Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Comptage d'extensions cubiques avec résolvante quadratique fixée

Anna Morra
(papier joint avec Henri Cohen)

Université Bordeaux 1

Séminaire de Cryptographie - Université de Rennes
12 Décembre 2008

Introduction

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- K un corps de nombres
- G un groupe de permutations transitif sur n lettres

Introduction

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

- K un corps de nombres
- G un groupe de permutations transitif sur n lettres

$$\mathcal{F}_{K,n}(G) = \{\text{extensions } L/K, [L:K] = n, \text{la clôture galoisienne } N \text{ de } L/K \text{ a } \mathrm{Gal}(N/K) \simeq G\}/\simeq$$

Introduction

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

- K un corps de nombres
- G un groupe de permutations transitif sur n lettres

$$\mathcal{F}_{K,n}(G) = \{\text{extensions } L/K, [L:K] = n, \text{la clôture galoisienne } N \text{ de } L/K \text{ a } \mathrm{Gal}(N/K) \simeq G\}/\simeq$$

$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_{K,n}(G), \mathcal{N}\mathfrak{d}(L/K) \leq X\}|.$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Plusieurs questions :

- Calculer la valeur exacte de $N_{K,n}(G,X)$ pour (K,n,G,X) fixés.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Plusieurs questions :

- Calculer la valeur exacte de $N_{K,n}(G,X)$ pour (K,n,G,X) fixés.
- Calculer la formule asymptotique de $N_{K,n}(G,X)$ pour (K,n,G) fixés et X allant vers infini.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Plusieurs questions :

- Calculer la valeur exacte de $N_{K,n}(G, X)$ pour (K, n, G, X) fixés.
- Calculer la formule asymptotique de $N_{K,n}(G, X)$ pour (K, n, G) fixés et X allant vers infini.
- Calculer des tables de corps de nombres dans $\mathcal{F}_{K,n}(G)$ jusqu'à une certaine borne X sur le discriminant relatif.

Conjectures

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On s'attend de trouver

$$N_{K,n}(X) \sim c_{K,n} X.$$

Conjecture 1 (Malle)

$$N_{K,n}(G, X) \sim c \cdot X^a (\log X)^{b-1}$$

avec des constantes explicites a dépendante seulement de G, et b dépendante de G et K.

Conjectures

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

On s'attend de trouver

$$N_{K,n}(X) \sim c_{K,n} X.$$

Conjecture 1 (Malle)

$$N_{K,n}(G, X) \sim c \cdot X^a (\log X)^{b-1}$$

avec des constantes explicites a dépendante seulement de G, et b dépendante de G et K.

- La conjecture a été prouvée pour les groupes abeliens G (Mäki, Wright) et pour toutes les extensions de degré $n \leq 4$ (Davenport-Heilbronn, Datskovsky-Wright, Cohen-Diaz y Diaz-Olivier,Bhargava)
  excepté le cas $G = A_4$
- Klüners a donné des contre-exemples.
- Récemment, Türkelli a proposé une correction.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Conjecture 2 (Conjecture de Malle "faible")

Il existe $c > 0$ *tel que pour tout* $\varepsilon > 0$

$$c \cdot X^a < N_{K,n}(G, X) < X^{a+\varepsilon}.$$

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Conjecture 2 (Conjecture de Malle "faible")

Il existe $c > 0$ *tel que pour tout* $\varepsilon > 0$

$$c \cdot X^a < N_{K,n}(G, X) < X^{a+\varepsilon}.$$

La conjecture "faible" est vraie pour

- $n = 4$, $G = S_4$ et K un corps de nombres quelconque (Yukie).
- $n = 5$ and $G = S_5$ (Kable-Yukie).
- les groupes nilpotents G (Klüners-Malle).

Théorie des corps des classes

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Quand G est abelien, la théorie des corps des classes décrit complètement $N_{K,n}(G, X)$:

Example 1

$$N_{K,2}(C_2, X) = -1 + \sum_{\mathcal{N}(\mathfrak{a}) \leq X} 2^{\mathrm{rk}(Cl_{\mathfrak{a}}^{+}(K))} M_K\left(\frac{X}{\mathcal{N}(\mathfrak{a})}\right)$$

Théorie des corps des classes

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Quand G est abelien, la théorie des corps des classes décrit complètement $N_{K,n}(G, X)$:

Example 1

$$N_{K,2}(C_2, X) = -1 + \sum_{\mathcal{N}(\mathfrak{a}) \leq X} 2^{\mathrm{rk}(Cl_{\mathfrak{a}}^{+}(K))} M_K\left(\frac{X}{\mathcal{N}(\mathfrak{a})}\right)$$

mais

- On ne peut pas déduire une formule asymptotique à partir de ce type de formule.
- Ce n'est pas assez efficace non plus pour les calculs explicits, si comparé avec les résultats obtenus avec la théorie de Kummer.

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise la théorie de Kummer pour décire $\mathcal{F}_{K,n}(G)$

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise la théorie de Kummer pour décire $\mathcal{F}_{K,n}(G)$
- On étudie la série de Dirichlet associée au comptage de discriminants

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise la théorie de Kummer pour décire $\mathcal{F}_{K,n}(G)$
- On étudie la série de Dirichlet associée au comptage de discriminants
- En principe, on peut appliquer cette méthode pour toutes les extensions abeliennes (et aussi pour les extensions "solubles") mais les formules ne sont pas assez explicites en général.

Théorie de Bhargava et espaces préhomogènes

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise les *espaces préhomogènes* (Sato, 1960).

Théorie de Bhargava et espaces préhomogènes

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise les *espaces préhomogènes* (Sato, 1960).
- On paramétrise les anneaux de nombres de degré n par des classes de formes, modulo une action de groupe naturelle (exemple : formes quadratiques binaires modulo $\mathrm{SL}_2(\mathbb{Z})$

Théorie de Bhargava et espaces préhomogènes

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- On utilise les *espaces préhomogènes* (Sato, 1960).
- On paramétrise les anneaux de nombres de degré n par des classes de formes, modulo une action de groupe naturelle (exemple : formes quadratiques binaires modulo $\mathrm{SL}_2(\mathbb{Z})$
- Résultats de Bhargava pour les extensions de degré 4 et 5 sur $\mathbb{Q}$.

Extensions quadratiques (C_2)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$ trivial.

Extensions quadratiques (C_2)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$ trivial.
- Sur K quelconque

$$N_{K,2}(C_2, X) \sim \frac{1}{2^{r_2}} \frac{\mathrm{Res}_{s=1}\zeta_K(s)}{\zeta_K(2)} X$$

([CoDiOl], en utilisant la théorie de Kummer; mais ce résultat est aussi caché dans un papier de Datskowsky-Wright)

Extensions cycliques cubiques (C_3)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$

$$N_{\mathbb{Q},3}(C_3, X) \sim \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 (\mathrm{mod}\ 6)} \left(1 - \frac{2}{p(p+1)}\right) X^{1/2}$$

(Cohn, en utilisant la théorie de Kummer)

Extensions cycliques cubiques (C_3)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$

$$N_{\mathbb{Q},3}(C_3, X) \sim \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 (\mathrm{mod}\ 6)} \left(1 - \frac{2}{p(p+1)}\right) X^{1/2}$$

(Cohn, en utilisant la théorie de Kummer)

- Sur K quelconque

$$N_{K,3}(C_3, X) \sim \begin{cases} c_K(C_3) X^{1/2} \log X & \text{if } \zeta_3 \in K \\ c_K(C_3) X^{1/2} & \text{if } \zeta_3 \notin K. \end{cases}$$

([CoDiOl], en utilisant la théorie de Kummer)

Extensions cubiques non-galoisiennes (S_3)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$

$$N_{\mathbb{Q},3}(S_3, X) \sim \frac{1}{\zeta(3)} X$$

(Davenport-Heilbronn, en utilisant les formes cubiques binaires)

Extensions cubiques non-galoisiennes (S_3)

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Sur $\mathbb{Q}$

$$N_{\mathbb{Q},3}(S_3, X) \sim \frac{1}{\zeta(3)} X$$

(Davenport-Heilbronn, en utilisant les formes cubiques binaires)

- Sur K quelconque

$$N_{K,3}(S_3, X) \sim \left(\frac{2}{3}\right)^{r_1-1} \left(\frac{1}{6}\right)^{r_2} \frac{\mathrm{Res}_{s=1}\zeta_K(s)}{\zeta_K(3)} X$$

(Datskovsky-Wright, en utilisant les formes cubiques binaires)

Extensions quartiques et quintiques

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- $G = C_4, V_4$: Baily (sur $\mathbb{Q}$, mais les formules ne sont pas correctes), [CoDiOl] pour K quelconque.

Extensions quartiques et quintiques

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- $G = C_4, V_4$: Baily (sur $\mathbb{Q}$, mais les formules ne sont pas correctes), [CoDiOl] pour K quelconque.
- $G = D_4$: [CoDiOl]

Extensions quartiques et quintiques

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- $G = C_4, V_4$: Baily (sur $\mathbb{Q}$, mais les formules ne sont pas correctes), [CoDiOl] pour K quelconque.
- $G = D_4$: [CoDiOl]
- $G = S_4$ sur $K = \mathbb{Q}$:

$$N_{\mathbb{Q},4}(S_4, X) \sim \frac{5}{6} \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4}\right) X$$

(Bhargava)

Extensions quartiques et quintiques

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- $G = C_4, V_4$: Baily (sur $\mathbb{Q}$, mais les formules ne sont pas correctes), [CoDiOl] pour K quelconque.
- $G = D_4$: [CoDiOl]
- $G = S_4$ sur $K = \mathbb{Q}$:

$$N_{\mathbb{Q},4}(S_4, X) \sim \frac{5}{6} \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4}\right) X$$

(Bhargava)

- $G = S_5$ sur $K = \mathbb{Q}$: [Bh].

Extensions quartiques et quintiques

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- $G = C_4, V_4$: Baily (sur $\mathbb{Q}$, mais les formules ne sont pas correctes), [CoDiOl] pour K quelconque.
- $G = D_4$: [CoDiOl]
- $G = S_4$ sur $K = \mathbb{Q}$:

$$N_{\mathbb{Q},4}(S_4, X) \sim \frac{5}{6} \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4}\right) X$$

(Bhargava)

- $G = S_5$ sur $K = \mathbb{Q}$: [Bh].
- $G = S_4, S_5$, sur K quelconque : Yukie (seulement la conjecture “faible”).

Extensions de type A_4

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

- $G = A_4$, sur K quelconque (inclus $K = \mathbb{Q}$): on n'a toujours pas un résultat complet qui prouve la conjecture de Malle dans ce cas
- Wong en 2005 a prouvé

$$N_{A_4,K}(X) = O(X^{5/6+\varepsilon})$$

- Mais la conjecture de Malle dit:

$$N_{A_4,K}(X) = O(X^{1/2+\varepsilon}).$$

Extensions de type A_4

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

- $G = A_4$, sur K quelconque (inclus $K = \mathbb{Q}$): on n'a toujours pas un résultat complet qui prouve la conjecture de Malle dans ce cas
- Wong en 2005 a prouvé

$$N_{A_4,K}(X) = O(X^{5/6+\varepsilon})$$

- Mais la conjecture de Malle dit:

$$N_{A_4,K}(X) = O(X^{1/2+\varepsilon}).$$

- mais on peut calculer $N_{A_4,K}(X, C_3)$ i.e. on fixe une résolvante cubique (Cohen).

Vers notre problème

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Les extensions de type A_4 avec résolvante cubique fixée ont été traitées. Qu'est-ce qu'on peut dire à propos des extensions cubiques avec une résolvante quadratique fixée?

Vers notre problème

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Les extensions de type A_4 avec résolvante cubique fixée ont été traitées. Qu'est-ce qu'on peut dire à propos des extensions cubiques avec une résolvante quadratique fixée?
- Si l'on compare les formules asymptotiques pour les extensions cubiques avec les tables des extensions cubiques, l'asymptotique convèrge très lentement. Pourquoi?

Vers notre problème

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

- Les extensions de type A_4 avec résolvante cubique fixée ont été traitées. Qu'est-ce qu'on peut dire à propos des extensions cubiques avec une résolvante quadratique fixée?
- Si l'on compare les formules asymptotiques pour les extensions cubiques avec les tables des extensions cubiques, l'asymptotique convèrge très lentement. Pourquoi?
- Une des raisons est que le deuxième terme principal est prévu être en $O(X^{5/6})$, ce qui est grand comparé au terme principal. D'autres raisons peuvent venir de la théorie du corps de classes. Le même phénomène se présente pour les extensions de type A_4 et S_4.

Notre problème

Introduction

Notre problème

Théorie de Kummer (cas particulier)

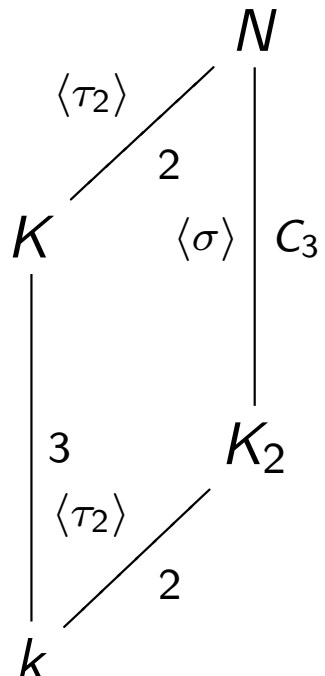
La série de Dirichlet fondamentale

Exemples

Soit k un corps de nombres, K_2 une extension quadratique de k fixée.

On définit $\mathcal{F}(K_2)$ l'ensemble des extensions cubiques K de k (mod $\sim$) telles que la clôture de Galois N contienne K_2.

Si l'on permet $[K_2 : k] = 1$ on peut aussi décrire les extensions cubiques cycliques.



Notre but

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On cherche une formule asymptotique pour

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \leq X\}| \ .$$

Notre but

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On cherche une formule asymptotique pour

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \leq X\}|\ .$$

Mais $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$
et $\mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2$,
on étudie

$$M(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{f}(K/k) \leq X\}|$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

ρ une racine cubique primitive de l'unité

Théorème 1 (M., Cohen)

Soit k un corps de nombres, K_2 une extension de k, $[K_2 : k] \leq 2$. Alors

1. *Si $k = K_2$ et $\rho \in k$ ou $k \neq K_2$ et $\rho \in K_2 \setminus k$, alors*

$$M(K_2/k, X) = C \cdot X(\log(X) + D - 1) + O(X^{\alpha+\varepsilon}), \quad \alpha < 1$$

2. *Dans tous les autres cas*

$$M(K_2/k, X) = C \cdot X + O(X^{\alpha+\varepsilon}), \quad \alpha < 1$$

Les constantes C (et D quand elle est présente) sont explicites et dépendent seulement k et K_2.

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Soit E un corps de nombres, $n > 1$ tel que $\zeta_n \in E$.

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Soit E un corps de nombres, $n > 1$ tel que $\zeta_n \in E$.

- Toutes les extensions cycliques de degré n de E sont de la forme

$$F = E(\sqrt[n]{\alpha}),$$

où $\alpha \in E^*$ est tel que $\overline{\alpha}$ est exactement d'ordre n dans E^*/E^{*n}.

Théorie de Kummer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Soit E un corps de nombres, $n > 1$ tel que $\zeta_n \in E$.

- Toutes les extensions cycliques de degré n de E sont de la forme

$$F = E(\sqrt[n]{\alpha}),$$

où $\alpha \in E^*$ est tel que $\overline{\alpha}$ est exactement d'ordre n dans E^*/E^{*n}.

- $F_1 = E(\sqrt[n]{\alpha_1})$ et $F_2 = E(\sqrt[n]{\alpha_2})$ sont E-isomorphes ssi

$$\alpha_2 = \alpha_1^j \gamma^n,$$

j entier premier avec n, $\gamma \in E^*$.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Soit ρ une racine cubique primitive de l'unité.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Soit ρ une racine cubique primitive de l'unité.
- Pour appliquer la théorie de Kummer on a besoin de considérer les extensions cubiques cycliques N_z/L, où $L = K_2(\rho)$, $N_z = N(\rho)$.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Soit ρ une racine cubique primitive de l'unité.
- Pour appliquer la théorie de Kummer on a besoin de considérer les extensions cubiques cycliques N_z/L, où $L = K_2(\rho)$, $N_z = N(\rho)$.
- Pour simplicité, on va considerer seulement le cas plus général, où $k \neq K_2 \neq L$.

Le cas général

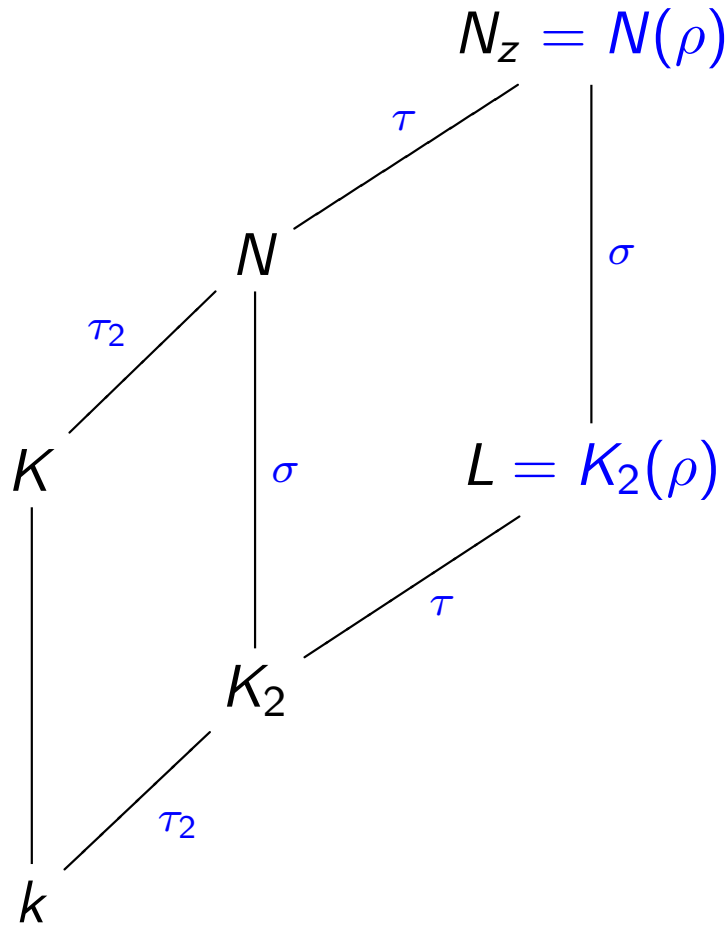
Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples



$$\tau^2 = \tau_2^2 = 1, \quad \tau\tau_2 = \tau_2\tau, \quad \tau\sigma = \sigma\tau, \quad \tau_2\sigma = \sigma^{-1}\tau_2$$

Notation

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On utilisera la notation de l'anneau de groupe $\mathbb{Z}[\mathrm{Gal}(L/k)]$: Pour tout groupe M sur lequel $G = \mathrm{Gal}(L/k)$ agit on note

$$M[\tau + 1] = \{m \in M \mid m\tau(m) = 1\}, \ldots$$

Notation

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On utilisera la notation de l'anneau de groupe $\mathbb{Z}[\mathrm{Gal}(L/k)]$:
Pour tout groupe M sur lequel $G = \mathrm{Gal}(L/k)$ agit on note

$$M[\tau + 1] = \{m \in M \mid m\tau(m) = 1\}, \ldots$$

Enfin on écrit

$$M[\tau + 1, \tau_2 + 1] = M[\tau + 1] \cap M[\tau_2 + 1], \ldots$$

Première bijection

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Proposition 2

Il existe une bijection entre :

- *les éléments de* $\mathcal{F}(K_2)$ *(classes d'isomorphisme d'extensions* K/k *ayant résolvente quadratique isomorphe à* K_2*)* , *et*
- *éléments* $\overline{\alpha} \in \mathcal{L} = (L^*/L^{*3})[\tau+1, \tau_2+1]$, $\overline{\alpha} \neq \overline{1}$, $\alpha \sim \alpha^{-1}$.

Première bijection

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Proposition 2

Il existe une bijection entre :

- *les éléments de* $\mathcal{F}(K_2)$ *(classes d'isomorphisme d'extensions* K/k *ayant résolvente quadratique isomorphe à* K_2*)* , *et*
- *éléments* $\overline{\alpha} \in \mathcal{L} = (L^*/L^{*3})[\tau+1, \tau_2+1]$, $\overline{\alpha} \neq \overline{1}$, $\alpha \sim \alpha^{-1}$.

$$\overline{\alpha} \in \mathcal{L} \Leftrightarrow \begin{cases} \alpha \in L^* \\ \alpha\tau(\alpha) = \gamma^3, \quad \gamma \in L^* \\ \alpha\tau_2(\alpha) = \gamma'^3, \quad \gamma' \in L^* \end{cases}$$

Preuve

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Thèorème de Kummer : $N_z = L(\sqrt[3]{\alpha})$, $\overline{\alpha} \neq \overline{1}$, unique dans (L^*/L^{*3}) mod $\overline{\alpha} \sim \overline{\alpha}^{-1}$

Preuve

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Thèorème de Kummer : $N_z = L(\sqrt[3]{\alpha})$, $\overline{\alpha} \neq \overline{1}$, unique dans (L^*/L^{*3}) mod $\overline{\alpha} \sim \overline{\alpha}^{-1}$
- Soit $\theta^3 = \alpha, \sigma(\theta) = \rho\theta$

Preuve

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Thèorème de Kummer : $N_z = L(\sqrt[3]{\alpha})$, $\overline{\alpha} \neq \overline{1}$, unique dans (L^*/L^{*3}) mod $\overline{\alpha} \sim \overline{\alpha}^{-1}$
- Soit $\theta^3 = \alpha, \sigma(\theta) = \rho\theta$
- $\tau(\rho) = \rho^{-1}$: $\sigma(\theta\tau(\theta)) = \rho\theta\tau(\sigma(\theta)) = \rho\theta\tau(\rho\theta) = \theta\tau(\theta)$ $\Rightarrow \theta\tau(\theta) \in L^* \Rightarrow \alpha\tau(\alpha) \in L^{*3}$ i.e. $\overline{\alpha} \in (L^*/L^{*3})[\tau + 1]$.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Preuve

- Thèorème de Kummer : $N_z = L(\sqrt[3]{\alpha})$, $\overline{\alpha} \neq \overline{1}$, unique dans (L^*/L^{*3}) mod $\overline{\alpha} \sim \overline{\alpha}^{-1}$
- Soit $\theta^3 = \alpha, \sigma(\theta) = \rho\theta$
- $\tau(\rho) = \rho^{-1}$: $\sigma(\theta\tau(\theta)) = \rho\theta\tau(\sigma(\theta)) = \rho\theta\tau(\rho\theta) = \theta\tau(\theta)$ $\Rightarrow \theta\tau(\theta) \in L^* \Rightarrow \alpha\tau(\alpha) \in L^{*3}$ i.e. $\overline{\alpha} \in (L^*/L^{*3})[\tau + 1]$.
- De la même manière on prouve $\overline{\alpha} \in (L^*/L^{*3})[\tau_2 + 1]$.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Preuve

- Thèorème de Kummer : $N_z = L(\sqrt[3]{\alpha})$, $\overline{\alpha} \neq \overline{1}$, unique dans (L^*/L^{*3}) mod $\overline{\alpha} \sim \overline{\alpha}^{-1}$
- Soit $\theta^3 = \alpha, \sigma(\theta) = \rho\theta$
- $\tau(\rho) = \rho^{-1}$: $\sigma(\theta\tau(\theta)) = \rho\theta\tau(\sigma(\theta)) = \rho\theta\tau(\rho\theta) = \theta\tau(\theta)$ $\Rightarrow \theta\tau(\theta) \in L^* \Rightarrow \alpha\tau(\alpha) \in L^{*3}$ i.e. $\overline{\alpha} \in (L^*/L^{*3})[\tau + 1]$.
- De la même manière on prouve $\overline{\alpha} \in (L^*/L^{*3})[\tau_2 + 1]$.
- Donc

$$\overline{\alpha} \in \mathcal{L} = (L^*/L^{*3})[\tau + 1, \tau_2 + 1]$$

Le groupe de Selmer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On définit

$$V_3(L) = \{u \in L^* \mid u\mathbb{Z}_L = \mathfrak{q}^3, \exists \text{ un idéal } \mathfrak{q} \subset L\}$$

le groupe des 3-**unités virtuelles**

Le groupe de Selmer

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On définit

$$V_3(L) = \{u \in L^* \mid u\mathbb{Z}_L = \mathfrak{q}^3, \exists \text{ un idéal } \mathfrak{q} \subset L\}$$

le groupe des 3-**unités virtuelles**

$$S_3(L) = V_3(L)/L^{*3}$$

le 3-**groupe de Selmer**

la bijection fondamentale

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Proposition 3

Il existe une bijection entre $\mathcal{F}(K_2)$ *et les classes d'équivalence de triplets* $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$ *tels que*

1. *Les* $\mathfrak{a}_i$ *sont idéaux entiers, sans facteur carré premiers entre eux de* L *tels que* $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ *et* $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[\tau+1, \tau_2+1]$, *où* I *est le groupe des idéaux fractionnaires de* L.
   On appelera J *l'ensemble de ces couples* $(\mathfrak{a}_0, \mathfrak{a}_1)$
2. $\overline{u} \in \mathcal{S} = S_3(L)[\tau+1, \tau_2+1]$, *et* $\overline{u} \neq 1$ *quand* $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$.

modulo la rélation d'équivalence $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u}) \sim (\mathfrak{a}_1, \mathfrak{a}_0, 1/\overline{u})$

un théorème de Hecke

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Soit F/E une extension cyclique cubique, $F = E(\sqrt[3]{\alpha})$.

Le théorème de Hecke nous donne le conducteur de F/E dans la forme

$$\mathfrak{f}(F/E) = \prod_{\mathfrak{p} \text{ id premier de } E} \mathfrak{p}^{v(\mathfrak{p})}$$

un théorème de Hecke

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Soit F/E une extension cyclique cubique, $F = E(\sqrt[3]{\alpha})$.

Le théorème de Hecke nous donne le conducteur de F/E dans la forme

$$\mathfrak{f}(F/E) = \prod_{\mathfrak{p} \text{ id premier de } E} \mathfrak{p}^{v(\mathfrak{p})}$$

où la valeur des $v(\mathfrak{p})$ dépend seulement des conditions suivantes:

- $\mathfrak{p} \mid 3$ ou pas
- $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 3$ ou pas
- la valeur maximale k pour laquelle la congruence suivante est soluble:

$$x^3 \equiv \alpha \pmod{{}^*\mathfrak{p}^{k+v_{\mathfrak{p}}(\alpha)}}$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Theorem 4

On écrit uniquement $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ *avec* $(\mathfrak{a}_0, \mathfrak{a}_1) \in J$, $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$. *Alors*

$$\mathfrak{f}(N/K_2) = \frac{3\mathfrak{a}_\alpha \prod_{p|3\mathbb{Z}_k} (p\mathbb{Z}_{K_2})^{e(p/3)/2} \prod_{\substack{p|3\mathbb{Z}_k \\ e(\mathfrak{p}/3)\ odd}} (p\mathbb{Z}_{K_2})^{1/2}}{\prod_{\substack{p|3\mathbb{Z}_k \\ p\nmid\mathfrak{a}_\alpha}} (p\mathbb{Z}_{K_2})^{\lceil a_\alpha(p)e(\mathfrak{p}/p)\rceil/e(\mathfrak{p}/p)}}.$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Definition 5

- Si $\mathfrak{a}$ est un idéal de k, on pose $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})$,
- si $\mathfrak{a}$ est un idéal de K_2, on pose $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{a})^{1/[K_2:k]}$.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Definition 5

- Si $\mathfrak{a}$ est un idéal de k, on pose $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})$,
- si $\mathfrak{a}$ est un idéal de K_2, on pose $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{a})^{1/[K_2:k]}$.

Remark

La notation est consistente :
si $\mathfrak{a}$ est un idéal de k

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}\mathbb{Z}_{K_2})$$

La série de Dirichlet fondamentale

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Definition 6

On définit la série de Dirichlet fondamentale, pour $\mathrm{Re}(s) > 1$

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} .$$

La série de Dirichlet fondamentale

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Definition 6

On définit la série de Dirichlet fondamentale, pour $\mathrm{Re}(s) > 1$

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} .$$

Par la bijection fondamentale

$$\Phi(s) = \frac{1}{2} \sum_{(\mathfrak{a}_0, \mathfrak{a}_1) \in J} \sum_{\overline{u} \in \mathcal{S}} \frac{1}{\mathcal{N}(\mathfrak{f}(N/K_2))^s} ,$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Donc grâce au théorème de Hecke,

$$\Phi(s) = \frac{1}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(\mathfrak{p})^{s/2}} \sum_{(\mathfrak{a}_0, \mathfrak{a}_1) \in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s},$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Donc grâce au théorème de Hecke,

$$\Phi(s) = \frac{1}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{s/2}} \sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s},$$

où

$$S_{\alpha_0}(s) = \sum_{\overline{u}\in\mathcal{S}} \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_k \\ \mathfrak{p}\nmid\mathfrak{a}_\alpha}} \mathcal{N}(p)^{\lceil a_{\alpha_0 u}(p) e(\mathfrak{p}/p)\rceil s/e(\mathfrak{p}/p)},$$

Forme finale de la série de Dirichlet

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Après beaucoup de calculs (suites exactes, congruences, groupes de Selmer, inclusion-exclusion...) on obtient la formule finale pour la série de Dirichlet

Theorem 7 (M., Cohen)

On a

$$\Phi(s) = \frac{|(U(L)/U(L)^3)[\tau+1,\tau_2+1]|}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\substack{\mathfrak{p}|3\mathbb{Z}_k,\\ e(\mathfrak{p}/3)\ odd}}\mathcal{N}(\mathfrak{p})^{s/2}}\cdot$$

$$\cdot\sum_{\mathfrak{b}\in\mathcal{B}}\left(\frac{[\mathcal{N}](\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))}\right)^s\frac{P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[\tau+1,\tau_2+1]|}\sum_{\chi\in\widehat{G_{\mathfrak{b}}}}F(\mathfrak{b},\chi,s)\,.$$

Les autres cas

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Cas	type d'ext.	ρ	τ, τ_2	T
1	cyclique	$\rho \in k$	$\tau = \tau_2 = 1$	$\emptyset$
2	cyclique	$\rho \notin k$	$\tau_2 = 1$ $\tau(\rho) = \rho^{-1}$	$T = \{\tau + 1\}$
3	non-cyclique	$\rho \in k$	$\tau = 1$ $\tau_2(\rho) = \rho$	$T = \{\tau_2 + 1\}$
4	non-cyclique	$\rho \in K_2 \setminus k$	$\tau = 1$ $\tau_2(\rho) = \rho^{-1}$	$T = \{\tau_2 - 1\}$
5	non-cyclique	$\rho \notin K_2$	$\tau, \tau_2 \neq 1$ $\tau(\rho) = \rho^{-1}$ $\tau_2(\rho) = \rho$	$T = \{\tau + 1,$ $\tau_2 + 1\}$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

- Dans les cas 2,3 et 5 on expand $\Phi(s)$ autour du pôle $s = 1$

$$\Phi(s) = \frac{C}{(s-1)} + O(1),$$

grâce à un théorème tauberien

$$M(K_2/k, X) = C \cdot X + O(X^{\alpha+\varepsilon}), \quad (\alpha < 1)$$

- Dans les cas 1 et 4 on obtient de façon similaire

$$\Phi(s) = \frac{C}{(s-1)^2} + \frac{C \cdot D}{(s-1)} + O(1), \text{ donc}$$

$$M(K_2/k, X) = C \cdot X(\log(X) + D - 1) + O(X^{\alpha+\varepsilon}), \quad (\alpha < 1)$$

Exemples

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

Extensions cycliques cubiques de $\mathbb{Q}$

Dans ce cas on obtient

$$\sum_{K/\mathbb{Q} \text{ type } C_3} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 3} \left(1 + \frac{2}{p^s}\right),$$

et donc

$$M(\mathbb{Q}, X) = C \cdot X + O(X^{\alpha+\varepsilon}),$$

avec

$$\begin{aligned} C &= \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{2}{p(p+1)}\right) \\ &= 0.158528258396142060283507820357 5\ldots \end{aligned}$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Corps cubiques purs sur $\mathbb{Q}$

Cas (4) : $K_2 = \mathbb{Q}(\rho)$ et $L = K_2$, donc $K/\mathbb{Q}$ est un *corps cubique pur* i. e. $K = \mathbb{Q}(\sqrt[3]{m})$. On obtient

$$\sum_{K/\mathbb{Q} \text{ pure cubic}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p \neq 3} \left(1 + \frac{2}{p^s}\right)$$
$$+ \frac{1}{3} \prod_{p \equiv \pm 1 \pmod 9} \left(1 + \frac{2}{p^s}\right) \prod_{p \not\equiv \pm 1 \pmod 9} \left(1 - \frac{1}{p^s}\right).$$

Introduction
Notre problème
Théorie de Kummer (cas particulier)
La série de Dirichlet fondamentale
Exemples

et donc

$$M(\mathbb{Q}(\sqrt{-3}), X) = C \cdot X \cdot (\log(X) + D - 1) + O(X^{\alpha+\varepsilon}),$$

où

$$C = C(\mathbb{Q}(\sqrt{-3})) = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$
$$= 0.066907733301378371291841632984295\ldots$$
$$D = D(\mathbb{Q}(\sqrt{-3})) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2}$$
$$= 3.450222797830591962790711919671110\ldots,$$

et γ est la constante d'Euler.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

Cas (5) : $K_2 = \mathbb{Q}(\sqrt{\Delta})$ **avec** $\Delta \neq -3$

Il existe une fonction $\phi_\Delta(s)$ holomorphe pour $\mathrm{Re}(s) > 1/2$ telle que

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K)^s} = \phi_\Delta(s) + \frac{3^{r_2(\Delta)}}{6} L_3(s) \prod_{\left(\frac{-3\Delta}{p}\right)=1} \left(1 + \frac{2}{p^s}\right),$$

où

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{si } 3 \nmid \Delta, \\ 1 + 2/3^s & \text{si } \Delta \equiv 3 \pmod 9, \\ 1 + 2/3^s + 6/3^{2s} & \text{si } \Delta \equiv 6 \pmod 9. \end{cases}$$

$r_2(\Delta) = 1$ pour $\Delta < 0$, $r_2(\Delta) = 0$ sinon.

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

On pose $\Delta' = -3\Delta$ si $3 \nmid \Delta$ et $\Delta' = -\Delta/3$ si $3 \mid \Delta$, et on note $\chi_{\Delta'}$ le caractère $\left(\frac{\Delta'}{\cdot}\right)$. Alors si $\Delta \neq -3$ est un discriminant fondamental, pour tout $\varepsilon > 0$ on a

$$M(\mathbb{Q}(\sqrt{\Delta}), X) = C \cdot X + O(X^{\alpha+\varepsilon}),$$

avec

$$C = \frac{3^{r_2(\Delta)} \ell_3 L(\chi_{\Delta'}, 1)}{\pi^2} \prod_{p \mid \Delta'} \left(1 - \frac{1}{p+1}\right) \cdot \prod_{\left(\frac{\Delta'}{p}\right)=1} \left(1 - \frac{2}{p(p+1)}\right), \quad \text{where}$$

$$\ell_3 = \begin{cases} 11/9 & \text{si } 3 \nmid \Delta, \\ 5/3 & \text{si } \Delta \equiv 3 \pmod 9, \\ 7/5 & \text{si } \Delta \equiv 6 \pmod 9. \end{cases}$$

Introduction

Notre problème

Théorie de Kummer (cas particulier)

La série de Dirichlet fondamentale

Exemples

En particulier, si $\Delta < 0$, $3 \nmid h(\Delta)$, on a simplement $\phi_\Delta(s) = -1/2$, donc

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2} L_3(s) \prod_{\left(\frac{-3\Delta}{p}\right)=1} \left(1 + \frac{2}{p^s}\right),$$

Examples 8

$$\sum_{K \in \mathcal{F}(\mathbb{Q}(\sqrt{-1}))} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{\left(\frac{12}{p}\right)=1} \left(1 + \frac{2}{p^s}\right)$$

$$\sum_{K \in \mathcal{F}(\mathbb{Q}(\sqrt{-2}))} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{\left(\frac{24}{p}\right)=1} \left(1 + \frac{2}{p^s}\right)$$

$$\sum_{K \in \mathcal{F}(\mathbb{Q}(\sqrt{-6}))} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{s}}\right) \prod_{\left(\frac{8}{p}\right)=1} \left(1 + \frac{2}{p^s}\right)$$