Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Pierre Damey

Existence et construction des extensions galoisiennes d'un corps de caractéristique $\neq 2$ à groupe de Galois isomorphe au groupe du carré ou au groupe des quaternions

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 2 (1967-1968), exp. n° 18, p. 1-7

<http://www.numdam.org/item?id=SDPP_1967-1968__9_2_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
9e année, 1967/68, n° 18

25 mars 1968

EXISTENCE ET CONSTRUCTION DES EXTENSIONS GALOISIENNES D'UN CORPS DE CARACTÉRISTIQUE $\neq 2$ À GROUPE DE GALOIS ISOMORPHE AU GROUPE DU CARRÉ OU AU GROUPE DES QUATERNIONS

par Pierre DAMEY

Problème. - Etant donné un corps κ de caractéristique différente de 2 , trouver une extension galoisienne N de ce corps, dont le groupe de Galois soit isomorphe au groupe des quaternions, et qui contienne une extension donnée de κ (de degré $\leqslant 4$!) quadratique ou biquadratique.

1. Groupes d'ordre 8 non abéliens.

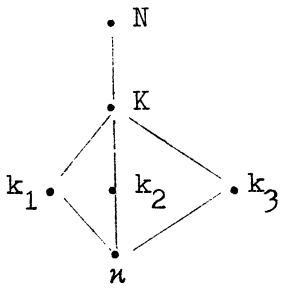
Il y a 5 groupes d'ordre 8 , dont 2 seulement sont non abéliens. Ces 2 groupes sont : le groupe du carré et le groupe des quaternions.

Par générateurs et relations, ils sont donnés ainsi :

- Groupe du carré : $\langle \sigma , \tau \rangle$: $\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma = \sigma^3 \tau$ ou $\tau\sigma = \sigma^{-1} \tau$ (c'est le groupe diédral d'ordre $2n$ avec $n = 4$).
- Groupe des quaternions : $\langle \sigma , \tau \rangle$: $\sigma^4 = 1$, $\tau^4 = 1$, $\tau^2 = \sigma^2$, $\tau\sigma = \sigma^{-1} \tau$.

2. Propriétés. Extension carrée (resp. extension quaternionique).

Soit l'extension N/κ dont le groupe de Galois est isomorphe au groupe du carré (resp. des quaternions).



N/κ carrée (resp. quaternionique). Les sous-corps galoisiens sont : K un biquadratique, et k_1 , k_2 , k_3 3 quadratiques.

- Si N/κ est carrée, N/k_1 est cyclique de degré 4 et N/k_2 et N/k_3 non cycliques (2 , 2) .

- Si $N/\varkappa$ est quaternionique, N/k_i est cyclique de degré 4 pour $i = 1, 2, 3$.

Enfin, ce qui distingue aussi le groupe du carré du groupe des quaternions est que le groupe du carré $\mathfrak{G}$ est un produit semi-direct d'un groupe G cyclique d'ordre 4 par un groupe g cyclique d'ordre 2 (i. e. il existe $\bar{g}$, relèvement de g dans $\mathfrak{G}$).

En termes d'extensions, N carrée est composée de k_1 et de K_1 (invariant de $\langle 1, \tau \rangle$) linéairement disjointes.

3. Résolution du problème.

Historiquement, le problème fut pris sous la forme suivante :

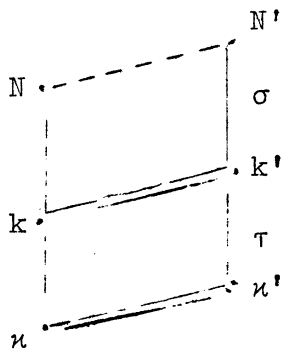
K extension biquadratique de $\varkappa$ est donnée, on cherche N/K quadratique telle que $N/\varkappa$ soit quaternionique ([2] et [3]).

La méthode utilisée ici sera de chercher l'existence et la construction d'extensions N quaternioniques sur $\varkappa$, cycliques de degré 4 sur un corps k donné, extension quadratique de $\varkappa$.

Pour cela nous utiliserons la méthode de Kümmer, par les résolvantes de Lagrange, qui utilise les racines 4-ième de l'unité.

Donc schématiquement, nous rajoutons éventuellement les racines 4-ièmes de l'unité au corps $\varkappa$, et nous cherchons alors les extensions quaternioniques de ce nouveau corps de base (de façon générale, $L' = L(\sqrt{-1})$).

Remarque : $\varkappa'$ et N ne sont pas toujours linéairement disjoints !



Une extension quaternionique N' sera une extension :

- cyclique de degré 4 de k',
- galoisienne sur $\varkappa'$,
- non abélienne sur $\varkappa'$,
- non décomposée par rapport à k'.

La <u>difficulté</u> réside dans la traduction de la décomposition de l'extension N'/ν' .

Nous avons différents cas à étudier provenant du fait que ν' et N sont, ou ne sont pas, linéairement indépendants sur ν :

<u>1er cas</u> : $-1 \in \nu^2$, $\nu' = \nu$.
<u>2e cas</u> : $-1 \notin \nu^2$ et $k = \nu(\sqrt{-1})$, $k = \nu'$.
<u>3e cas</u> : $-1 \notin k^2$ et $-1 \in N^2$, $K = k'$.
<u>4e cas</u> : $-1 \notin N^2$.

Voyons les 1er et 4e cas.

<u>1er cas</u> : $-1 \in \nu^2$.

$$\begin{matrix} k. \\ | \\ \nu. \end{matrix} \quad k = \nu(\sqrt{m}) , \qquad m \in \nu \backslash \nu^2 , \qquad g = \mathrm{Gal}(k/\nu) .$$

$$N/k \begin{Bmatrix} \text{cyclique de degré } 4 \\ \text{galoisienne sur } \nu \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} F \text{ sous-groupe de } k^*/k^{*4} \text{ , cyclique} \\ \text{d'ordre } 4 \text{ invariant par } \mathrm{Gal}(k/\nu) = g \end{Bmatrix}$$

(le symbole $\longleftrightarrow$ est mis pour correspondance biunivoque). Alors g opère sur F .

$$N/\nu \text{ non abélienne} \iff g \text{ opère non trivialement sur } F .$$

g opère sur F , on associe Φ homomorphisme de g dans Aut X (X groupe des caractères de $\mathrm{Gal}(N/k) = G$ à valeurs dans ν) de la façon suivante :

$$\tau \in g = \mathrm{Gal}(k/\nu) , \qquad \chi \in X , \qquad \sigma \in G = \mathrm{Gal}(N/k) ,$$

$$[\Phi(\tau)\chi](\sigma) = [\chi(\sigma^{-1})]^{\tau} \qquad \text{(dans le cas général)} .$$

D'après J. J. PAYAN [1], à partir de Φ et de F uniquement, on sait reconnaître si l'extension N/ν est décomposée (à l'aide d'un 2-cocycle de X^2 à valeurs dans k^*).

Dans le cas présent,

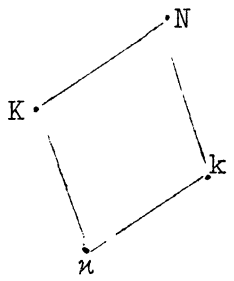
$$\Phi(\tau)\chi = \chi^{-1} .$$

Soit F donné par un système de représentant ; on prend

$$\alpha \in k \backslash k^2 , \qquad F = \{\dot{1} , \dot{\alpha} , \dot{\alpha}^2 , \dot{\alpha}^3\} .$$

$$N/\nu \begin{Bmatrix} \underline{\text{galoisienne}}, \underline{\text{non abélienne}} \\ \underline{\text{cyclique sur}} \ k \end{Bmatrix} \iff \alpha \in k \backslash k^2 \ \underline{\text{et}} \ N_{k/\nu}(\alpha) \in k^4 \quad (\dot{\alpha}^{\tau} = \dot{\alpha}^3) .$$

Extension carrée :



Soit $N/\mathcal{K}$ carrée, cyclique sur k, soit $\bar{\tau}$ un relèvement de τ dans $\mathfrak{G} = \mathrm{Gal}(N/\mathcal{K})$.

Notons K_1 le corps des invariants par $\bar{\tau}$. $\exists\ \theta \in K_1$ tel que les $\mathcal{K}$-conjugués de θ forment une base de N/k.

$\beta_{\chi^x} = \langle \theta , \chi^x \rangle^4$, $\langle \theta , \chi^x \rangle = \sum_{\sigma \in G} \chi^x(\sigma^{-1})\theta^\sigma$, résolvante de Lagrange ; on a

$$(\langle \theta , \chi \rangle)^{\bar{\tau}} = \langle \theta^{\bar{\tau}} , (\Phi(\tau)\chi) \rangle$$
$$= \langle \theta , \Phi(\tau)\chi \rangle = \langle \theta , \chi^{-1} \rangle .$$

Il est immédiat que $\beta_{\chi^x} \in k^*$ $(\langle \theta , \chi \rangle^\sigma = \chi(\sigma)\langle \theta , \chi \rangle)$,

$$F = \{\dot{\beta}_\chi , \dot{\beta}_{\chi^2} , \dot{\beta}_{\chi^3} , \dot{\beta}_{\chi^4}\}$$

convient, et l'on a

$$\beta_\chi^\tau = \beta_{\chi^3} ; \quad N(\beta_\chi) \in \mathcal{K}^{*4} ; \quad \beta_{\chi^2} \in \mathcal{K}^2 ; \quad \beta_{\chi^4} \in \mathcal{K}^4 ; \quad \beta_{\chi^2}/\beta_\chi^2 \in k^4 .$$

Il se trouve que : Inversement, si F est engendré par des éléments vérifiant ces propriétés, alors l'extension N/k associée à F est une extension carrée sur $\mathcal{K}$ (il faut voir qu'elle est décomposée).

THÉORÈME. - $F = \{\dot{1} , \dot{\alpha} , \dot{\alpha}^2 , \dot{\alpha}^3\}$ donne une extension décomposée si, et seulement si,

$$\alpha \in k \setminus k^2 \quad \text{et} \quad N_{k/\mathcal{K}}(\alpha) \in \mathcal{K}^4 .$$

(On prend $\beta_\chi = \alpha$, $\beta_{\chi^3} = \alpha^\tau$, $\beta_{\chi^4} = 1$, et $\beta_{\chi^2} = [a^4(\alpha + \alpha^\tau + 2a^2)]^2$, avec $N_{k/\mathcal{K}}(\alpha) = a^4$.)

On en déduit le théorème suivant, en prenant $(-1 \in \mathcal{K}^2)$:

THÉORÈME. - k extension quadratique de κ , se plonge dans une extension carrée (resp. quaternionique) cyclique sur k , si, et seulement si,

$$\exists\, \alpha \in k\backslash k^2 , \qquad N_{k/\kappa}(\alpha) = a^4 , \quad a \in \kappa .$$

En effet, $k(\sqrt[4]{\alpha})/\kappa$ carrée $\iff$ $k(\sqrt[4]{m\alpha})/\kappa$ quaternionique $(k = \kappa(\sqrt{m}))$, car

$$\begin{Bmatrix} N_{k/\kappa}(\alpha) \in \kappa^4 \\ \alpha \in k\backslash k^2 \end{Bmatrix} \iff \begin{Bmatrix} N_{k/\kappa}(m\alpha) \in k^4\backslash\kappa^4 \\ m\alpha \in k\backslash k^2 \end{Bmatrix} ,$$

puisque N/κ dans les deux cas est galoisienne, non abélienne, cyclique sur k .

Existence :

$$N_{k/\kappa}(\alpha) = a^4 \iff \exists\, \mu \in k^* , \quad \alpha = a^2 \frac{\mu}{\mu^\tau} ,$$

$$\alpha \text{ non carré} \iff \mu\mu^\tau \text{ non carré de } k ;$$

il n'y a existence que si $\exists\, \mu \in k$: $N(\mu) \notin \kappa^2 \cup m\kappa^2$, donc

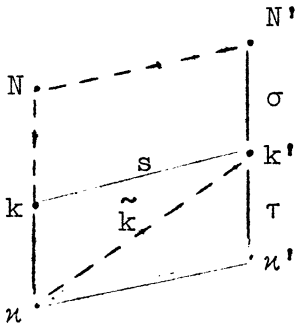
$$\mathrm{Card}(N(k^*)/\kappa^{*2}) > 2 .$$

Sous-corps quadratiques : l'un correspond à

$$\sqrt[2]{\beta}_{\chi^2} \overset{(2)}{\supset} \alpha + \alpha^\tau + 2a^2 \overset{(2)}{=} \mu\mu^\tau .$$

Ce sont k , $\kappa(\sqrt{\mu\mu^\tau})$ et $\kappa(\sqrt{m\mu\mu^\tau})$.

4e cas : $-1 \notin N^2$.



Il est clair que : N/κ carrée (resp. quaternionique) $\Longrightarrow$ N'/κ' carrée (resp. quaternionique).

Inversement : Soit N' une extension cyclique de degré 4 de k' , et notons :

- σ le générateur de $\mathrm{Gal}(N'/k')$,
- s le générateur de $\mathrm{Gal}(k'/k)$,
- τ le générateur de $\mathrm{Gal}(k'/\kappa')$.

THÉORÈME. - N' contient une sous-extension N carrée sur $\varkappa$, cyclique sur k (resp. quaternionique sur $\varkappa$) si, et seulement si :

- N'/$\varkappa$' est carrée sur $\varkappa$' (resp. quaternionique) ;
- N'/k est abélienne décomposée ;
- Un relèvement de s et un relèvement de τ (dans $\mathrm{Gal}(N'/\varkappa)$) commutent.

$$N_1 \text{ invariants de } N' \text{ pour } \langle 1 , \bar{s}\rangle , \qquad N_1 = K(\sqrt{\theta}) ,$$
$$N_2 \text{ invariants de } N' \text{ pour } \langle 1 , \bar{s}\sigma^2\rangle , \qquad N_2 = K(\sqrt{-\theta}) .$$

En explicitant, on arrive à :

Extension carrée (resp. quaternionique), si $\exists\, \alpha \in k'\backslash k'^2$,

$$\alpha\alpha^s = a^4 , \quad a \in k ,$$
$$\alpha\alpha^\tau = b^4 , \quad b \in \varkappa' \qquad (\text{resp. } \alpha\alpha^\tau = m^2 b^4) ,$$
$$aa^\tau = bb^s \qquad (\text{resp. } aa^\tau = mbb^s) .$$

Dans le cas de l'extension carrée, on peut toujours se ramener au cas où $\alpha \in \tilde{k} = x(\sqrt{-m})$ avec $N_{\tilde{k}/\varkappa}(\alpha) \in \varkappa^4$ et $\alpha \in k'\backslash k'^2$.

Résultats dans le cas où $\varkappa = \mathbb{Q}$: $-1 \notin \mathbb{Q}^2$, et -1 n'est pas somme de carrés dans $\mathbb{Q}$.

- Extensions carrées cycliques sur $\mathbb{Q}' = \mathbb{Q}(\sqrt{-1})$:

$$N = \mathbb{Q}'(\sqrt[4]{\alpha}) , \qquad |\alpha| \in \mathbb{Q}\backslash\mathbb{Q}^2 .$$

- Extensions carrées cycliques sur $k = \mathbb{Q}(\sqrt{m})$, contenant $\mathbb{Q}'$: Condition nécessaire et suffisante d'existence : $-m$, somme de deux carrés de $\mathbb{Q}$ sans être un carré dans $\mathbb{Q}$.

On prend

$$N = K(\sqrt{\alpha}) , \quad \alpha \in \mathbb{Q}' , \qquad N_{\mathbb{Q}'/\mathbb{Q}}(\alpha) = -m .$$

- Extensions carrées linéairement disjointes de $\mathbb{Q}'$: $N(k^*)/\mathbb{Q}^{*2}$ est infini, donc tout corps k se plonge dans une extension carrée, cyclique sur k .

On prend

$$\mu \in \tilde{k} = \mathbb{Q}(\sqrt{-m}) , \quad \text{avec } N_{\tilde{k}/\mathbb{Q}}(\mu) \notin k'^2 = \mathbb{Q}^2(\sqrt{m} , \sqrt{-1}) , \qquad a \in \mathbb{Q}^* .$$

$$N' = k'(\sqrt[4]{\alpha}) , \qquad \alpha = a^2 \frac{\mu}{\mu^s}$$

contient deux extensions, carrées sur $\mathbb{Q}$, cycliques sur k .

- Extensions quaternioniques de Q : $k = \mathbb{Q}(\sqrt{m})$, m quadratfrei, entier.

k se plonge dans une extension quaternionique si, et seulement si, m est somme de trois carrés.

Soit

$$m > 0 , \qquad m \not\equiv -1(8) .$$

Construction :

$$m = p^2 + q^2 + r^2 , \qquad u = p + \sqrt{m} , \qquad v = r + s\sqrt{-1} ;$$

$$\alpha = mu^2 \frac{v}{v^s} a^2 \frac{\lambda}{\lambda^s} , \qquad a \in \mathbb{Q} , \quad \lambda \in \tilde{k} , \quad \lambda\lambda^s vv^s \notin k'^2 .$$

Les sous-corps quadratiques sont $\mathbb{Q}(\sqrt{\lambda\lambda^s vv^s})$ et $\mathbb{Q}(\sqrt{m\lambda\lambda^s vv^s})$.

L'étude des propriétés arithmétiques de ces extensions $N/\mathbb{Q}$ non abéliennes, des extensions non ramifiées, et le calcul du discriminant de $N/\mathbb{Q}$ sont en cours.

L'ensemble de ce travail sera publié ultérieurement. Il est effectué en commun avec J. J. PAYAN [1].

BIBLIOGRAPHIE

[1] PAYAN (J. J.). - Le critère de décomposition d'une extension sur un sous-corps du corps de base (à paraître).

[2] ROSENBLÜTH (Emanuel). - Die arithmetische Theorie und die Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage, Monatsh. für Math., t. 41, 1934, p. 85-125.

[3] WITT (Ernst). - Theorie der quadratischen Formen in beliebigen Körpern, J. für die reine und angew. Math., t. 176, 1937, p. 31-44.