

PIERRE DAMEY

Extensions cycliques de degré 4, non ramifiées d'un corps quadratiques sur $\mathbb{Q}$

Séminaire de théorie des nombres de Bordeaux (1968-1969), exp. n° 12, p. 1-6

http://www.numdam.org/item?id=STNB_1968-1969____A12_0

© Université Bordeaux 1, 1968-1969, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

EXTENSIONS CYCLIQUES DE DEGRÉ 4 , NON RAMIFIÉES D'UN CORPS QUADRATIQUE SUR $\mathbb{Q}$

par

Pierre DAMEY

-:-:-:-:-

Notation. $m \in \mathbb{Z} \setminus \mathbb{Z}^2$ on pose $k = \mathbb{Q}(\sqrt{m})$
 $\tilde{k} = \mathbb{Q}(\sqrt{-m})$

- $\mathcal{K}$ groupe des classes de k , au sens restreint.
- r_1 (resp. r_2) le nombre de groupes cycliques d'ordre 2 (resp. supérieure ou égale à 2^2) dans la décomposition de $\mathcal{K}$ en produit direct de groupes cycliques .
- Mêmes définitions pour $\tilde{r}_1$ et $\tilde{r}_2$.

Problème : relations entre r_2 et $\tilde{r}_2$.

- Etude des extensions cycliques de degré 4 , non ramifiées du corps k .

Propriété. Ce sont des extensions galoisiennes, non abéliennes de $\mathbb{Q}$.

- D'après la théorie du corps de classe il y a une bijection entre les sous-groupes H du groupe $\mathcal{K}$ dont le quotient $\mathcal{K}/H$ est cyclique de degré 4 et les extensions N non ramifiées, cycliques de degré 4 du corps k .

12-02

Or N galoisien sur $\mathbb{Q} \Leftrightarrow H$ globalement invariant par $\text{Gal}(k/\mathbb{Q})$
puis N non abélienne sur $\mathbb{Q} \Leftrightarrow \text{gal}(k/\mathbb{Q})$ opère non trivialement sur $\mathcal{K}/_H$.

Ici 1) Notons $\overline{\mathfrak{M}}$ le conjugué de l'idéal $\mathfrak{M}$, du corps k ;

$$\text{cl}(\mathfrak{M}) \in H \Rightarrow \text{cl}(\overline{\mathfrak{M}}) \in H \quad \text{car} \quad \text{cl}(\overline{\mathfrak{M}}) = \text{cl}^{-1}(\mathfrak{M}).$$

2) Si $\text{cl}(\mathfrak{M})$ engendre le quotient $\mathcal{K}/_H$, l'égalité

$$\text{cl}(\mathfrak{M})H = \overline{\text{cl}(\mathfrak{M})}H \Rightarrow \text{cl}(\mathfrak{M}^2) \in H,$$

contrarie le fait que $\text{cl}(\mathfrak{M})$ engendre le quotient qui est cyclique de degré 4.

Conséquence. N est une extension non abélienne de $\mathbb{Q}$, galoisienne. Il n'y a que deux cas possibles

1) $\text{Gal}(N/\mathbb{Q})$ isomorphe au groupe du carré

2) $\text{Gal}(N/\mathbb{Q})$ isomorphe au groupe des quaterniens.

Mais dans le cas d'une extension quaternionique, en considérant le groupe d'inertie d'un diviseur premier p ramifié dans k un raisonnement rapide montre que $\mathfrak{P}$ est encore ramifié dans N/k . (cf. Redei und Reichardt: Klassengruppe eines beliebigen quadratischen Zahlkörpers J. für Mathematik Bd 170 Het. 2. 1933).

D'où finalement il ne reste que les extensions carrées de degré 8 sur $\mathbb{Q}$.

Dénombrement de ces extensions non ramifiées

En utilisant le résultat de la théorie du corps des classes, il suffit de compter le nombre de sous-groupe de $\mathcal{K}$, cyclique de degré 4.

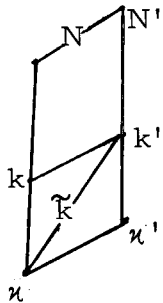
On obtient alors

$2^{r_1+r_2}$ éléments d'ordre 2 ou plus ,

$2^{r_1+2r_2}$ éléments d'ordre 4 ou plus ,

d'où $2^{r_1+r_2-1} 2^{r_2} (2^{r_2}-1)$ sous groupes cycliques d'ordre 4 .

Existence et construction d'extensions carrées sur κ ,
cycliques sur k . (κ corps de caractéristique $\neq 2$).



Idée : On veut utiliser les résolvantes de Lagrange, méthode de Kummer, donc on a besoin des racines 4-ième de l'unité : on les rajoute (éventuellement).

Alors N'/κ est extension carrée (si N et κ' disjoints)

Etude de la réciproque : N'/κ extension carrée peut-on trouver N tel que N/κ soit une extension carrée, cyclique de d° 4 sur k .

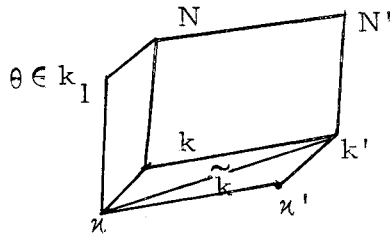
A l'aide du critère de décomposition d'une extension (cf. J. J. Payan, Annales E. N. S. 1/3 , 1968) on peut aboutir au résultat suivant :

L'existence d'une extension carrée N , linéairement disjointe de κ' équivaut à l'existence d'un élément $\alpha \in \tilde{k}$ vérifiant :

$$\alpha \in \tilde{k} , \alpha \notin k'^2 \text{ et } N_{\tilde{k}/\kappa}(\alpha) \in \kappa^4 .$$

Éléments de démonstration :

$$\text{Gal}(N/k) = \{1, \sigma, \sigma^2, \sigma^3\} , \text{Gal}(k/\kappa) = \{1, \tau\} , \text{Gal}(\kappa'/\kappa) = \{1, s\} .$$



Condition nécessaire.

Soit $\theta \in K_1$, corps de degré 4 sur κ tel que N soit le composé de k et de K_1 , avec

$B = \{ \theta, \theta^\sigma, \theta^{\sigma^2}, \theta^{\sigma^3} \}$ base de K_1 sur κ .

Alors B est une base de l'extension N/k , et aussi de l'extension N'/k' .

Posons $\langle \theta, \chi \rangle = \sum_{\sigma} \chi(\sigma^{-1}) \theta^{\sigma}$ (la résolvante de Lagrange).

Alors $\alpha = (\langle \theta, \chi \rangle)^4$ vérifie

$$\left| \begin{array}{l} \alpha \in \tilde{k} \\ \alpha \notin k'^2 \\ N_{\tilde{k}/\kappa}(\alpha) \in \kappa^4 \end{array} \right.$$

Condition suffisante.

En utilisant le critère de décomposition on peut construire un "bon" 2-cocycle ce qui donne une extension diédrale.

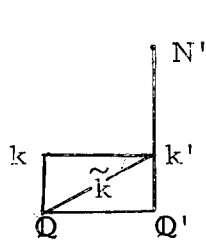
Mieux on obtient deux sous-extensions N et $\hat{N}$.

Etude de la ramification.

$$N \rightarrow \alpha \in \tilde{k} : \alpha \bar{\alpha} = a^4 \Rightarrow \boxed{\alpha = a^2 \frac{\mu}{u} \quad \mu \in \tilde{k}}$$

Alors on obtient l'écriture suivante :

on va décomposer l'idéal (α) de $\tilde{k}$ en produit d'idéaux entiers en isolant la participation de 2 à cet idéal.



$$\alpha \in \tilde{k} : \alpha \notin k'^2 \quad \alpha \alpha^s = a^4 \quad a \in \mathbb{Q}$$

$$\alpha = a^2 \frac{\mu}{\mu^s} \quad \mu \in \tilde{k}$$

$$a \in \mathbb{Q}$$

$$\mu \mu^s \notin k'^2$$

$$(\alpha) = \mathfrak{N}^4 \mathfrak{U} \overline{\mathfrak{U}}^3 \mathfrak{b}^2 \mathfrak{C} \quad \text{avec}$$

- $\mathfrak{U}$ idéal entier de $\tilde{k}$ de norme sans facteur carré et sans facteur ramifié, premier avec 2.
- b entier naturel, sans facteur carré, impair premier avec $N(\mathfrak{U})$
- $\mathfrak{C}$ idéal entier de $\tilde{k}$ sans facteur 4^{ième} puissance et ne comprenant que des facteurs divisant (2).

Remarque : α , -4α , α^3 et $-4\alpha^3$ donne la même extension
 $(-4 = (1+i)^4 \in k'^4)$.

THEOREME. N extension carrée régulière cyclique sur k correspond :

- un entier b impair sans facteur carré, sans facteur ramifié dans $\tilde{k}$
- un couple d'idéaux $(\mathfrak{U}, \overline{\mathfrak{U}})$ conjugués de $O_{\tilde{k}}$, premiers à b, de norme impaire sans facteur carré, ni ramifié.
- un idéal $\mathfrak{C}$ avec soit $\mathfrak{C} = O_{\tilde{k}}$ soit $\mathfrak{C} = q_{\tilde{k}} \overline{q_{\tilde{k}}}^3$ si $(2) = q_{\tilde{k}} \overline{q_{\tilde{k}}}$,
- un couple (resp. 2 couples) de classes d'idéaux conjugués $cl(\mathfrak{M})$ et $cl(\overline{\mathfrak{M}})$, (resp. $cl(\mathfrak{N})$, $cl(\overline{\mathfrak{N}})$, $cl(\overline{q_{\tilde{k}}} \mathfrak{N})$ et $cl(q_{\tilde{k}} \overline{\mathfrak{N}})$) vérifiant $cl(\mathfrak{M}^4) = cl(\mathfrak{U}^2)$ (resp. $cl(\mathfrak{N}^2) = cl(\mathfrak{U}^2) cl(q_{\tilde{k}}^2)$) si $\mathfrak{C} = O_{\tilde{k}}$ (resp. $\mathfrak{C} = q_{\tilde{k}} \overline{q_{\tilde{k}}}^3$) (classes au sens restreint).

Un calcul élémentaire montre que la partie modérée du discriminant de l'extension $N/\mathbb{k}$ est

$$(\Delta_{N/\mathbb{Q}_t}) = b^4 [N_{\tilde{\mathbb{k}}/\mathbb{Q}}(\mathfrak{A})]^6.$$

Pour avoir une extension non ramifiée, il faut donc $b = 1$ et $\mathfrak{A} = (1)$.

Donc $(\alpha) = \mathfrak{N}^4 \mathfrak{C}$ nécessairement.

Pour savoir si on a alors une extension non ramifiée, on utilise les lemmes suivants :

LEMME 1. Si $m = -1(4)$ $N'/\mathbb{k}$, modérément ramifiée $\Leftrightarrow N/\mathbb{k}$ et $N/\mathbb{k}$ modérément ramifiée.

Si $m \neq -1(4)$ $N'/\mathbb{k}$, modérément ramifiée $\Leftrightarrow$ une et une seule des deux, modérément ramifiée.

(La démonstration utilise l'étude des groupes d'inertie (cf. Serre, corps locaux, ch. IV, prop. 2, p. 70).

LEMME 2. Si $\mathfrak{C} \neq \mathcal{O}_{\tilde{\mathbb{k}}}$ $N'/\mathbb{k}$, est sauvagement ramifiée.

A l'aide de ces lemmes, on arrive au résultat suivant :

Si $\mathbb{k} = \mathbb{Q}(\sqrt{m})$ $m > 0$, $\tilde{\mathbb{k}} = \mathbb{Q}(\sqrt{m})$, on a

$$r_2 \leq \tilde{r}_2 \leq r_2 + 1.$$

(On dénombre les classes d'idéaux vérifiant $\text{cl } \mathfrak{N}^4$ principal, et le nombre d'extensions non ramifiées correspondant à un idéal (α) . Ici interviennent les unités).