Base du groupe des unités cyclotomiques de Washington pour certains corps

SOUANEF Rafik

Université de Franche-Comté

29 septembre 2024

Introduction

Notations

Dans tout ce qui suit, on note $\mathbb{K}$ un corps de nombres abélien.
On note $\mathrm{E}(\mathbb{K})$ le groupe des unités de $\mathbb{K}$.
On note $h(\mathbb{K})$ le cardinal du groupe des classes d'idéaux de $\mathbb{K}$.
On note $\zeta_n = \exp(2i\pi/n)$.

Théorème

Soit k une extension finie de $\mathbb{Q}_p$. Soit K/k une extension abélienne finie. On a

$$\mathrm{E}(\mathrm{k})/\,\mathrm{N}_{\mathrm{K}/\mathrm{k}}\,\mathrm{E}(\mathrm{K}) \simeq \mathrm{Gal}(\mathrm{K}/\mathrm{k})_0.$$

Introduction - Les unités

Théorème

Soit k une extension finie de $\mathbb{Q}_p$. Soit K/k une extension abélienne finie. On a

$$\mathrm{E}(\mathrm{k})/\,\mathrm{N}_{\mathrm{K}/\mathrm{k}}\,\mathrm{E}(\mathrm{K}) \simeq \mathrm{Gal}(\mathrm{K}/\mathrm{k})_0.$$

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.

Introduction - Les unités cyclotomiques

Histoire

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

Introduction - 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 $h^+(\mathbb{Q}(\zeta_p))$.

Théorème

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

Unités cyclotomiques

Définition

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

Définition

On note $\mathrm{Sin}(\mathbb{K})$ l'intersection de $\mathrm{E}(\mathbb{K})$ avec le module galoisien engendré par les racines de l'unité de $\mathbb{K}$ et les

$$\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{K}\cap\mathbb{Q}(\zeta_d)}(1 - \zeta_d).$$

Unités cyclotomiques

Proposition

Le groupe $\mathrm{Sin}(\mathbb{K})$ est engendré par :
-les racines de l'unité de $\mathbb{K}$
-les $\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{K}\cap\mathbb{Q}(\zeta_d)}(1-\zeta_d^a)$ avec $d \mid n$ tel que d soit composé et $d \wedge (n/d) = 1$ et $a \wedge d = 1$
-les $\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{K}\cap\mathbb{Q}(\zeta_d)}(1-\zeta_d/1-\zeta_d^a)$ avec d une puissance d'un nombre premier divisant n, vérifiant $d \wedge (n/d) = 1$ et $a \wedge d = 1$.

Unités cyclotomiques

Théorème (Sinnott, 1980/1981)

Les groupes $\mathrm{Was}(\mathbb{K})$ et $\mathrm{Sin}(\mathbb{K})$ sont d'indice fini dans $\mathrm{E}(\mathbb{K})$ (et ce sont des groupes abéliens de type fini, de rang $r_1 + r_2 - 1$). On a

$$[\mathrm{E}(\mathbb{K}) : \mathrm{Sin}(\mathbb{K})] \longleftrightarrow h^+(\mathbb{K}).$$

Unités cyclotomiques

Théorème (Sinnott, 1980/1981)

Les groupes $\mathrm{Was}(\mathbb{K})$ et $\mathrm{Sin}(\mathbb{K})$ sont d'indice fini dans $\mathrm{E}(\mathbb{K})$ (et ce sont des groupes abéliens de type fini, de rang $r_1 + r_2 - 1$). On a

$$[\mathrm{E}(\mathbb{K}) : \mathrm{Sin}(\mathbb{K})] \longleftrightarrow h^+(\mathbb{K}).$$

Attention

Dans la suite, on quotiente ces groupes par celui des racines de l'unités.

Unités cyclotomiques

Théorème (Sinnott, 1980/1981)

Les groupes $\mathrm{Was}(\mathbb{K})$ et $\mathrm{Sin}(\mathbb{K})$ sont d'indice fini dans $\mathrm{E}(\mathbb{K})$ (et ce sont des groupes abéliens de type fini, de rang $r_1 + r_2 - 1$). On a

$$[\mathrm{E}(\mathbb{K}) : \mathrm{Sin}(\mathbb{K})] \longleftrightarrow h^+(\mathbb{K}).$$

Attention

Dans la suite, on quotiente ces groupes par celui des racines de l'unités.

Théorème (Gold et Kim, 1989, Kucera, 1991/1992)

Dans le cas $\mathbb{K} = \mathbb{Q}(\zeta_n)$, une <u>base</u> de $\mathrm{Was}(\mathbb{Q}(\zeta_n)) = \mathrm{Sin}(\mathbb{Q}(\zeta_n))$ a été explicitée.

Mon travail

Proposition

Soit $\mathbb{K}$ un corps de nombres de nombres abélien. Soit $(x_1, \ldots, x_r)$ une $\mathbb{Z}$-base de $\mathrm{Was}(\mathbb{K})$. Quitte à renuméroter les x_i, on suppose, pour un certain $r' \in [\![0; r]\!]$, que $x_1, \ldots, x_{r'}$ sont d'ordre 2 dans le quotient $\mathrm{E}(\mathbb{K})/\mu(\mathbb{K})\mathrm{E}^+(\mathbb{K})$ et que $x_{r'+1}, \ldots, x_r$ sont d'ordre 1. Alors, la famille $(|x_1||x_1|, \ldots, |x_1||x_{r'}|, |x_{r'+1}|, \ldots, |x_r|)$ est une base de $\mathrm{Was}(\mathbb{K}^+)$.

Corps totalement déployés

Définition

Supposons $\mathbb{K}$ de conducteur $n = \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{r} q_i$. On dit que $\mathbb{K}$ est totalement déployé si

$$\mathbb{K} = \mathbb{K}_1 \cdots \mathbb{K}_r$$

où $\mathbb{K}_i$ est un sous-corps de $\mathbb{Q}(\zeta_{q_i})$.

Remarque

Certains cas sont traités dans
-Werl, Milan "On bases of Washington's group of circular units of some real cyclic number fields", JNT, 2014
-Kučera, Radan "The circular units and the Stickelberger ideal of a cyclotomic field revisited", Acta Arith., 2016

Mon travail

Théorème

Si $\mathbb{K}$ est totalement déployé, alors $\mathrm{Was}(\mathbb{K})$ est un facteur direct de $\mathrm{Was}(\mathbb{Q}(\zeta_n))$ et on sait expliciter une base de $\mathrm{Was}(\mathbb{K})$.

Mon travail

Théorème

Si $\mathbb{K}$ est totalement déployé, alors $\mathrm{Was}(\mathbb{K})$ est un facteur direct de $\mathrm{Was}(\mathbb{Q}(\zeta_n))$ et on sait expliciter une base de $\mathrm{Was}(\mathbb{K})$.

Corollaire

Soient $A_1, \ldots, A_k$ des parties disjointes de $[\![1, r]\!]$.
En notant $h_p^+(\mathbb{K})$ la p-partie du nombre de classes de $\mathbb{K}^+$, on a, pour tout p premier impair

$$\prod_{j=1}^{k} h_p^+(\mathbb{K}_{A_j}) \mid h_p^+(\mathbb{K}).$$