition des degrés de ses facteurs, permet de retrouver la structure complète des cycles de G .

Plan

- 1 Introduction
 - Énoncé du théorème de Chebotarev
 - Fil de la démonstration
- 2 Démonstration
 - Transformée de Mellin tronquée
 - Facteurs γ et répartition des zéros
 - Conclusion

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

- on a $-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_0^{\infty} \psi(x) x^{-s} \frac{dx}{x}$;

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

- on a $-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_0^{\infty} \psi(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) x^s \frac{ds}{s}$;

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

- on a $-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_0^{\infty} \psi(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) x^s \frac{ds}{s}$;
- le théorème des résidus implique $\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)}$;

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

- on a $-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_0^{\infty} \psi(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) x^s \frac{ds}{s}$;
- le théorème des résidus implique $\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)}$;
- on montre que $\zeta(s) \neq 0$ pour $\operatorname{Re}(s) = 1$, donc $\sum_{\rho} \frac{x^{\rho}}{\rho} = o(x)$, et $\psi(x) \sim x$;

On va s'inspirer des preuves du théorème des nombres premiers et du théorème de la progression arithmétique de Dirichlet.

Exemple du théorème des nombres premiers

Soient $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $\psi(x) = \sum_{p^r \leq x} \ln(p)$. Alors,

- on a $-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_0^{\infty} \psi(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) x^s \frac{ds}{s}$;
- le théorème des résidus implique $\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)}$;
- on montre que $\zeta(s) \neq 0$ pour $\operatorname{Re}(s) = 1$, donc $\sum_{\rho} \frac{x^{\rho}}{\rho} = o(x)$, et $\psi(x) \sim x$;
- on en déduit $\pi(x) \sim \operatorname{Li}(x) \sim \frac{x}{\ln(x)}$ par une transformée d'Abel.

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\overline{\mathbb{Q}(e^{2i\pi/q})}/\mathbb{Q}) \simeq (\overline{\mathbb{Z}/q\mathbb{Z}})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\overline{\mathbb{Z}/q\mathbb{Z}})^*$. Alors,

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\mathbb{Q}(\overline{e^{2i\pi/q}})/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\mathbb{Z}/q\mathbb{Z})^*$. Alors,

- on a $F_a(s) := -\frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \frac{L'}{L}(s, \chi) = s \int_0^{\infty} \psi_a(x) x^{-s} \frac{dx}{x}$;

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\mathbb{Q}(\overline{e^{2i\pi/q}})/\mathbb{Q}) \simeq (\widehat{\mathbb{Z}/q\mathbb{Z}})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\widehat{\mathbb{Z}/q\mathbb{Z}})^*$. Alors,

- on a $F_a(s) := -\frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \frac{L'}{L}(s, \chi) = s \int_0^{\infty} \psi_a(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi_a(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F_a(s) x^s \frac{ds}{s}$;

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\mathbb{Q}(\overline{e^{2i\pi/q}})/\mathbb{Q}) \simeq (\widehat{\mathbb{Z}/q\mathbb{Z}})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\widehat{\mathbb{Z}/q\mathbb{Z}})^*$. Alors,

- on a $F_a(s) := -\frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \frac{L'}{L}(s, \chi) = s \int_0^{\infty} \psi_a(x) x^{-s} \frac{dx}{x}$;
- on en déduit $\psi_a(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F_a(s) x^s \frac{ds}{s}$;
- le théorème des résidus implique

$$\psi_a(x) = \frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \left(-\sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{L'(0, \chi)}{L(0, \chi)} \right) + o(x) ;$$

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\mathbb{Q}(\overline{e^{2i\pi/q}})/\mathbb{Q}) \simeq (\widehat{\mathbb{Z}/q\mathbb{Z}})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\widehat{\mathbb{Z}/q\mathbb{Z}})^*$. Alors,

- on a $F_a(s) := -\frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \frac{L'}{L}(s, \chi) = s \int_0^{\infty} \psi_a(x) x^{-s} \frac{dx}{x}$;

- on en déduit $\psi_a(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F_a(s) x^s \frac{ds}{s}$;

- le théorème des résidus implique

$$\psi_a(x) = \frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \left(-\sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{L'(0, \chi)}{L(0, \chi)} \right) + o(x) ;$$

- le caractère principal contribue avec un x , et $\psi_a(x) \sim \frac{x}{\varphi(q)}$;

Si G est un groupe fini, on pose $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$. On a $\text{Gal}(\overline{\mathbb{Q}(e^{2i\pi/q})}/\mathbb{Q}) \simeq (\widehat{\mathbb{Z}/q\mathbb{Z}})^* \simeq (\mathbb{Z}/q\mathbb{Z})^*$.

Exemple du théorème de la progression arithmétique de Dirichlet

Soit $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $\chi \in (\widehat{\mathbb{Z}/q\mathbb{Z}})^*$. Alors,

- on a $F_a(s) := -\frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \frac{L'}{L}(s, \chi) = s \int_0^{\infty} \psi_a(x) x^{-s} \frac{dx}{x}$;

- on en déduit $\psi_a(x) = -\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F_a(s) x^s \frac{ds}{s}$;

- le théorème des résidus implique

$$\psi_a(x) = \frac{1}{\varphi(q)} \sum_{\chi} \chi(a^{-1}) \left(-\sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{L'(0, \chi)}{L(0, \chi)} \right) + o(x) ;$$

- le caractère principal contribue avec un x , et $\psi_a(x) \sim \frac{x}{\varphi(q)}$;

- on en déduit $\pi_a(x) \sim \frac{\text{Li}(x)}{\varphi(q)} \sim \frac{1}{\varphi(q)} \frac{x}{\ln(x)}$.

Généralisation de la stratégie à $G = \text{Gal}(L/K)$

Généralisation de la stratégie à $G = \text{Gal}(L/K)$

Pour tout caractère irréductible Φ de G , on pose

$$\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in I} \Phi \left(\left(\frac{L/K}{\mathfrak{F}, \mathfrak{p}} \right)^m \alpha \right), \text{ avec } \mathfrak{F} | \mathfrak{p}.$$

Généralisation de la stratégie à $G = \text{Gal}(L/K)$

Pour tout caractère irréductible Φ de G , on pose $\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in I} \Phi\left(\left(\frac{L/K}{\mathfrak{p}, \mathfrak{p}}\right)^m \alpha\right)$, avec $\mathfrak{P}|\mathfrak{p}$. Si $L(s, \Phi, L/K)$ est la fonction L d'Artin associée à Φ , alors on a

$$-\frac{L'}{L}(s, \Phi, L/K) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \Phi_K(\mathfrak{p}^m) \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-ms}.$$

Généralisation de la stratégie à $G = \text{Gal}(L/K)$

Pour tout caractère irréductible Φ de G , on pose $\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in I} \Phi\left(\left(\frac{L/K}{\mathfrak{F}, \mathfrak{p}}\right)^m \alpha\right)$, avec $\mathfrak{F}|\mathfrak{p}$. Si $L(s, \Phi, L/K)$ est la fonction L d'Artin associée à Φ , alors on a

$$-\frac{L'}{L}(s, \Phi, L/K) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \Phi_K(\mathfrak{p}^m) \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-ms}.$$

Pour démontrer le théorème de Chebotarev en suivant l'esprit des preuves précédentes, on pose

$$F_C(s) = - \sum_{\Phi} \frac{|C|}{|G|} \bar{\Phi}(g) \frac{L'}{L}(s, \Phi, L/K),$$

où $g \in C$, et en avant Guingamp.

Plan

1 Introduction

- Énoncé du théorème de Chebotarev
- Fil de la démonstration

2 Démonstration

- Transformée de Mellin tronquée
- Facteurs γ et répartition des zéros
- Conclusion

$$F_C(s) \simeq \sum_{\substack{\mathfrak{p} \text{ non ram.} \\ \left[\frac{L/K}{\mathfrak{p}}\right]^m = C}} \sum_{m=1}^{\infty} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-ms}.$$

$$F_C(s) \simeq \sum_{\substack{\mathfrak{p} \text{ non ram.} \\ \left[\frac{L/K}{\mathfrak{p}}\right]^m = C}} \sum_{m=1}^{\infty} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-ms}.$$

Lemme (Transformée de Mellin tronquée)

Si $y > 0$, $\sigma > 0$ et $T > 0$, alors

$$\left| \frac{1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s} ds - 1 \right| \leq y^\sigma \min(1, T^{-1} |\ln(y)|^{-1}) \text{ si } y > 1,$$

$$\left| \frac{1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s} ds \right| \leq y^\sigma \min(1, T^{-1} |\ln(y)|^{-1}) \text{ si } 0 < y < 1.$$

On a alors

$$\psi_C(x) = \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{p})^m \leq x \\ \mathfrak{p} \text{ non ramifié} \\ \left[\frac{L/K}{\mathfrak{p}}\right]^m = C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds + \text{reste},$$

avec F_C est une combinaison linéaire de fonctions L d'Artin, et

$$\text{reste} \leq \frac{2}{\ln(2)} \frac{\ln(x) \ln(d_L)}{|G|} + \frac{73}{4} n_K \ln(x) + \frac{145}{6} n_K T^{-1} x (\ln(x))^2.$$

Bref, on a

$$\psi_C(x) \simeq \int_{\text{segment vertical}} \left(\text{somme de fonctions } \frac{L'}{L} \text{ d'Artin} \right) \frac{x^s}{s} ds.$$

Plan

1 Introduction

- Énoncé du théorème de Chebotarev
- Fil de la démonstration

2 Démonstration

- Transformée de Mellin tronquée
- Facteurs γ et répartition des zéros
- Conclusion

Posons $I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds$, où F_C est une combinaison linéaire de fonctions L d'Artin. Problème : on ne sait pas dire grand chose sur ces fonctions L .

Posons $I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds$, où F_C est une combinaison linéaire de fonctions L d'Artin. Problème : on ne sait pas dire grand chose sur ces fonctions L.

Soit $g \in C$, et soit H le sous-groupe de G engendré par g , E le corps fixé par H , et notons avec la lettre χ les caractères irréductibles de H (qui sont de dimension 1).

Posons $I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds$, où F_C est une combinaison linéaire de fonctions L d'Artin. Problème : on ne sait pas dire grand chose sur ces fonctions L .

Soit $g \in C$, et soit H le sous-groupe de G engendré par g , E le corps fixé par H , et notons avec la lettre χ les caractères irréductibles de H (qui sont de dimension 1).

Lemme

On a $I_C(x, T) = -\frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{L'}{L}(s, \chi, L/E) ds$.

Posons $I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds$, où F_C est une combinaison linéaire de fonctions L d'Artin. Problème : on ne sait pas dire grand chose sur ces fonctions L .

Soit $g \in C$, et soit H le sous-groupe de G engendré par g , E le corps fixé par H , et notons avec la lettre χ les caractères irréductibles de H (qui sont de dimension 1).

Lemme

On a $I_C(x, T) = -\frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{L'}{L}(s, \chi, L/E) ds$.

On a ramené l'étude de fonctions L d'Artin à celle de fonctions L abéliennes.

Propriétés classiques des fonctions L abéliennes

Soit $F(\chi)$ le conducteur de χ , et soit $A(\chi) = d_E N_{E/\mathbb{Q}}(F(\chi))$. On définit $\delta_{\chi=1}(\chi) = \begin{cases} 1 & \text{si } \chi = 1 \\ 0 & \text{sinon} \end{cases}$. Écrivons $n_E = a(\chi) + b(\chi)$, de sorte que si

$$\gamma_\chi(s) = \left(\pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) \right)^{b(\chi)} \left(\pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \right)^{a(\chi)}$$

et

$$\xi(s, \chi) = (s(s-1))^{\delta_{\chi=1}(\chi)} A(\chi)^{s/2} \gamma_\chi(s) L(s, \chi)$$

alors ξ est une fonction entière, et on a l'équation fonctionnelle $\xi(1-s, \bar{\chi}) = W(\chi)\xi(s, \chi)$.

Propriétés classiques des fonctions L abéliennes

Soit $F(\chi)$ le conducteur de χ , et soit $A(\chi) = d_E N_{E/\mathbb{Q}}(F(\chi))$. On définit $\delta_{\chi=1}(\chi) = \begin{cases} 1 & \text{si } \chi = 1 \\ 0 & \text{sinon} \end{cases}$. Écrivons $n_E = a(\chi) + b(\chi)$, de sorte que si

$$\gamma_\chi(s) = \left(\pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) \right)^{b(\chi)} \left(\pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \right)^{a(\chi)}$$

et

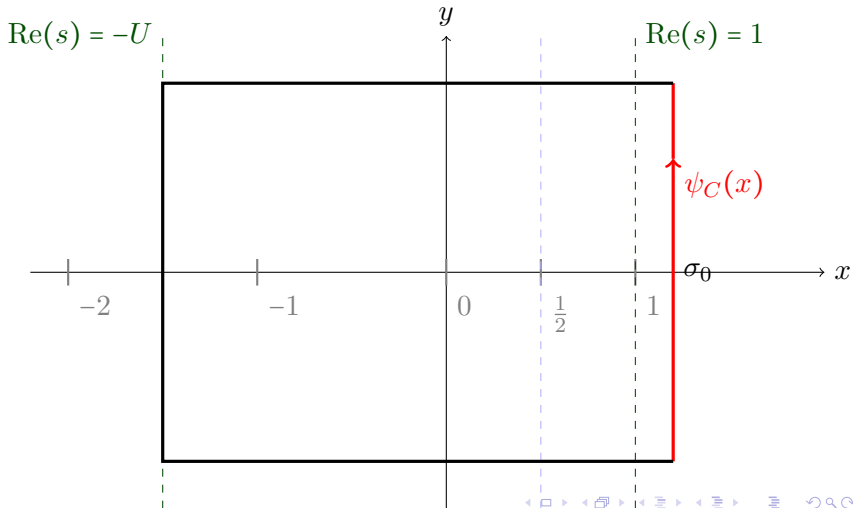
$$\xi(s, \chi) = (s(s-1))^{\delta_{\chi=1}(\chi)} A(\chi)^{s/2} \gamma_\chi(s) L(s, \chi)$$

alors ξ est une fonction entière, et on a l'équation fonctionnelle

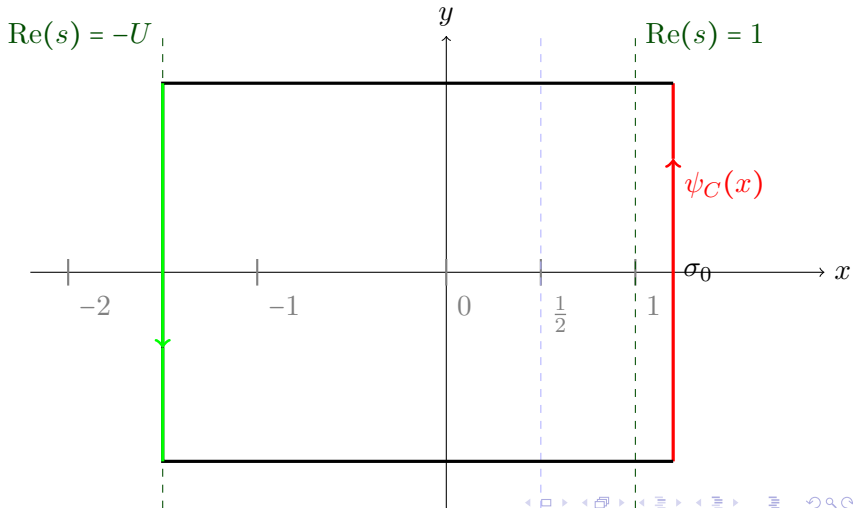
$\xi(1-s, \bar{\chi}) = W(\chi) \xi(s, \chi)$. On peut écrire

$$\xi(s, \chi) = e^{B_1(\chi) + B(\chi)s} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

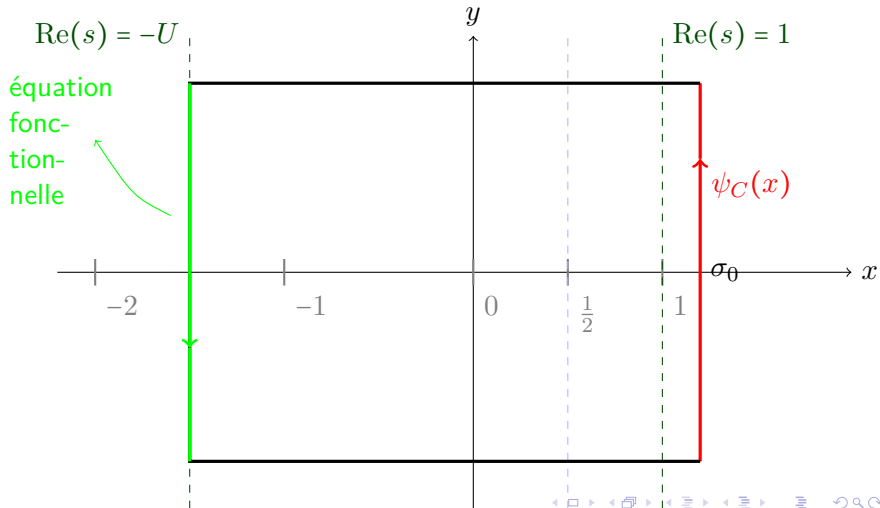
Approximation par une intégrale sur un contour



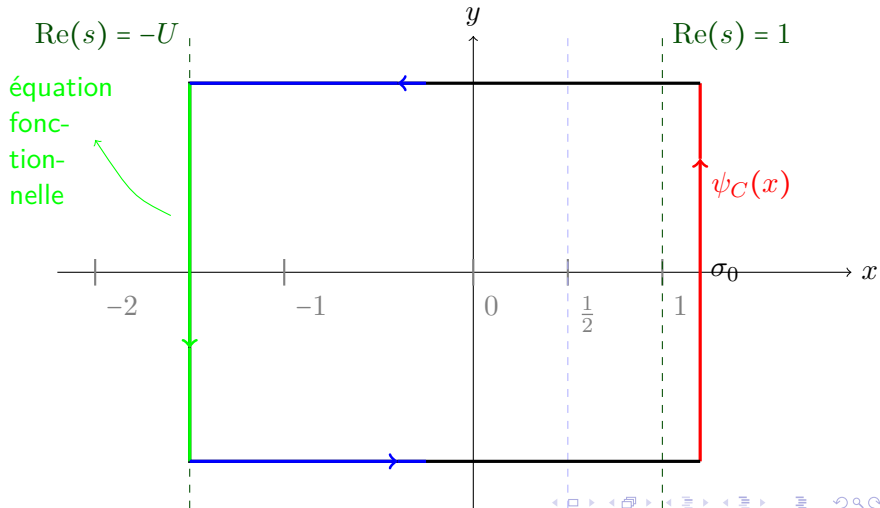
Approximation par une intégrale sur un contour



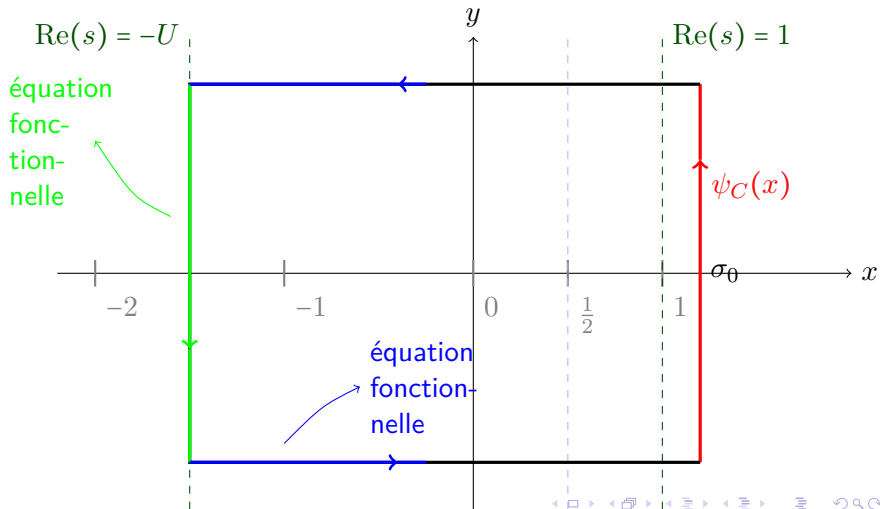
Approximation par une intégrale sur un contour



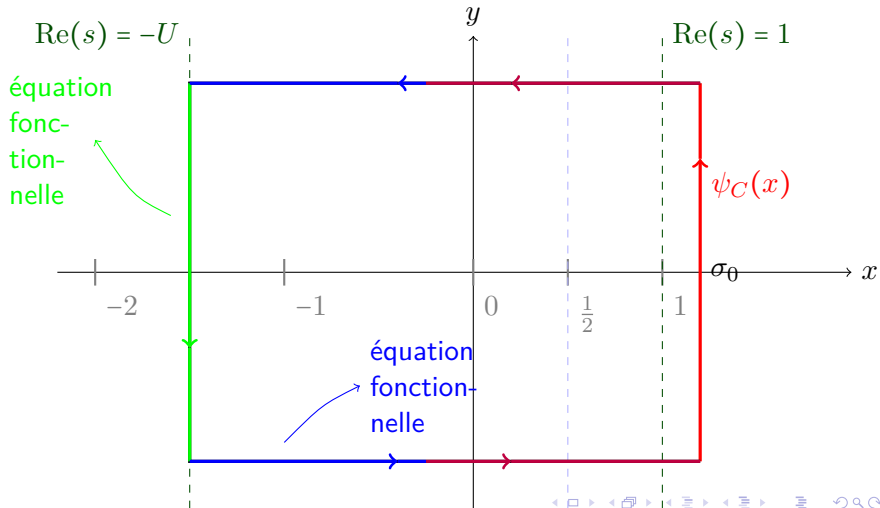
Approximation par une intégrale sur un contour



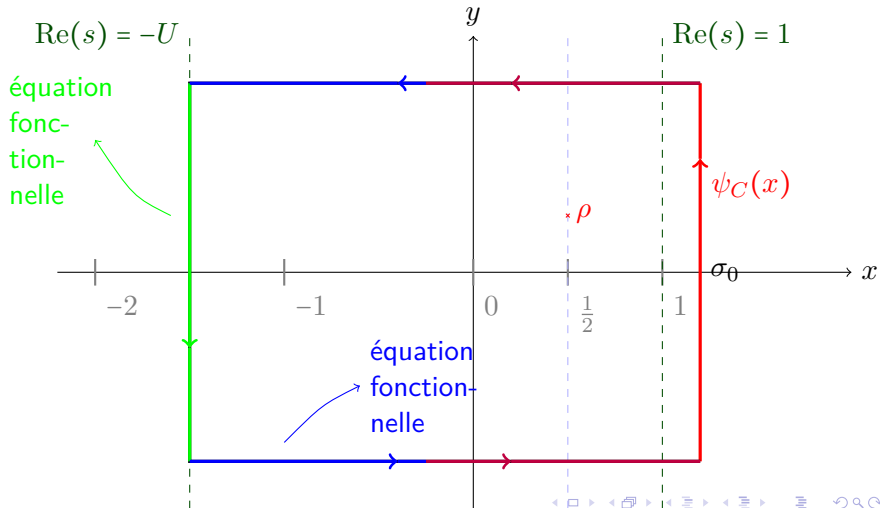
Approximation par une intégrale sur un contour



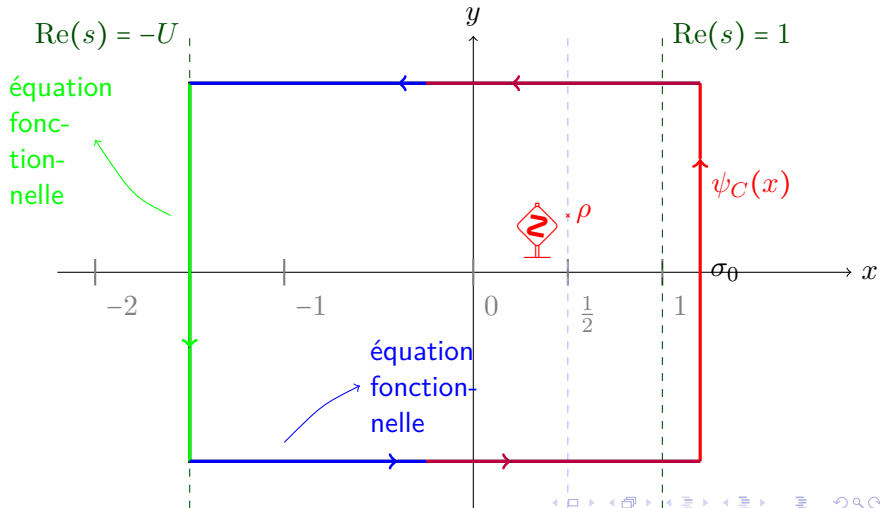
Approximation par une intégrale sur un contour



Approximation par une intégrale sur un contour



Approximation par une intégrale sur un contour



Densité des zéros des fonctions L abéliennes

Lemme

$$\begin{aligned} \frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) &= \sum_{\rho} \left(\frac{1}{s - \rho} + \frac{1}{s - \bar{\rho}} \right) - \ln(A(\chi)) \\ &\quad - 2\delta_{\chi=1}(\chi) \left(\frac{1}{s} + \frac{1}{s-1} \right) - 2 \frac{\gamma'_{\chi}(s)}{\gamma_{\chi}}. \end{aligned}$$

Densité des zéros des fonctions L abéliennes

Lemme

$$\frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) = \sum_{\rho} \left(\frac{1}{s - \rho} + \frac{1}{s - \bar{\rho}} \right) - \ln(A(\chi)) - 2\delta_{\chi=1}(\chi) \left(\frac{1}{s} + \frac{1}{s-1} \right) - 2 \frac{\gamma'_{\chi}(s)}{\gamma_{\chi}}.$$

Lemme (Densité des zéros)

Soit $n_{\chi}(t)$ le nombre de zéros $\rho = \beta + i\gamma$ de $L(\cdot, \chi)$ avec $0 < \beta < 1$ et $|\gamma - t| \leq 1$. Pour tout t , on a

$$n_{\chi}(t) + n_{\chi}(-t) \leq \frac{5}{2} \left[\ln(A(\chi)) + n_E \left(\ln \left(\frac{|t| + 3}{2\pi} \right) + 2 \right) + \text{fioritures} \right].$$

Lemme (Densité des zéros)

Soit $n_\chi(t)$ le nombre de zéros $\rho = \beta + i\gamma$ de $L(\cdot, \chi)$ avec $0 < \beta < 1$ et $|\gamma - t| \leq 1$. Pour tout t , on a

$$n_\chi(t) + n_\chi(-t) \leq \frac{5}{2} \left[\ln(A(\chi)) + n_E \left(\ln \left(\frac{|t| + 3}{2\pi} \right) + 2 \right) + \text{fioritures} \right].$$

Ce lemme permet de contrôler les sommes sur les zéros.

Lemme (Densité des zéros)

Soit $n_\chi(t)$ le nombre de zéros $\rho = \beta + i\gamma$ de $L(\cdot, \chi)$ avec $0 < \beta < 1$ et $|\gamma - t| \leq 1$. Pour tout t , on a

$$n_\chi(t) + n_\chi(-t) \leq \frac{5}{2} \left[\ln(A(\chi)) + n_E \left(\ln \left(\frac{|t| + 3}{2\pi} \right) + 2 \right) + \text{fioritures} \right].$$

Ce lemme permet de contrôler les sommes sur les zéros.

Exemple

$$\begin{aligned} \left| \sum_{|\rho| \geq 1} \left(\frac{1}{2 - \rho} + \frac{1}{\rho} \right) \right| &\leq \sum_{\substack{t = -\infty \\ t \text{ impair}}}^{\infty} \sum_{\substack{|\rho| \geq 1 \\ t \leq \gamma \leq t+2}} \frac{2}{|\rho|^2} \\ &\leq 2 \sum_{j=0}^{\infty} \frac{n_\chi(2j+2) + n_\chi(-(2j+2))}{(2j+1)^2} + 2n_\chi(0) \end{aligned}$$

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

- en chaque zéro ρ de $L(s, \chi)$, de résidu $\frac{x^\rho}{\rho}$;

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

- en chaque zéro ρ de $L(s, \chi)$, de résidu $\frac{x^\rho}{\rho}$;
- en chaque pôle de γ_χ , *i.e.* de Γ , *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi) \frac{x^{-m}}{-m}$ ou $b(\chi) \frac{x^{-m}}{-m}$;

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

- en chaque zéro ρ de $L(s, \chi)$, de résidu $\frac{x^\rho}{\rho}$;
- en chaque pôle de γ_χ , *i.e.* de Γ , *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi) \frac{x^{-m}}{-m}$ ou $b(\chi) \frac{x^{-m}}{-m}$;
- un résidu éventuellement en 0, plus compliqué, mais en $o(x)$;

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

- en chaque zéro ρ de $L(s, \chi)$, de résidu $\frac{x^\rho}{\rho}$;
- en chaque pôle de γ_χ , *i.e.* de Γ , *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi) \frac{x^{-m}}{-m}$ ou $b(\chi) \frac{x^{-m}}{-m}$;
- un résidu éventuellement en 0, plus compliqué, mais en $o(x)$;
- en $s = 1$ si $L(s, \chi) = \zeta_L(s)$, de résidu $-x$.

Théorème des résidus

Résidus de $\frac{L'}{L}(s, \chi) \frac{x^s}{s}$:

- en chaque zéro ρ de $L(s, \chi)$, de résidu $\frac{x^\rho}{\rho}$;
- en chaque pôle de γ_χ , *i.e.* de Γ , *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi) \frac{x^{-m}}{-m}$ ou $b(\chi) \frac{x^{-m}}{-m}$;
- un résidu éventuellement en 0, plus compliqué, mais en $o(x)$;
- en $s = 1$ si $L(s, \chi) = \zeta_L(s)$, de résidu $-x$.

Donc $\psi_C(x) \simeq \frac{|C|}{|G|} x + \frac{|C|}{|G|} \sum_{\chi} \sum_{\rho} \frac{x^\rho}{\rho}$.

Théorème (Formule explicite pour ψ_C)

Si $x \geq 2$ et $T \geq 2$, alors

$$\left| \psi_C(x) - \frac{|C|}{|G|}x + S(x, T) \right| \leq \frac{|C|}{|G|} \left(24, 2n_L \frac{x(\ln(x))^2}{T} \right. \\ \left. + 7, 1 \frac{x \ln(x)}{T-1} \left[\ln(d_L) + 0, 9 \right. \right. \\ \left. \left. + n_L (\ln(T+5) + 2) \right] \right. \\ \left. + \textit{de la littérature} \right),$$

où

$$S(x, T) = \frac{|C|}{|G|} \sum_x \bar{\chi}(g) \left(\sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right).$$

Plan

1 Introduction

- Énoncé du théorème de Chebotarev
- Fil de la démonstration

2 Démonstration

- Transformée de Mellin tronquée
- Facteurs γ et répartition des zéros
- Conclusion

Le problème est dorénavant d'estimer

$$S(x, T) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left(\sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^{\rho}}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right).$$

Le problème est dorénavant d'estimer

$$S(x, T) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left(\sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^{\rho}}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right).$$

Lemme (Régions sans zéro pour ζ_L)

La fonction ζ_L n'a pas de zéros $\rho = \beta + i\gamma$ dans la région délimitée par les conditions

$$|\gamma| \geq \frac{1}{1 + 4 \ln(d_L)}$$

Le problème est dorénavant d'estimer

$$S(x, T) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left(\sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^{\rho}}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right).$$

Lemme (Régions sans zéro pour ζ_L)

La fonction ζ_L n'a pas de zéros $\rho = \beta + i\gamma$ dans la région délimitée par les conditions

$$|\gamma| \geq \frac{1}{1 + 4 \ln(d_L)}$$

et

$$\beta \geq 1 - \frac{\left(12 - \sqrt{\frac{179}{2}}\right)^2}{\frac{2719}{3} \ln(d_L) + n_L \left(\frac{469}{4} \ln \left(\frac{3+|\gamma|}{2\pi} \right) + \frac{64}{29} \right) + \frac{3307}{12}}.$$

Lemme (Zéro « proche » de 1 pour ζ_L)

Si $n_L > 1$, alors ζ_L a au plus un zéro $\rho = \beta + i\gamma$ dans la région délimitée par les conditions

$$|\gamma| \leq \frac{1}{4 \ln(d_L)} \quad \text{et} \quad \beta \geq 1 - \frac{1}{4 \ln(d_L)}.$$

Ce zéro, s'il existe, est réel et simple, et correspond à un unique caractère (réel) χ_0 qui annule $L(\cdot, \chi_0)$. Par ailleurs, si $n_L = 1$, alors ζ_L n'admet pas de zéro tel que $|\gamma| < 14$.

Estimations finales

Pour rappel, on a

$$\begin{aligned} \left| \psi_C(x) - \frac{|C|}{|G|}x + S(x, T) \right| &\leq \frac{|C|}{|G|} \left(24, 2n_L \frac{x(\ln(x))^2}{T} \right. \\ &+ 7, 1 \frac{x \ln(x)}{T-1} \left[\ln(d_L) + 0, 9 \right. \\ &\left. \left. + n_L (\ln(T+5) + 2) + \text{etc} \right] \right). \end{aligned}$$

Estimations finales

Pour rappel, on a

$$\begin{aligned} \left| \psi_C(x) - \frac{|C|}{|G|}x + S(x, T) \right| &\leq \frac{|C|}{|G|} \left(24, 2n_L \frac{x(\ln(x))^2}{T} \right. \\ &+ 7, 1 \frac{x \ln(x)}{T-1} \left[\ln(d_L) + 0, 9 \right. \\ &+ \left. n_L (\ln(T+5) + 2) + \text{etc} \right]. \end{aligned}$$

Théorème

Si ζ_L vérifie GRH, alors $\forall x \geq 2$,

$$\begin{aligned} \left| \psi_C(x) - \frac{|C|}{|G|}x \right| &\leq \frac{|C|}{|G|} \sqrt{x} \ln(x) \left[1, 2 \ln(d_L) + 0, 6 \ln(x) n_L \right. \\ &+ \left. \text{etc} \right]. \end{aligned}$$

Estimations finales

Pour rappel, on a

$$\begin{aligned} \left| \psi_C(x) - \frac{|C|}{|G|}x + S(x, T) \right| &\leq \frac{|C|}{|G|} \left(24, 2n_L \frac{x(\ln(x))^2}{T} \right. \\ &+ 7, 1 \frac{x \ln(x)}{T-1} \left[\ln(d_L) + 0, 9 \right. \\ &+ \left. n_L (\ln(T+5) + 2) + \text{etc} \right]. \end{aligned}$$

Estimations finales

Pour rappel, on a

$$\begin{aligned} \left| \psi_C(x) - \frac{|C|}{|G|}x + S(x, T) \right| &\leq \frac{|C|}{|G|} \left(24, 2n_L \frac{x(\ln(x))^2}{T} \right. \\ &+ 7, 1 \frac{x \ln(x)}{T-1} \left[\ln(d_L) + 0, 9 \right. \\ &\left. \left. + n_L (\ln(T+5) + 2) + \text{etc} \right] \right). \end{aligned}$$

Théorème

Si β_0 est l'éventuel zéro « proche » de 1 de ζ_L , alors pour tout $x \geq \exp(54990, 25n_L(\ln(9d_L^8))^2)$,

$$\left| \psi_C(x) - \frac{|C|}{|G|}x - \frac{|C|}{|G|} \chi_0(g) \frac{x^{\beta_0}}{\beta_0} \right| \leq 4 \cdot 10^{12} \frac{|C|}{|G|} x \exp\left(-\frac{1}{8} \sqrt{\frac{\ln(x)}{n_L}}\right).$$

Passage de ψ_C à π_C

$$\text{Posons } \theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \left[\frac{L/K}{\mathfrak{p}} \right] = C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})).$$

Passage de ψ_C à π_C

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \left[\frac{L/K}{\mathfrak{p}}\right] = C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p}))$. On a :

$$\sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) = \theta_C(x^{1/2}) + \theta_C(x^{1/3}) + \dots + \theta_C(x^{1/[\ln(x)/\ln(2)]})$$

Passage de ψ_C à π_C

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \left[\frac{L/K}{\mathfrak{p}}\right] = C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p}))$. On a :

$$\sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) = \theta_C(x^{1/2}) + \theta_C(x^{1/3}) + \dots + \theta_C(x^{1/[\ln(x)/\ln(2)]})$$

$$\text{Alors, } \psi_C(x) - \theta_C(x) = \sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) \leq \frac{22}{15} n_K \sqrt{x} \ln(x).$$

Passage de ψ_C à θ_C

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \left[\frac{L/K}{\mathfrak{p}}\right] = C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p}))$. On a :

$$\sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) = \theta_C(x^{1/2}) + \theta_C(x^{1/3}) + \dots + \theta_C(x^{1/[\ln(x)/\ln(2)]})$$

$$\text{Alors, } \psi_C(x) - \theta_C(x) = \sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) \leq \frac{22}{15} n_K \sqrt{x} \ln(x).$$

Donc $\psi_C(x) \simeq \theta_C(x)$.

Passage de ψ_C à π_C

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p}))$. On a :

$$\sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) = \theta_C(x^{1/2}) + \theta_C(x^{1/3}) + \dots + \theta_C(x^{1/[\ln(x)/\ln(2)]})$$

Alors, $\psi_C(x) - \theta_C(x) = \sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathfrak{p} \text{ non ramifié} \\ N_{K/\mathbb{Q}}(\mathfrak{p}^m) \leq x}} \ln(N_{K/\mathbb{Q}}(\mathfrak{p})) \leq \frac{22}{15} n_K \sqrt{x} \ln(x)$.

Donc $\psi_C(x) \simeq \theta_C(x)$. On conclut avec

$$\pi_C(x) = \frac{\theta_C(x)}{\ln(x)} + \int_2^x \frac{\theta_C(t)}{t(\ln(t))^2} dt.$$

Références :

- J. Lagarias, A. Odlyzko, *Effective versions of the Chebotarev density theorem*, in : Algebraic Number Fields, ed. A. Fröhlich, Academic Press, New York, 1977, p. 409–464.
- J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications mathématiques de l'I.H.É.S, tome 54 (1981), p. 123–201.
- B. Winckler, *Théorème de Chebotarev effectif*, preprint.