Séminaire Dubreil.
Algèbre et théorie
des nombres

Jean-Jacques Payan

Construction des corps abéliens de degré 5

Séminaire Dubreil. Algèbre et théorie des nombres, tome 15, n° 2 (1961-1962), exp. n° 18, p. 1-8

<http://www.numdam.org/item?id=SD_1961-1962__15_2_A7_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
15e année, 1961/62, n° 18

7 mai 1962

CONSTRUCTION DES CORPS ABÉLIENS DE DEGRÉ 5

par Jean-Jacques PAYAN

On se propose dans ce qui suit de construire les corps abéliens de degré 5 sur Q en introduisant une racine cinquième d'un nombre convenablement choisi dans le corps des racines cinquièmes de l'unité. Cette méthode est une généralisation de celle utilisée par A. CHÂTELET dans l'étude des corps abéliens de degré 3 ([1], p. 117-127).

1. Quadruplets canoniques et idéaux essentiels.

On notera $C(5)$ le corps engendré par une racine cinquième de l'unité ε_k non réelle $(\varepsilon_k = e^{2ik\pi/5})$. Les ε_k $(k = 1, 2, 3, 4)$ forment une base des entiers de $C(5)$. Le groupe de Galois de $C(5)$ est formé de 4 éléments notés $[i]$, définis par $[i]\,\varepsilon_k = \varepsilon_{ik}$, i premier avec 5 modulo 5. Ce groupe est isomorphe au groupe multiplicatif des entiers mod 5 premiers avec 5. Il possède un sous-groupe non banal formé des éléments $[1]$ et $[4]$, sous-groupe auquel correspond le sous-corps quadratique réel de $C(5)$ de discriminant 5. On notera α_j l'image de α par $[j]$ et en particulier $[1]\,\alpha = \alpha_1$.

Propriétés arithmétiques de $C(5)$. - Les unités de $C(5)$ forment un groupe multiplicatif infini dont les éléments sont de la forme $(-\varepsilon_1)^x \eta^y$ avec x défini mod 10 et $y \in Z$, η étant une unité réelle convenable (par exemple $(1 + \sqrt{5})/2$).

Si p est un nombre premier rationnel, l'idéal (p) se décompose de la façon suivante :

$p \equiv \pm 2 \mod 5$ $\quad$ (p) indécomposable de norme p^4

$p \equiv -1 \mod 5$ $\quad$ $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ avec $\mathfrak{p}_1 \neq \mathfrak{p}_2$ et de norme commune p^2

$p \equiv +1 \mod 5$ $\quad$ $(p) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4$ avec $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\forall\ i \neq j$

la norme commune étant égale à p

$p = 5$ alors $(5) = (\varepsilon_1 - 1)^4$.

Les corps $C(5)$ et $Q(\sqrt{5})$ étant tous deux à idéaux principaux, on peut énoncer les propriétés précédentes à l'aide des nombres premiers bases des idéaux premiers correspondants.

Quadruplet canonique. - On appellera quadruplet canonique un système de 4 entiers conjugués $\|\alpha_1 , \alpha_2 , \alpha_3 , \alpha_4\|$ de $C(5)$ premiers entre eux deux à deux et sans facteur carré.

On peut alors énoncer : un quadruplet d'entiers conjugués est canonique si et seulement si leur norme commune est sans facteur carré et première avec 5 .

Nous serons amenés à considérer également que $\|\varepsilon_i , \varepsilon_{2i} , \varepsilon_{3i} , \varepsilon_{4i}\|$, i premier avec 5 , est un quadruplet canonique.

Idéaux essentiels [(2)]. - On appellera idéal essentiel un idéal $\mathfrak{I}$ de $C(5)$ vérifiant la propriété suivante :

(a) $\forall$ i défini mod 5 , premier avec 5 , $\mathfrak{I}_1^i \mathfrak{I}_i^{-1} = \mathfrak{B}_{1,i}^5$ où $\mathfrak{B}_{1,i}$ est un idéal de $C(5)$.

Pour déterminer la forme des idéaux essentiels de $C(5)$, on écrit

$$\mathfrak{I} = \prod_{j=1}^{n} \mathfrak{L}_j$$

avec $N(\mathfrak{L}_j) = p_j^{m_j}$ où p_j est un nombre premier rationnel, il suffit alors d'examiner les facteurs $\mathfrak{L}_j$.

$$\mathfrak{L}_j = \prod_{i=1}^{4} P_i^{h(i)} \quad ,$$

les idéaux P_i étant des idéaux premiers de norme multiple de p_j . La condition (a) donne $ih(i) \equiv c \mod 5$. En rassemblant ces résultats on voit que

$$\mathfrak{I} = (\lambda^5 \alpha_1 \quad \alpha_2^3 \quad \alpha_3^2 \quad \alpha_4^4)$$

avec $\lambda \in C(5)$ et $\|\alpha_1 , \alpha_2 , \alpha_3 , \alpha_4\|$ quadruplet canonique.

Si $\alpha_1 = \varepsilon_i$, $\mathfrak{I}$ est puissance cinquième d'un idéal de $C(5)$; si $\lambda = 1$, $\mathfrak{I}$ sera appelé idéal essentiel canonique.

2. Équation abélienne de degré 5.

Soit $P \in Q[x]$ abélien de degré 5, il est également irréductible sur $C(5)$. Si on note θ_1, θ_2, θ_3, θ_4, θ_5 les zéros de P en les numérotant convenablement, les transformations du groupe de Galois de $Q(\theta_i)$ sont σ, σ^2, σ^3, σ^4 et σ^5 = identités, avec $\sigma(\theta_u) = \theta_{u+1}$.

Introduisons pour l'étude de P les résolvantes de Lagrange des θ_u, elles sont définies par :

$$\overline{\theta_{u,j}} = \sum_{i \bmod 5} \theta_{u+i}\, \varepsilon_j^i \quad .$$

On peut examiner l'effet des éléments du groupe de Galois de P et de $C(5)$ sur les $\overline{\theta_{u,j}}$.

$$\sigma^h \overline{\theta_{u,j}} = \sum_{i \bmod 5} \theta_{u+h+i}\, \varepsilon_j^i = \overline{\theta_{u+h,j}}$$

$$= \varepsilon_j^{-h} \sum_{i+h \bmod 5} \theta_{u+i+h}\, \varepsilon_j^{i+h} = \varepsilon_j^{-h}\, \overline{\theta_{u,j}} \quad ;$$

$$[k]\, \overline{\theta_{u,j}} = \overline{\theta_{u,jk}} \quad .$$

On peut alors énoncer

THÉORÈME. - Une condition nécessaire et suffisante pour que P, de degré 5, soit abélien est qu'il existe deux quadruplets de nombres conjugués de $C(5)$ $|\lambda_1, \lambda_2, \lambda_3, \lambda_4|$ et $\|\alpha_1, \alpha_2, \alpha_3, \alpha_4\|$ le second étant un quadruplet canonique tel que $\overline{\theta_{u,j}}^2 = \overline{\theta_{u,2j}}\, \lambda_j^2/\lambda_{2j}\, \alpha_{2j}\, \alpha_{4j}$, $\forall\ j = 1, 2, 3, 4$.

La condition $\overline{\theta_{u,j}}^2 = \overline{\theta_{u,2j}}\, \dfrac{\lambda_j^2}{\lambda_{2j}}\, \alpha_{2j}\, \alpha_{4j}$, $\forall\ j$, est équivalente aux conditions surabondantes

$$\begin{cases} \overline{\theta_{u,j}}^{5} = \lambda_j^5\ \alpha_j\ \alpha_{2j}^3\ \alpha_{3j}^2\ \alpha_{4j}^4 \\ \overline{\theta_{u,j}}\ \overline{\theta_{u,2j}} = \dfrac{\lambda_j\ \lambda_{2j}}{\lambda_{3j}}\ \alpha_{3j}\ \alpha_{4j}\ \overline{\theta_{u,3j}} \\ \overline{\theta_{u,j}}\ \overline{\theta_{u,4j}} = \lambda_j\ \lambda_{4j}\ \alpha_j\ \alpha_{2j}\ \alpha_{3j}\ \alpha_{4j} \quad . \end{cases}$$

Condition nécessaire. - Supposons l'équation abélienne. Considérons alors $\overline{\theta_{u,j}}^{5}$ comme

$$\sigma^h\ \overline{\theta_{u,j}}^{5} = (\varepsilon_j^{-h})^5\ \overline{\theta_{u,j}}^{5} = \overline{\theta_{u,j}}^{5} \quad ,$$

$\overline{\theta_{u,j}}^{5}$ est un élément de $C(5)$; considérons alors l'idéal $\mathfrak{I}$ engendré par $\overline{\theta_{u,1}}^{5}$

$$\mathfrak{I}_1^i\ \mathfrak{I}_i^{-1} = (\overline{\theta_{u,1}}^{5})^i\ (\overline{\theta_{u,i}}^{5})^{-1} = (\overline{\theta_{u,1}}^{5i}\overline{\theta_{u,i}}^{-5})$$

mais

$$\overline{\theta_{u,1}}^{i}\ \overline{\theta_{u,i}}^{-1} \in C(5) \implies \mathfrak{I}_1^i\ \mathfrak{I}_i^{-1} = (\overline{\theta_{u,1}}^{i}\ \overline{\theta_{u,i}}^{-1})^5 \quad .$$

$\mathfrak{I}$ est un idéal essentiel. On peut donc écrire

$$\overline{\theta_{u,1}}^{5} = u_1\ \lambda_1^5\ \alpha_1\ \alpha_2^3\ \alpha_3^2\ \alpha_4^4$$

$\|\alpha_1, \alpha_2, \alpha_3, \alpha_4\|$ étant un quadruplet canonique, $\lambda_1 \in C(5)$ et u_1 étant une unité, mais $u_1 = (-\varepsilon_1)^x\ \eta^y$ en remplaçant éventuellement α_i par $\varepsilon_{4i}^x\ \alpha_i$ et λ_1 par $-\lambda_1$ on peut se ramener à

$$\overline{\theta_{u,1}}^{5} = \eta^{2y}\ \lambda_1^5\ \alpha_1\ \alpha_2^3\ \alpha_3^2\ \alpha_4^4$$

on en déduit

$$\overline{\theta_{u,4}}^{5} = \eta^{2y}\ \lambda_4^5\ \alpha_4\ \alpha_3^3\ \alpha_2^2\ \alpha_1^4 \quad ;$$

soit encore

$$(\overline{\theta_{u,1}}\ \overline{\theta_{u,4}})^5 = \eta^{4y}(\lambda_1\ \lambda_4\ \alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)^5 \quad ;$$

mais $\overline{\theta_{u,1}}\ \overline{\theta_{u,4}} \in C(5)$ d'où

$$4y \equiv 0 \mod 5 \implies y \equiv 0 \mod 5$$

et on peut faire entrer η dans λ_1. On obtient donc

$$\overline{\theta_{u,j}}^5 = \lambda_j^5\ \alpha_j\ \alpha_{2j}^3\ \alpha_{3j}^2\ \alpha_{4j}^4$$

ce qui entraîne

$$\overline{\theta_{u,j}}\ \overline{\theta_{u,4j}} = \lambda_j\ \lambda_{4j}\ \alpha_j\ \alpha_{2j}\ \alpha_{3j}\ \alpha_{4j}$$

et finalement

$$\overline{\theta_{u,j}}^2 = \overline{\theta_{u,2j}}\ \frac{\lambda_j^2}{\lambda_{2j}}\ \alpha_{2j}\ \alpha_{4j} \quad .$$

Condition suffisante. - On se donne la trace s des θ_u et en posant $X = 5\theta_u - s$ et $m = \alpha_1\ \alpha_2\ \alpha_3\ \alpha_4$ on obtient :

$$\begin{cases}
X = \overline{\theta_{u,1}} + \overline{\theta_{u,2}} + \overline{\theta_{u,3}} + \overline{\theta_{u,4}} \\
\overline{X\theta_{u,1}} = \frac{\lambda_1^2}{\lambda_2}\alpha_2\alpha_4\ \overline{\theta_{u,2}} + \frac{\lambda_1\lambda_2}{\lambda_3}\alpha_3\alpha_4\overline{\theta_{u,3}} + \frac{\lambda_1\lambda_3}{\lambda_4}\alpha_2\alpha_4\ \overline{\theta_{u,4}} + \lambda_1\lambda_4\ m \\
\overline{X\theta_{u,2}} = \frac{\lambda_2\lambda_4}{\lambda_1}\alpha_1\alpha_3\ \overline{\theta_{u,1}} + \frac{\lambda_1\lambda_2}{\lambda_3}\alpha_3\alpha_4\overline{\theta_{u,3}} + \frac{\lambda_2^2}{\lambda_4}\alpha_3\alpha_4\ \overline{\theta_{u,4}} + \lambda_2\lambda_3\ m \\
\overline{X\theta_{u,3}} = \frac{\lambda_3^2}{\lambda_1}\alpha_1\alpha_2\ \overline{\theta_{u,1}} + \frac{\lambda_3\lambda_4}{\lambda_2}\alpha_1\alpha_2\ \overline{\theta_{u,2}} + \frac{\lambda_1\lambda_3}{\lambda_4}\alpha_2\alpha_4\ \overline{\theta_{u,4}} + \lambda_2\lambda_3\ m \\
\overline{X\theta_{u,4}} = \frac{\lambda_2\lambda_4}{\lambda_1}\alpha_1\alpha_3\ \overline{\theta_{u,1}} + \frac{\lambda_3\lambda_4}{\lambda_2}\alpha_1\alpha_2\ \overline{\theta_{u,2}} + \frac{\lambda_4^2}{\lambda_3}\alpha_1\alpha_3\ \overline{\theta_{u,3}} + \lambda_1\lambda_4\ m
\end{cases}$$

ces 5 équations linéaires en $\overline{\theta_{u,j}}$ sont compatibles ce qui entraîne

$$\begin{vmatrix} -X & 1 & 1 & 1 & 1 \\ \lambda_1 \lambda_4 m & -X & \frac{\lambda_1^2}{\lambda_2}\alpha_2 \alpha_4 & \frac{\lambda_1 \lambda_2}{\lambda_3}\alpha_3 \alpha_4 & \frac{\lambda_1 \lambda_3}{\lambda_4}\alpha_2 \alpha_4 \\ \lambda_2 \lambda_3 m & \frac{\lambda_2 \lambda_4}{\lambda_1}\alpha_1 \alpha_3 & -X & \frac{\lambda_1 \lambda_2}{\lambda_3}\alpha_3 \alpha_4 & \frac{\lambda_2^2}{\lambda_4}\alpha_3 \alpha_4 \\ \lambda_2 \lambda_3 m & \frac{\lambda_3^2}{\lambda_1}\alpha_1 \alpha_2 & \frac{\lambda_3 \lambda_4}{\lambda_2}\alpha_1 \alpha_2 & -X & \frac{\lambda_1 \lambda_3}{\lambda_4}\alpha_2 \alpha_4 \\ \lambda_1 \lambda_4 m & \frac{\lambda_2 \lambda_4}{\lambda_1}\alpha_1 \alpha_3 & \frac{\lambda_3 \lambda_4}{\lambda_2}\alpha_1 \alpha_2 & \frac{\lambda_4^2}{\lambda_3}\alpha_1 \alpha_3 & -X \end{vmatrix} = 0$$

En développant ce déterminant on obtient :

$$X^5 - 5m(\lambda_1 \lambda_4 + \lambda_2 \lambda_3) X^3 - 5m\Big[\sum_{i=1}^{4} \lambda_i^2 \lambda_{3i} \alpha_{2i} \alpha_{4i}\Big] X^2$$

$$+ 5m\Big[m(\lambda_1^2 \lambda_4^2 + \lambda_2^2 \lambda_3^2 - \lambda_1 \lambda_2 \lambda_3 \lambda_4) - \sum_{i=1}^{4} \lambda_i \lambda_{3i}^3 \alpha_i \alpha_{2i}^2 \alpha_{4i}\Big] X$$

$$- m\Big[\sum_{i=1}^{4} \lambda_i^5 \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 + m \sum_{i=1}^{4} \alpha_i \alpha_{2i}(4\lambda_i \lambda_{3i}^2 \lambda_{4i}^2 + \lambda_{2i} \lambda_{3i}^2 \lambda_{4i}^2 - 4\lambda_{2i} \lambda_{3i}^3 \lambda_{4i}$$

$$- \lambda_i \lambda_{2i} \lambda_{4i}^3)\Big] = 0$$

Les θ_u sont donc zéros d'un polynôme de degré 5..Les relations

$\overline{\theta_{u,j}}^2 \overline{\theta_{u,2j}}^{-1} = \frac{\lambda_j^2}{\lambda_{2j}} \alpha_{2j} \alpha_{4j}$, $\overline{\theta_{u,j}}\ \overline{\theta_{u,4j}} = \lambda_j \lambda_{4j} m$ combinées avec

$$5\theta_u - s = \overline{\theta_{u,1}} + \overline{\theta_{u,2}} + \overline{\theta_{u,3}} + \overline{\theta_{u,4}}$$

montrent que $\overline{\theta_{u,j}}$ est une fraction rationnelle en θ_u à coefficients dans $C(5)$; c'est aussi une fraction rationnelle en $\theta_u + \theta_{u'}$. Si le polynôme précédemment

formé n'était pas irréductible, il aurait soit un zéro dans Q soit deux zéros θ_u et $\theta_{u'}$ dont la somme serait rationnelle. Les résolvantes $\overline{\theta_{u,j}}$ correspondantes seraient des éléments de C(5) et $\overline{\theta_{u,j}}^5$ donc aussi $\alpha_j\ \alpha_{2j}^3\ \alpha_{3j}^2\ \alpha_{4j}^4$ serait une puissance cinquième exacte ce qui est incompatible avec le fait que $||\alpha_1,\alpha_2,\alpha_3,\alpha_4||$ est un quadruplet canonique. Le corps engendré par les $\overline{\theta_{u,j}}$ est normal et abélien, le sous-corps engendré par θ_u est donc aussi abélien.

3. Génération d'un corps abélien de degré 5.

Considérons deux quintuplets $||\theta_u\ ,\ \theta_{u+1}\ ,\ \theta_{u+2}\ ,\ \theta_{u+3}\ ,\ \theta_{u+4}||$ et $||\delta_u\ \delta_{u+1}\ \delta_{u+2}\ \delta_{u+3}\ \delta_{u+4}||$ ordonnés à une permutation circulaire près. Ils appartiennent à un même corps abélien de degré 5 si et seulement si les quadruplets canoniques correspondants $||\alpha_1\ ,\ \alpha_2\ ,\ \alpha_3\ ,\ \alpha_4||$ et $||\beta_1\ ,\ \beta_2\ ,\ \beta_3\ ,\ \beta_4||$ sont associés par des unités réelles $(\alpha_i = u\beta_i)$ avec u unité réelle.

En effet posons

$$\delta_u = a + b\theta_{u+1} + c\theta_{u+2} + d\theta_{u+3} + e\theta_{u+4} \quad ,$$

d'où il vient

$$\overline{\delta_{u,i}} = \overline{\theta_{u,i}}(b\varepsilon_j + c\varepsilon_{2j} + d\varepsilon_{3j} + e\varepsilon_{uj}) \qquad (i.j \equiv 1 \bmod 5) \quad ,$$

et alors

$$\overline{\delta_{u,i}}^5 = \mu_i^5\ \beta_i\ \beta_{2i}^3\ \beta_{3i}^2\ \beta_{4i}^4 = (b\varepsilon_j + c\varepsilon_{2j} + d\varepsilon_{3j} + e\varepsilon_{4j})^5\ \lambda_i^5\ \alpha_i\ \alpha_{2i}^3\ \alpha_{3i}^2\ \alpha^4 \quad ,$$

ce qui entraîne bien $\beta_i = u\alpha_i$ avec u unité réelle. Réciproquement si $\alpha_i = u\beta_i$ alors

$$\overline{\delta_{u,i}}^5 = \gamma_i^5\ \overline{\theta_{u,i}}^5 \quad ,$$

d'où

$$\delta_u = a + b\theta_{u+1} + c\theta_{u+2} + d\theta_{u+3} + e\theta_{u+4} \quad .$$

On voit donc qu'à un corps abélien dont l'ordre des éléments conjugués est fixé à une permutation circulaire près correspond un idéal essentiel canonique. Si on considère les autres ordres des quintuplets tels que les éléments du groupe de

Galois soient encore représentés par des permutations circulaires on obtient les idéaux conjugués.

Réciproquement si on considère un idéal essentiel canonique, il lui correspond 5 corps abéliens obtenus avec les quadruplets $\|\varepsilon_i\ \alpha_1\ ,\ \varepsilon_{2i}\ \alpha_2\ ,\ \varepsilon_{3i}\ \alpha_3\ ,\ \varepsilon_{4i}\ \alpha_4\|$ $i = 0\ ,\ 1\ ,\ 2\ ,\ 3\ ,\ 4$. Il y a un cas d'exception celui où les différents quadruplets $\|\varepsilon_i\ \alpha_1\ ,\ \varepsilon_{2i}\ \alpha_2\ ,\ \varepsilon_{3i}\ \alpha_3\ ,\ \varepsilon_{4i}\ \alpha_4\|$ sont conjugués c'est-à-dire si $\alpha_1 = \varepsilon_j$. A l'idéal essentiel canonique correspondant (l'idéal unité) ne correspond qu'un corps engendré par les racines du polynôme $x^5 - 10\,x^3 + 5\,x^2 + 10\,x + 1$ obtenu pour $\alpha_i = \varepsilon_i$, $\lambda_i = 5$ et une trace nulle.

BIBLIOGRAPHIE

[1] CHÂTELET (Albert). - Arithmétique des corps abéliens du 3e degré ; Ann. scient. Ec. Norm. Sup., t. 63, 1946, p. 109-160.

[2] CHÂTELET (Albert). - Idéaux principaux dans les corps circulaires, Colloques internationaux du C. N. R. S. : Algèbre et Théorie des nombres [24. 1949. Paris ; p. 103-106. - Paris, Centre national de la Recherche scientifique, 1950.

[3] PAYAN (Jean-Jacques). - Construction des corps abéliens de degré 5. - C. R. Acad. Sc. Paris, t. 254, 1962, p. 3618-3620.