

J. J. PAYAN

Ordres monogènes des corps cycliques de degré premier

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 68-74

http://www.numdam.org/item?id=STNG_1971-1972__1__68_0

© Institut Fourier – Université de Grenoble, 1971-1972, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble 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/>

ORDRES MONOGENES DES CORPS CYCLIQUES DE DEGRE PREMIER

par J.J. PAYAN le 12.4.72

I. RAPPELS ET DEFINITIONS.

Soit K/k une extension de corps de nombres. Notons A_k et A_K les anneaux d'entiers respectifs de k et K . L'existence de θ dans A_K vérifiant $A_K = A_k[\theta]$ -on dira alors que l'ordre maximal A_K est monogène- outre son intérêt "historique" a l'avantage de faciliter considérablement les calculs dans A_K . Cette existence a fait l'objet de nombreux travaux notamment dans le cas $[K:k] = 3$ (voir par exemple [5]). Notons $\Delta(\theta)$ le discriminant d'un θ de K et $N(\theta)$ sa norme relativement à k et posons $\vartheta = w + u\theta + v\theta^2$ avec u, v, w dans k . Un calcul élémentaire montre que $\Delta(\vartheta) = \Delta(\theta)(N(u+vS-v\theta))^2$ où S désigne la trace de θ . On en déduit donc que s'il existe θ tel que $A_K = A_k[\theta]$ les classes modulo A_k de ϑ tels que $A_K = A_k[\vartheta]$ sont en correspondance bijective avec les unités de A_K de la forme $u'+v'\theta$ où $u', v' \in A_k$. Dans le cas $k = \mathbb{Q}$ le théorème de Thue montre qu'il existe un nombre fini au plus de telles classes.

On supposera désormais que K/k est cyclique de degré premier p impair, on posera $\text{Gal } K/k = \langle \sigma \rangle$ et on notera $\Delta_{K/k}$ le discriminant de K/k .

Dans le cas $k = \mathbb{Q}$, $\Delta_{K/k} = (p_1 p_2 \dots p_t)^{p-1}$ où les p_i sont des nombres premiers, deux à deux distincts, vérifiant $p_i \equiv 1 \pmod{p}$ si K/k est modérément ramifiée, et où $p_1 = p^2$ et les p_i premiers deux à deux distincts et $p_i \equiv 1 \pmod{p}$ si K/k est sauvagement ramifiée; on sait que le groupe des classes ambiges est un espace vectoriel de dimension $t-1$ sur F_p et que toute classe ambige contient des idéaux ambiges. Il existe donc une relation de dépendance, modulo les idéaux principaux, entre les idéaux $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ de K ramifiés et une seule au produit près par un élément de F_p^* . [voir [1] et [3] pour des justifi-

cations).

On sait également qu'une condition nécessaire à l'existence d'un θ tel que $A_K = Z[\theta]$ est que tous les nombres premiers q avec $q < p$ soient inertes dans K/\mathbb{Q} (voir [4]).

II. ETUDE DU CAS $k = \mathbb{Q}$.

On pose pour chaque p_i qui apparaît dans $\Delta_{K/k}$, $p_i = p_i^3$. Nous pouvons alors énoncer :

Proposition 1.

Pour qu'il existe θ tel que $A_K = Z[\theta]$ il faut que $p_1 \dots p_t$ soit une norme d'entier pour K/\mathbb{Q} .

Démonstration : On remarque que $A_K = Z[\theta]$ si et seulement si $\Delta(\theta) = (p_1 \dots p_t)^{p-1}$ et que $\Delta(\theta) = N(\delta(\theta))$ où $\delta(\theta)$ désigne la différentielle de θ on en déduit que si $A_K = Z[\theta]$ alors $N(\delta(\theta)) = (p_1 \dots p_t)^{p-1}$ d'où le résultat.

Dans le cas $p = 3$ on peut expliciter ce résultat en utilisant l'écriture $m = \frac{a^2 + 27b^2}{4}$ si K/\mathbb{Q} est modérément ramifiée (resp $m = \frac{a^2 + 3b^2}{4}$ avec $b \neq 0$ (3) si K/\mathbb{Q} est sauvagement ramifiée) avec $m = p_1 \dots p_t$ (resp $m = p_2 \dots p_t$) et K/\mathbb{Q} corps de décomposition du polynôme $X^3 - 3mX - am$. (voir [2] ou [3]).

Proposition 2.

Pour qu'il existe θ avec $A_K = Z[\theta]$ dans le cas $p = 3$ il faut $\frac{p_i - 1}{p_i - 1} a^3 \equiv 1 \pmod{p_i}$ (resp $(3a)^3 \equiv 1 \pmod{p_i}$) pour $i = 2, 3, \dots, t$ si K/\mathbb{Q} est modérément (resp sauvagement) ramifiée.

Démonstration : On exprime que m (resp $3^2 m$) est une norme en utilisant le théorème des normes de Hasse. m est une norme locale pour tous les q premiers avec m . Compte tenu de la formule du produit il reste à écrire que m (resp $3^2 m$) est une norme locale pour tous les p_i avec $i > 1$. Comme am est une norme cela revient à écrire que a (resp $3a$) est une norme pour tous

les p_i avec $i > 1$ d'où la condition.

Remarque 1 :

La condition nécessaire, d'existence de θ tel que $A_K = Z[\theta]$ portant sur la décomposition de 2, à savoir $2Z$ inerte dans K/Q équivaut à a impair.

Remarque 2 :

Si $b^2 = 1$ ou si $a = 1$ dans le cas modérément ramifié, A_K est monogène.

Exemple 1 : La propriété pour A_K d'être monogène ne dépend pas seulement du discriminant de K/Q comme le montre le cas des deux corps cubiques de discriminant $(19.43)^2$. L'un associé à la décomposition $19.43 = \frac{1+27.11^2}{4}$ a un ordre maximal monogène, l'autre est associé à l'écriture

$19.43 = \frac{55^2+27.3^2}{4}$. On voit facilement grâce à la proposition 2 que 19.43 n'est pas une norme donc que A_K n'est pas monogène dans le second cas.

Exemples 2 (dûs à Nicole Moser) A_K peut être monogène en dehors des cas triviaux $b^2 = 1$ et $a = 1$. C'est ainsi que si K est le corps de discriminant $(19.61)^2$ associé à l'écriture $19.61 = \frac{37^2+27.11^2}{4}$, alors

$A_K = Z[\theta]$ où θ est une racine de

$$X^3 + X^2 - 2704 X - 55031 .$$

Si K est le corps de discriminant $(9.1447)^2$ où $1447 = \frac{41^2+337^2}{4}$ alors

$A_K = Z[\theta]$ avec θ racine de

$$X^3 - 21.1447 X + 1409.1447 .$$

Dans le cas $p > 3$ il est beaucoup moins aisé d'expliciter la condition $p_1 \dots p_t$ norme. On obtient cependant un résultat simple concernant la monogénéité de A_K dans le cas sauvagement ramifié.

Théorème 1.

Si $p \geq 5$ et K/Q sauvagement ramifiée A_K n'est pas monogène.

Démonstration : Remarquons d'abord que si $A_K = Z[\theta]$ alors

$(\theta - \sigma^i \theta)A_K = \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_t$ pour $i = 1, 2, \dots, p-1$. Posons $\varphi_i = \theta - \sigma^i \theta$. Il est clair que φ_i / φ_j est une unité de A_K et en particulier

$$\frac{\varphi_2}{\varphi_1} = \frac{\varphi_1 + \sigma \varphi_1}{\varphi_1} = 1 + \frac{\sigma \varphi_1}{\varphi_1}$$

est une unité de A_K . Ecrivons que $N \frac{\varphi_2}{\varphi_1} = \pm 1$.

$$N \frac{\varphi_2}{\varphi_1} = N \left(1 + \frac{\sigma \varphi_1}{\varphi_1}\right) = 1 + N \frac{\sigma \varphi_1}{\varphi_1} + \text{Tr}_{K/Q}(\psi)$$

avec $\psi \in A_K$. K/Q étant sauvagement ramifiée on sait (voir [7] chap. V, §3) que $\text{Tr}_{K/k} \psi \in p\mathbb{Z}$ il en résulte $N \frac{\varphi_2}{\varphi_1} = \pm 1 \equiv 2 \pmod{p}$ ce qui est incompatible avec $p \geq 5$.

Exemple 3 : Ce théorème permet d'exhiber des exemples de corps pour lesquels la "bonne" relation entre les idéaux ambiges est vérifiée, où il n'y a pas de diviseurs communs extraordinaires et où n'existe pas de θ avec $A_K = \mathbb{Z}[\theta]$. C'est notamment le cas pour l'extension cyclique de degré 5 (resp 7) et de conducteur 5^2 (resp 7^2).

La remarque suivante montre qu'il n'y a en revanche pas d'obstruction due au degré dans le cas de ramification modérée.

Remarque 3 :

Si $\ell = 2p+1$ est un nombre premier ce qui se produit pour $p = 3, 5, 11, 19, 23, \dots$ le corps K de discriminant ℓ^{p-1} a un anneau d'entier monogène. Il suffit pour s'en convaincre de remarquer que K est le sous-corps réel maximal de $\mathbb{Q}^{(\ell)}$ et de prendre $\theta = \zeta + \zeta^{-1}$ où ζ est une racine primitive ℓ -ième de l'unité.

III. ETUDE DU CAS QUADRATIQUE IMAGINAIRE.

On supposera que p ne divise pas le nombre de classe de k . On peut alors encore affirmer que le p -groupe des classes ambiges est un F_p -espace vectoriel, sa dimension est égale à $t-1$ (où t désigne encore le nombre de diviseurs premiers de $\Delta_{K/k}$) si $p \geq 5$ ou si $p = 3$ et $k \neq \mathbb{Q}(\sqrt{-3})$. Dans

le cas $p = 3$ et $k = \mathbb{Q}(\sqrt{-3})$, la dimension est $t-1$ ou $t-2$ suivant que les racines cubiques de l'unité sont normes ou pas pour $K/\mathbb{Q}(\sqrt{-3})$.

Commençons par le cas $k = \mathbb{Q}(\sqrt{-3})$ et $p = 3$, on peut alors trouver $\alpha \in A_k^*$, α sans facteur cubique tel que $K = k(\alpha^{1/3})$. On démontre alors (voir [6]).

Proposition 3.

Pour que les racines cubiques de l'unité soient normes pour K/k il faut et il suffit que tous les diviseurs premiers p_i de α distincts du diviseur premier p_0 de 3 vérifient $N_{k/\mathbb{Q}} p_i \equiv 1 \pmod{9}$.

Proposition 4.

Si K/\mathbb{Q} est abélienne et ramifiée en dehors de 3 il y a deux relations de dépendance indépendantes entre les classes d'idéaux ambiges de K/k , l'une est obtenue en écrivant la décomposition de $\alpha^{1/3}$ dans A_K l'autre en étendant à K la relation de dépendance des classes ambiges de K_0/\mathbb{Q} , où K_0 est le sous-corps réel maximal de K . Si tous les nombres premiers q modérément ramifiés dans K/\mathbb{Q} vérifient $q \equiv 1 \pmod{9}$, il existe une classe ambige ne contenant pas d'idéal ambige et les racines primitives cubiques de l'unité sont normes sans être normes d'entiers de K .

La démonstration du théorème 1 s'étend sans difficulté au cas k quadratique imaginaire et on obtient :

Théorème 1 bis.

Si K est une extension cyclique sauvagement ramifiée de degré premier p supérieur à 3 d'un corps quadratique k , A_K n'est pas A_k -monogène sauf peut-être dans les deux cas particuliers suivants :

- a) $p = 5$ et $k = \mathbb{Q}(\sqrt{-1})$
- b) $p = 7$ et $k = \mathbb{Q}(\sqrt{-3})$.

Remarque 4 :

Si on remplace k par un corps de nombres à une infinité d'unités, l'exemple des corps cyclotomiques $\mathbb{Q}^{(p^{\nu+1})}/\mathbb{Q}^{(p^{\nu})}$ montre que la ramification sauvage n'est plus un obstacle à l'existence d'un θ tel que $A_K = A_k[\theta]$.

La remarque suivante nous ramène à des questions de rationalité sur des variétés. (On pourra se reporter à [6] pour un point de vue plus général).

Remarque 5 :

Supposons $k = \mathbb{Q}$, $p = 3$ et la bonne relation de dépendance vérifiée -c'est-à-dire $\mathfrak{P}_1 \dots \mathfrak{P}_t \sim 1$. Notons φ_0 une base de $\mathfrak{P}_1 \dots \mathfrak{P}_t$ et posons

$u_0 = \frac{\sigma \varphi_0}{\varphi_0}$. L'application Φ_{u_0} qui à $\alpha \in A_K$ associe

$$\Phi_{u_0}(\alpha) = \alpha + u_0 \alpha^\sigma + u_0^{1+\sigma} \alpha^{\sigma^2}$$

est \mathbb{Z} -linéaire de rang 1. Son noyau est donc un sous- \mathbb{Z} -module de rang 2 de A_K et A_K sera monogène si et seulement si $\text{Ker } \Phi_{u_0} \cap U_K \neq \emptyset$ (où U_K désigne le groupe des unités de A_K).

Remarque 6 : (Jacques Martinet)

Si toute unité de norme 1 est totalement positive, ce qui entraîne notamment que le nombre de classes de K est pair, alors $\text{Ker } \Phi_{u_0} \cap U_K = \emptyset$.

BIBLIOGRAPHIE

- [1] - C. CHEVALLEY - "Sur la théorie du corps de classes dans les corps finis et dans les corps locaux". Journ. Fac. Sc. Tokyo. 1933, pp. 365-476.
- [2] - G. GRAS - "Sur le ℓ -groupe des classes d'une extension cyclique de degré ℓ ". Sémin. Th. Nombres - Univ. de Grenoble 1971-72.
- [3] - J. MARTINET - "A propos de classes d'idéaux". Sémin. th. Nombres - Univ. de Bordeaux, 1971-72.
- [4] - H. HASSE - "Zahlentheorie". Akad-Verlag Berlin 1963.
- [5] - T. NAGELL - "Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique". Ark. f. Mat. (6) - 1966, pp. 269-289.
- [6] - J.J. PAYAN - "Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur \mathbb{Q} ou sur un corps quadratique imaginaire". A paraître.
- [7] - J.P. SERRE - "Corps locaux". Hermann 1962.
