Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jacques Martinet

Bases d'entiers des extensions galoisiennes non abéliennes de degré 6 des rationnels

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 2 (1965-1966), exp. n° 21, p. 1-7

<http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A9_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
7e année, 1965/66, n° 21

23 mai 1966

BASES D'ENTIERS DES EXTENSIONS GALOISIENNES NON ABÉLIENNES DE DEGRÉ 6 DES RATIONNELS

par Jacques MARTINET

1. Problèmes abordés dans cet exposé.

Nous considérons un anneau de Dedekind A_k, de corps des fractions k. Si N désigne une extension de k, nous noterons A_N la clôture entière de A dans N. Nous ne considérons pour simplifier que le cas où N est une extension cyclique de k, de degré premier p, et nous supposons que k n'est pas de caractéristique p. Pour un corps L quelconque, L' désigne l'extension de L obtenue en adjoignant à L les racines p-ièmes de l'unité. A partir du § 2, nous nous limitons à $p = 3$. Nous nous proposons d'examiner les problèmes suivants :

PROBLÈME 1. - Donner une description des extensions cycliques de degré p de k (cette description sera faite à l'aide d'idéaux).

PROBLÈME 2. - Etudier les discriminants de ces extensions (plus précisément, trouver le nombre d'extensions de k cycliques de degré p ayant un discriminant donné).

PROBLÈME 3. - Etudier le A_k-module A_N ; dire s'il est libre ; dans ce cas, déterminer une base d'entiers. (Si A_N n'était pas A_k-libre, on pourrait chercher une décomposition de A_N sous la forme d'une somme (directe) de sous-modules :

$$A_N = \lambda_1 A_k + \ldots + \lambda_{p-1} A_k + \lambda_p \mathfrak{A} \qquad \lambda_i \in A_N ,$$

$\mathfrak{A}$ étant un idéal fractionnaire de A_k.)

PROBLÈME 4. - Soit G le groupe de Galois de N/k ; étudier le $A_k[G]$-module A_N. En particulier, donner des conditions assurant que A_N est $A_k[G]$-libre : c'est le problème des bases normales ; si le problème 2 est résolu, on peut alors se prononcer sur l'existence de bases d'entiers (cf. ARTIN, [1]), et savoir si A_N est $A_k[G]$-projectif (ce qui donne une condition nécessaire pour l'existence de bases normales).

2. Méthode du radical.

Nous utilisons une méthode connue sous le nom de "méthode du radical" ou "génération de Kummer" : il est bien connu que, sous nos hypothèses, on obtient N' en adjoignant à k' une racine p-ième d'un nombre de ce corps. Pratiquement, on procède de la façon suivante : soient $G = \{1 , \sigma , \dots , \sigma^{p-1}\}$ les p k'-automorphismes de N' , θ_0 un nombre primitif de N/k , de trace S , $\theta_i = \sigma^i \theta_0$, et j une racine p-ième primitive de l'unité ; on introduit la "résolvante de Lagrange"

$$\theta_{0,j} = \sum_{x \bmod p} j^x \theta_x \quad .$$

$\alpha = (\theta_{0,j})^p$ est un nombre de k' , et $N' = k'(\sqrt[p]{\alpha})$. Nous remarquons que

$$\theta_0 = \frac{1}{p} \left(S + \sum_j \theta_{0,j}\right) \quad ;$$

ainsi, la connaissance des résolvantes et de la trace d'un nombre détermine ce nombre.

On peut étendre l'application de la méthode à des cas plus généraux d'extensions: considérons un sous-corps k_0 de k , tel que k et N soient galoisiens sur k_0 (par exemple, $[k:k_0] = 2$, le groupe de Galois de N/k_0 étant le produit semi-direct de groupes cycliques d'ordre p et 2). Il y a, dans N , p corps conjugués $K_0 , \dots , K_{p-1}$, de degré p sur k_0 (où $K_i = \sigma^i K_0$) ; soit θ_0 un élément primitif de K_0/k_0 , $\theta_i = \sigma^i \theta_0$. On peut encore former les résolvantes

$$\theta_{0,j} = \sum_{x \bmod p} j^x \theta_x \quad .$$

Soit

$$\alpha = (\theta_{0,j})^p \qquad \alpha \in k' \quad .$$

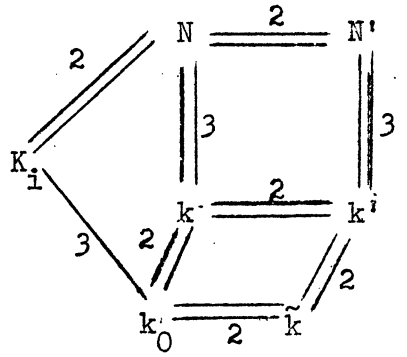
$k_0(\alpha)$ est un sous-corps de k' , noté $\tilde{k}$. On peut se poser les problèmes 1, 2, 3 pour K_0/k_0 ; l'étude se fait alors dans $\tilde{k}$.

3. Idéaux essentiels.

Je suppose maintenant $p = 3$; J.-J. PAYAN et moi-même avons étudié en détail ce cas, lorsque k_0 est le corps Q des rationnels. L'extension des résultats obtenus au cas de p quelconque, le groupe de Galois de N/Q étant le groupe dyhédrique, ne semble présenter que des difficultés techniques non insurmontables.

La situation est décrite par le schéma suivant, dans lequel les traits doubles désignent des extensions galoisiennes. Nous posons

$$\mathbf{A}_{k_0} = \mathbf{A}_k \cap k_0 , \qquad \mathbf{A}_{\tilde{k}} = \mathbf{A}_{k'} \cap \tilde{k} .$$



Remarque. - $[k':k] = 2$ si $j \notin k'$, $[k':k] = 1$ si $j \in k'$. Pour simplifier l'écriture, nous supposerons désormais $[k':k] = 2$.

Nous formons les résolvantes relatives à K_0 (resp. N). Soit θ_0 un élément primitif de K_0 (resp. N), et soit $\alpha = (\theta_{0,j})^3$. $k_0(\alpha) = \tilde{k}$ (resp. $k(\alpha) = k'$). Nous pouvons écrire (de manière unique) l'idéal principal (α) sous la forme

$$(\alpha) = \mathfrak{N}^3 \mathfrak{A}^2 \mathfrak{B} ,$$

où $\mathfrak{A}$ et $\mathfrak{B}$ sont des idéaux de $\mathbf{A}_k$ (resp. de $\mathbf{A}_{k'}$), sans facteurs carrés, premiers entre eux, et où $\mathfrak{N}$ est un idéal fractionnaire de $\mathbf{A}_k$ (resp. de $\mathbf{A}_{k'}$). Etant donné un nombre α de k (resp. de k'), si $N' = k'(\sqrt[3]{\alpha})$, N' doit être abélienne sur k ; cette condition est toujours réalisée si $k' = k$; au contraire, si $[k':k] = 2$, en désignant par un accent la conjugaison dans k (resp. k'), on doit avoir $\alpha^2/\alpha' \in \tilde{k}^3$ (resp. k'^3). On montre alors facilement que $\mathfrak{B} = \mathfrak{A}'$. Les idéaux $\mathfrak{N}$, $\mathfrak{A}$, $\mathfrak{A}'$ sont dits "idéaux essentiels" (cf. A. CHÂTELET, [2]). La donnée du corps N détermine α à la conjugaison près et au produit près par le cube d'un nombre de k (resp. k'), elle détermine donc le couple $(\mathfrak{A}, \mathfrak{A}')$, et, le choix de $\mathfrak{A}$ ayant été fait, la classe de $\mathfrak{N}$. Réciproquement, donnons-nous $\mathfrak{N}$ et $\mathfrak{A}$. Nous devons supposer $\mathfrak{N}^3 \mathfrak{A}^2 \mathfrak{A}'$ principal. Cela n'est pas suffisant en général. En effet, α^2/α' doit être le cube d'un idéal principal ;

$$(\alpha^2/\alpha') = \left[\frac{\alpha}{N(\mathfrak{N})\,N(\mathfrak{A})}\right]^3 ,$$

$N(\ )$ désignant la norme de $\tilde{k}/k_0$ (resp. k'/k). On voit donc que, si k_0 (resp. k) est un corps principal, (α^2/α') est toujours le cube d'un idéal principal. On peut alors écrire $\alpha^2/\alpha' = \varepsilon\lambda^3$, ε étant une unité ; cela s'écrit encore

$$\alpha\alpha' = \varepsilon^{-1}\left(\frac{\alpha}{\lambda}\right)^3 .$$

Donc, si toute unité de k_0 (resp. k) est un cube, ce qui est toujours réalisé si k_0 (resp. k) est le corps $\mathbb{Q}$ des rationnels, on pourrait associer au couple $(\mathfrak{N}, \mathfrak{A})$ un corps, pourvu que le α obtenu ne soit pas un cube.

Supposons maintenant $k_0 = Q$, et $A_{k_0} = Z$, et considérons la décomposition $(\alpha) = \mathfrak{n}^3\,\mathfrak{A}^2\,\mathfrak{A}'$, avec $\alpha \in k^2$. Alors, étant donné un idéal $\mathfrak{A}$, on peut facilement, en fonction du nombre de classes et du nombre d'unités fondamentales de $\tilde{k}$, déterminer le nombre d'extensions associées à un nombre α vérifiant $(\alpha) = \mathfrak{n}^3\,\mathfrak{A}^2\,\mathfrak{A}'$. Le discriminant de K_0/Q est, à une puissance de 3 près, $dN_{k/Q}(\mathfrak{A})^2$, d désignant le discriminant de k/Q. On trouve la puissance de 3 en question en étudiant des congruences dans $\tilde{k}$. On peut alors trouver le nombre de corps cubiques de discriminant donné, et le problème 2 est résolu pour K_0 (pour les détails, voir [3], chapitres I et II).

4. Entiers de K_0.

Soit θ_0 un entier de K_0. $\theta_{0,j}$ est aussi entier ;

$$(\theta_{0,j})^3 = \lambda^3\,\alpha \qquad \lambda \in \tilde{k}\ ,$$

et $(\lambda^3\,\alpha) = (\lambda\mathfrak{n})^3\,\mathfrak{A}^2\,\mathfrak{A}'$ est entier, d'où $\lambda \in \mathfrak{n}^{-1}$.

Réciproquement, si $\lambda \in \mathfrak{n}^{-1}$, il n'existe pas toujours de nombre S tel que $\theta_0 \in K_0$, de trace S, et vérifiant $(\theta_{0,j})^3 = \lambda^3\,\alpha$, soit entier. Néanmoins, on peut prouver le résultat :

Il existe un $\alpha \in \tilde{k}$ et un $\lambda \in \tilde{k}$, tels que 1, λ soit une base du Z-module $\mathfrak{n}^{-1}$, et tels que les nombres φ_0 et ψ_0, vérifiant $(\varphi_{0,j})^3 = \alpha$ ou $3^3\,\alpha$ et $(\psi_{0,j})^3 = \lambda^3\,\alpha$ ou $3^3\,\lambda^3\,\alpha$, construits avec une trace convenable, forment avec 1 une base du Z-module A_{K_0}. La détermination effective des nombres α et λ ayant les propriétés annoncées est faite dans [3], chapitre II, ce qui résoud le problème 3 pour K_0/Q.

5. Entiers de N.

On pourrait étudier les entiers de N en prenant la décomposition $(\alpha) = \mathfrak{n}_1^3\,\mathfrak{A}_1^2\,\mathfrak{A}_1'$, $\mathfrak{n}_1$ et $\mathfrak{A}_1$ étant des idéaux de k'. Il est toutefois plus commode de conserver les notations du § 4 ; il faut alors tenir compte de ce que l'idéal $\mathfrak{A}$ de $\tilde{k}$ peut avoir dans k' des facteurs carrés. Cela ne se produit en fait que pour

$$d \equiv -3 \mod 9\ ,$$

lorsque $\mathfrak{n}$ et 3 ne sont pas premiers entre eux. Ecrivons $3A_k = \mathfrak{P}^2$ si $3 \mid d$, et $\mathfrak{P} = \mathfrak{P}_1\,\mathfrak{P}_1'$ si $d \equiv -3 \mod 9$.

On peut déterminer le discriminant de N/K_0 par une étude locale, et en déduire les discriminants de N/Q, puis de N/k. Le critère d'Artin ([1]) montre alors

que A_N est un A_k-module libre. Pour la recherche de bases de A_N/A_k, on peut alors procéder de la façon suivante : à partir de la base 1, λ du Z-module $\mathfrak{N}^{-1}$, on construit un nombre λ_1 de k', ayant les propriétés suivantes :

si $3 \nmid d$ $\qquad A_{k'} = A_k + \lambda_1 A_k$;

si $3 \mid d$, et $(3, \mathfrak{A}) = (1)$ $\qquad A_{k'} = A_k + \frac{\lambda_1}{3} \mathfrak{P}$;

si $3 \mid d$, et $3 \mid \mathfrak{A}\mathfrak{A}'$ $\qquad \mathfrak{P}_1 \mathfrak{P}_1'^2 A_{k'} = 3A_k + \lambda_1 A_k$.

On peut alors obtenir une base de A_N/A_k du type 1, ω_0, ψ_0, où $\omega_0 \in K_0$, φ et ψ étant déterminés par leur trace, et par $(\omega_{0,j})^3 = \alpha$ ou $3^3 \alpha$, et $(\psi_{0,j})^3 = \lambda_1^3 \alpha$ ou $3^3 \lambda_1^3 \alpha$ (pour les détails, voir [4]).

6. Le $A_k[G]$-module A_N .

Soit L une extension abélienne des rationnels, de degré n, de groupe de Galois G, de discriminant D. On sait que A_L est $Z[G]$-libre si, et seulement si, D et n sont premiers entre eux (voir par exemple le rapport de Hilbert). Ceci peut s'interpréter de la façon suivante : " $(A_L\ Z[G])$-libre" équivaut à " $(A_L\ Z[G])$-projectif". Ce résultat est très particulier au corps des rationnels, et s'obtient à partir du théorème de Kronecker-Weber (ou, directement, par des sommes de Gauss). Pour des extensions cycliques de degré premier, l'expérience prouve qu'il est commode de considérer des bases (que nous appellerons quasi-normales), formées de 1 et de $p - 1$ entiers conjugués. En effet, quand le corps de base est le corps des rationnels, on a toujours des bases de ce type (cf. [5]). De plus, l'existence d'une base normale est subordonnée à l'existence d'une base quasi-normale. Dans le cas qui nous occupe (N est une extension galoisienne non abélienne des rationnels, de degré 6, et k son sous-corps quadratique), on a le théorème suivant.

THÉORÈME. - A_N ne peut admettre de base quasi-normale sur A_k que si les conditions suivantes sont satisfaites :

(i) Les idéaux $\mathfrak{A}$ et $3A_k$ sont premiers entre eux ;
(ii) L'idéal $\mathfrak{N}A_{k'}$ est principal.

De plus, si $3 \nmid d$, (i) est toujours vérifiée, et (ii) est suffisante.

Cela prouve que, contrairement à ce qui se passe pour le corps des rationnels, les extensions cycliques de degré premier d'un corps quadratique n'ont pas toujours

de bases quasi-normales, même si elles sont supposées galoisiennes sur Q, et si A_k est un anneau principal. Si $3|d$, les conditions (i) et (ii) ne sont plus suffisantes pour garantir l'existence de bases quasi-normales : il faut y ajouter des conditions portant sur les unités de k'.

L'existence de bases quasi-normales ne garantit nullement l'existence de bases normales : celles-ci ne peuvent exister que si N/k est modérément ramifiée (ce qui équivaut à A_N est $A_k[G]$-projectif). Mais la condition (ii), jointe à :

(iii) N/k est modérément ramifiée (condition qui entraîne (i)),

n'est pas encore suffisante ; il faut adjoindre à (ii) et (iii) des conditions portant sur les unités de k' (pour les détails, voir [3], chapitre III).

7. Remarques sur le Z-module A_N.

On peut se poser, pour les extensions galoisiennes non abéliennes de degré 6 des rationnels, les problèmes 1, 2, 3 et 4. Le problème 1 est résolu dès qu'il l'est pour les extensions cubiques des rationnels. Nous avons indiqué, au § 5, le calcul des discriminants, ce qui résoud le problème 2.

En ce qui concerne le problème 3, il est immédiat que la connaissance de bases d'entiers de N/k et de k/Q résoud ce problème pour N/Q. Reste le problème 4. On ne peut pas déduire sa solution des résultats des paragraphes précédents. Une condition nécessaire d'existence de bases normales est que N/Q soit modérément ramifiée. Nous ne savons pas si c'est suffisant. Toutefois, en tenant compte de l'examen de cas particuliers, il semble raisonnable de conjecturer que A_N admet toujours des bases normales sur Z.

BIBLIOGRAPHIE

[1] ARTIN (Emil). - Questions de base minimale dans la théorie des nombres algébriques, Colloques internationaux du Centre national de la Recherche scientifique : Algèbre et Théorie des nombres [24. 1949. Paris], p. 19-20. - Paris, Centre national de la Recherche scientifique, 1950.

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

[3] MARTINET (J.) et PAYAN (J.-J.). - Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne, J. für die reine und angew. Math. (à paraître).

[4] MARTINET (J.) et PAYAN (J.-J.). - Sur les bases d'entiers des extensions galoisiennes et non abéliennes de degré 6 des rationnels, J. für die reine und angew. Math. (à paraître).

[5] PAYAN (Jean-Jacques). - Contribution à l'étude des corps abéliens absolus de degré premier impair (Thèse Sc. math. Paris, 1964).