Les unités cyclotomiques des corps de nombres abéliens

SOUANEF Rafik

Université de Franche-Comté

23 novembre 2024

Introduction - Corps de nombres

Définition

Un corps de nombres est un corps de la forme $\mathbb{Q}(x)$ où $x \in \mathbb{C}$ satisfait $P(x) = 0$ pour un certain polynôme $P \in \mathbb{Q}[X] \setminus \{0\}$.

Introduction - Corps de nombres

Définition

Un corps de nombres est un corps de la forme $\mathbb{Q}(x)$ où $x \in \mathbb{C}$ satisfait $P(x) = 0$ pour un certain polynôme $P \in \mathbb{Q}[X] \setminus \{0\}$.

Remarque

Si P est de degré n, on peut montrer que l'on a

$$\mathbb{Q}(x) = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : (a_0, \ldots, a_{n-1}) \in \mathbb{Q}^n\}.$$

Dans tout ce qui suit, le corps $\mathbb{K}$ est un corps de nombres.

Introduction - Entiers algébriques

Définition

On dit que $x \in \mathbb{C}$ est un entier algébrique s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.
L'anneau des entiers (algébriques) de $\mathbb{K}$ est

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} : x \text{ est un entier algébrique}\}.$$

Introduction - Entiers algébriques

Définition

On dit que $x \in \mathbb{C}$ est un entier algébrique s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.
L'anneau des entiers (algébriques) de $\mathbb{K}$ est

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} : x \text{ est un entier algébrique}\}.$$

Remarque

On peut penser (à tort) que l'on a $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[x]$.

Introduction - Entiers algébriques

Définition

On dit que $x \in \mathbb{C}$ est un entier algébrique s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.
L'anneau des entiers (algébriques) de $\mathbb{K}$ est

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} : x \text{ est un entier algébrique}\}.$$

Remarque

On peut penser (à tort) que l'on a $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[x]$.

Notation

On note $\mathrm{E}(\mathbb{K})$ le groupe des unités de $\mathbb{K}$.

Introduction - Corps de nombres abéliens

Définition

On pose $\exp(2i\pi/n) = \zeta_n$. On dit qu'un corps de nombres $\mathbb{K}$ est abélien s'il existe n tel que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$.

Introduction - Corps de nombres abéliens

Définition

On pose $\exp(2i\pi/n) = \zeta_n$. On dit qu'un corps de nombres $\mathbb{K}$ est abélien s'il existe n tel que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$.

Correction

Le corps de nombres $\mathbb{K}$ est abélien si $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ est abélien.

Dans ce qui suit, le corps $\mathbb{K}$ est supposé abélien.

Motivation - Les unités

Notation

On note $h(\mathbb{K})$ le cardinal du groupe des classes d'idéaux de $\mathbb{K}$.

Motivation - Les unités

Notation

On note $h(\mathbb{K})$ le cardinal du groupe des classes d'idéaux de $\mathbb{K}$.

Théorème (théorème d'Iwasawa)

Le $\Lambda(G)$-module $\mathrm{E}^1_\infty/\mathrm{Was}^1_\infty$ est isomorphe à $\Lambda(G)/I(G).\zeta_p$.

Motivation - Les unités

Notation

On note $h(\mathbb{K})$ le cardinal du groupe des classes d'idéaux de $\mathbb{K}$.

Théorème (théorème d'Iwasawa)

Le $\Lambda(G)$-module $\mathrm{E}^1_\infty/\mathrm{Was}^1_\infty$ est isomorphe à $\Lambda(G)/I(G).\zeta_p$.

Théorème (des unités de Dirichlet)

Le groupe $\mathrm{E}(\mathbb{K})$ est isomorphe au produit de $\mu(\mathbb{K})$ et d'un groupe abélien libre de rang $r_1 + r_2 - 1$ où r_1 désigne le nombre de plongements réels de $\mathbb{K}$ et r_2 désigne le nombre de plongements complexes de $\mathbb{K}$ à conjugaison près.

Les unités cyclotomiques

Histoire

C'est Kummer qui a eu l'idée de regarder un sous-groupe de $\mathrm{E}(\mathbb{Q}(\zeta_p))$ pour approximer ce dernier groupe. Il a remarqué que l'indice ce sous-groupe était égal à $h(\mathbb{Q}(\zeta_p) \cap \mathbb{R})$.

Les unités cyclotomiques

Histoire

C'est Kummer qui a eu l'idée de regarder un sous-groupe de $\mathrm{E}(\mathbb{Q}(\zeta_p))$ pour approximer ce dernier groupe. Il a remarqué que l'indice ce sous-groupe était égal à $h(\mathbb{Q}(\zeta_p) \cap \mathbb{R})$.

Définition

On pose $\mathcal{C}_n$ le groupe abélien (loi multiplicative) engendré par les racines de l'unité de $\mathbb{Q}(\zeta_n)$ et les $1 - \zeta_d^a$ pour $d \mid n$ et $a \in \mathbb{Z}$. On pose $\mathrm{Was}(\mathbb{K}) = \mathrm{E}(\mathbb{K}) \cap \mathcal{C}_n$.