Sur les classes ambiges et les ordres monogenes d'une extension cyclique de degre premier impair sur $\mathbf{Q}$ ou sur un corps quadratique imaginaire

J. J. PAYAN

I. Rappels et definition

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 est monogène — outre son intérêt »historique», a l'avantage de faciliter considérablement les calculs dans A_K. Cette existence a été étudiée en détail notamment dans le cas $[K : k] = 3$ ou 4 (voir [2] et [9]). C'est ainsi que s'il existe θ tel que $A_K = A_k[\theta]$ et si on pose $S = \mathrm{Tr}_{K/k}\,\theta$, on voit facilement que $\vartheta = u\theta + v\theta^2$, avec $u, v\, A_k$, vérifie $A_K = A_k[\vartheta]$ si et seulement si $u + v(S - \theta)$ est une unité de A_K. Dans le cas $k = \mathbf{Q}$, le théorème de Thue montre alors qu'il existe au plus un nombre fini de classes modulo $\mathbf{Z}$ de θ tels que $A_K = \mathbf{Z}[\theta]$.

Dans ce qui suit, k désignera, sauf mention explicite du contraire, soit le corps $\mathbf{Q}$ des nombres rationnels, soit un corps quadratique imaginaire. On supposera en outre que K/k est cyclique de degré premier impair p et on notera $\Delta_{K/k}$ le discriminant de K/k et σ un générateur de $G = \mathrm{Gal}\, K/k$. On sait que $\Delta_{K/k} = (\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_t)^{p-1}$, où les idéaux $\mathfrak{p}_1 \ldots \mathfrak{p}_t$ sont premiers entre eux deux à deux. En outre si K/k est modérément ramifiée (resp sauvagement ramifiée) les $\mathfrak{p}_i$ sont tous premiers (resp $\mathfrak{p}_1$ ou $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont puissances d'idéaux premiers au-dessus de (p), les autres $\mathfrak{p}_i$ étant premiers).

Notons U_K (resp U_k) le groupe des unités de A_K (resp A_k), $\mathscr{A}_p$ le p-groupe des classes ambiges de K/k, c'est-à-dire des classes invariantes par σ, et $h_{k,p}$ la participation de p au nombre de classes h_k de k.

On sait, voir [3], que

$$\mathrm{Card}\, \mathscr{A}_p = \frac{h_{k,p} \cdot p^{t-1}}{[U_k : U_k \cap N_{K/k}K^*]}$$

et que $U_k \cap N_{K/k}K^* = NU_K$ équivaut à: toute classe ambige est classe d'idéaux ambiges. Ce qui précède montre que si $h_{k,p} = 1$, $\mathscr{A}_p$ est un espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$ de dimension $t - 1 - [U_k : U_k \cap NK^*]$. Si $p \neq 3$ ou si $p = 3$ et $k \neq \mathbf{Q}(\sqrt{-3})$, $U_k = NU_K$; il en résulte qu'il existe une relation de dépendance modulo les idéaux principaux entre les idéaux $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ de K ramifiés dans K/k, et une seule au produit près par un élément de $(\mathbf{Z}/p\mathbf{Z})^*$.

Soit $\theta \in A_K$; l'égalité $A_K = A_k[\theta]$ est vraie si et seulement si le discriminant $\Delta(\theta)$ de θ vérifie $\Delta(\theta) \cdot A_k = \Delta_{K/k}$. Pour qu'un tel θ existe, il faut qu'il n'y ait pas de diviseurs communs extraordinaires des discriminants. Dans le cas $k = \mathbf{Q}$, cette dernière condition est vérifiée si et seulement si tous les nombres premiers q avec $q < p$ sont inertes (voir [6]).

Nous supposerons désormais $h_{k,p} = 1$.

Pour tout $\mathfrak{p}_i$ figurant dans l'écriture de $\Delta_{K/k}$, nous poserons $\mathfrak{p}_i A_K = \mathfrak{P}_i^p$ et nous pouvons énoncer:

Remarque 1. Si A_K est A_k-monogène alors $\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_t \sim 1$.

Il suffit pour s'en convaincre de voir que si $A_K = A_k[\theta]$ alors $N_{K/k}\delta(\theta) = (\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_t)^{p(p-1)}$ où $\delta(\theta)$ désigne la différente de θ. Il en résulte alors $\delta(\theta) = (\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_t)^{p-1}$. (L'écriture $\mathfrak{A} \sim 1$ pour un idéal $\mathfrak{A}$ de A_K significant qu'il est égal, au produit près par un idéal principal, à un idéal de A_k.)

II. Le cas $p = 3$

Si $k = \mathbf{Q}$, $\Delta_{K/Q} = (p_1 p_2 \ldots p_t)^2$ où les p_i sont des nombres premiers vérifiant $p_i \equiv 1$ (3) pour $t = 2, \ldots, t$ et $p_1 \equiv 1(3)$ si K/Q modérément ramifiée, $p_1 = 9$ sinon. On sait (voir par exemple [5]) que K est le corps de rupture du polynôme $X^3 - 3mX - am$ avec $m = p_1 \ldots p_t = (a^2 + 27b^2)/4$ et $a \equiv 1(3)$ dans le cas modérément ramifié, $m = p_2 \ldots p_t = (a^2 + 3b^2)/4$ avec $a \equiv 1(3)$ et $b \not\equiv 0(3)$ si 3 est ramifié.

Nous pouvons alors énoncer:

Proposition 1. *Pour que A_K soit monogène (dans le cas K cyclique de degré* 3 *sur* $\mathbf{Q}$*) il faut $a^{(p_i-1)/3} \equiv 1(p_i)$* (resp $(3a)^{(p_i-1)/3} \equiv 1(p_i)$) *pour $i = 2, 3, \ldots, t$ si K/Q est modérément* (resp *sauvagement*) *ramifiée.*

Démonstration. On exprime que m (resp 3^2m) est une norme en utilisant le théorème de Hasse. m est une norme locale pour tous les q premiers avec m. En utilisant la formule du produit (voir [11]), il reste à écrire que m (resp $9m$) est une norme locale pour tous les p_i avec $i \geq 2$. Cela revient à exprimer, compte tenu de am norme, que a (resp $3a$) est une norme locale pour tous les p_i avec $i \geq 2$ d'où la condition.

Remarque 2. Cette propriété peut s'obetnir à partir des résultats de [5].

Remarque 3. Pour que A_K soit monogène il faut qu'il n'y ait pas de diviseur extraordinaire commun, c'est-à-dire que $2\mathbf{Z}$ soit inerte dans $K/\mathbf{Q}$. On voit facilement que cette condition équivaut à a impair.

Remarque 4. Si $b^2 = 1$ ou si $a = 1$ dans le cas modérément ramifié, A_K est monogène. Ce ne sont pas les seuls cas où A_K est monogène (voir [10] et remarque 7 pour des exemples).

Exemple 1. La propriété pour A_K d'être monogène ne dépend pas seulement du discriminant de $K/\mathbf{Q}$ comme le montre le cas des deux corps cubiques de discriminant $(19\times 43)^2$. L'un associé à la décomposition $19.43 = (1+27\times 11^2)/4$ a un ordre maximal monogène (remarque 4), l'autre est associé à l'écriture $19.43 = (55^2+27.3^2)/4$ et on voit facilement que $55^6 \not\equiv 1(19)$ l'ordre maximal n'est donc pas monogène (prop. 1).

Supposons *maintenant* $k = \mathbf{Q}(\sqrt{-3})$ et notons $\mathfrak{p}_0$ l'idéal premier de A_k qui divise 3. On sait que $K = k(\alpha^{1/3})$ avec $\alpha \in A_k$ et α sans facteur cubique. Nous excluons le cas où $\alpha \in U_k$, c'est-à-dire K corps des racines 9-ièmes de l'unité et nous normaliserons un peu plus le choix de α en supposant d'une part que $\alpha \in \mathfrak{p}_0^2$ de l'autre que αA_k n'est pas le carré d'un idéal.

Nous commencons par énoncer:

PROPOSITION 2. *$U_k = U_k \cap NK^*$ si et seulement si tous les $\mathfrak{p}_i$ distincts de $\mathfrak{p}_0$ qui divisent α vérifient $N_{k/\mathbf{Q}}\mathfrak{p}_i \equiv 1(9)$.*

Démonstration. On exprime que $(-1+\sqrt{-3})/2$ est une norme en utilisant le théorème de Hasse. Comme il y a au plus un diviseur premier sauvagement ramifié la formule du produit des symboles de Hilbert (voir [5] et [10]) montre qu'il suffit d'exprimer que $(-1+\sqrt{-3})/2$ est norme locale pour tous les $\mathfrak{p}_i$ distincts de $\mathfrak{p}_0$. Cette dernière condition équivaut trivialement à $N_{k/\mathbf{Q}}\mathfrak{p}_i \equiv 1(9)$.

La théorie de Kummer (voir par exemple [4]) explicitée dans notre cas particulier [$K = \mathbf{Q}(\sqrt{-3}, \alpha^{1/3})$, α normalisé comme il a été précisé ci-dessus] précise les liens entre $\Delta_{K/k}$ et α.

Posons $\alpha A_k = \mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{p}_{r+1}^2 \ldots \mathfrak{p}_s^2$.

$$\mathfrak{p}_0 \text{ ne divise pas } \alpha \begin{cases} \textit{cas } a & \alpha \equiv \xi^3 \bmod \mathfrak{p}_0^3 \text{ alors } \Delta_{K/k} = (\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s)^2 \\ \textit{cas } b & \alpha \equiv \xi^3 \bmod \mathfrak{p}_0^2 \text{ alors } \Delta_{K/k} = (\mathfrak{p}_0^2\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s)^2 \\ \textit{cas } c & \alpha \equiv \xi^3 \bmod \mathfrak{p}_0 \text{ alors } \Delta_{K/k} = (\mathfrak{p}_0^3\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s)^2 \end{cases}$$

$$\mathfrak{p}_0 = \mathfrak{p}_1 \quad \textit{cas } d \quad \Delta_{K/k} = (\mathfrak{p}_0^4\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s)^2.$$

En écrivant la décomposition de $\alpha^{1/3}A_K$ en produit d'idéaux premiers, on obtient la relation suivante entre les $\mathfrak{P}_i$

$$\text{cas } a, b, c \quad \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_r\mathfrak{P}_{r+1}^2 \ldots \mathfrak{P}_s^2 \sim 1$$
$$\text{cas } d \quad \mathfrak{P}_0\mathfrak{P}_1 \ldots \mathfrak{P}_r\mathfrak{P}_{r+1}^2 \ldots \mathfrak{P}_s^2 \sim 1.$$

Compte tenu de la remarque 1 et de la proposition 1 nous pouvons écrire:

PROPOSITION 3. *Dans les cas c) et d)* $A_K = A_k[\alpha^{1/3}]$ *si* α *sans facteur carré. Si* $U_k = U_k \cap NK^*$, A_K *n'est jamais* A_k*-monogene dans le cas b) et dans les autres cas il est nécessaire que* α *soit sans facteur carré pour que* A_K *soit monogene.*

Terminons cet examen du cas $k = \mathbf{Q}(\sqrt{-3})$ en examinant l'éventualité $K/\mathbf{Q}$ abélienne. On notera alors K_0 l'extension intermédiaire cyclique de degré 3 sur $\mathbf{Q}$. On sait (voir [5]) que $K = \mathbf{Q}(\sqrt{-3})((\beta^2\bar{\beta})^{1/3})$ où β et $\bar{\beta}$ sont des éléments conjugués convenables de A_k. L'ensemble des résultats précédents appliqué à ce cas particulier entraîne:

PROPOSITION 4. *Si* K_0 *est ramifiée en dehors de* 3 *il y a deux relations de dépeendanc indépendantes entre les idéaux ambiges de* K/k*; l'une s'obtient en écrivant la décomposition de* $\alpha^{1/3}$ *dans* A_K*, l'autre en étendant a* K *la relation de dépendance des idéaux ambiges de* $K_0/\mathbf{Q}$*. Si tous les nombres premiers* $q \neq 3$ *ramifiés dans* $K_0/\mathbf{Q}$ *vérifient* $q \equiv 1(9)$ *il existe une classe ambige ne contenant pas d'idéal ambige,* $(-1 + \sqrt{-3})/2$ *est donc norme sans etre norme d'unité.*

III. Le cas $p \geq 5$

Supposons qu'il existe θ tel que $A_K = A_k[\theta]$, on peut alors écrire:

$$\delta(\theta)A_K = A_K \prod_{i=1}^{p-1} (\theta - \sigma^i\theta) = (\mathfrak{P}_1 \ldots \mathfrak{P}_t)^{p-1}$$

en remarquant que $1 - \sigma^i = (1 - \sigma^j)u_{i,j}$ avec $u_{i,j} \in \mathbf{Z}[G]$ et compte tenu de l'unicité de la relation de dépendance on obtient la:

PROPOSITION 5. *Si* $p \geq 5$ *il y a une seule relation de dépendance entre les idéaux ambiges et si* $A_K = A_k[\theta]$ *elle s'écrit* $\mathfrak{P}_1 \ldots \mathfrak{P}_t = (\theta - \sigma^i\theta)A_K$.

Nous sommes maintenant en mesure de démontrer le

THÉOREME. *Si* K/k *est sauvagement ramifiée* A_K *n'est pas* A_k*-monogene sauf peut etre dans les deux cas particuliers suivants:*

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

Démonstration. Supposons $A_K = A_k[\theta]$ et posons $\varphi_i = \theta - \sigma^i\theta$ pour $i = 1, 2, \ldots, p-1$. Il est clair que φ_i/φ_j est dans U_K et en particulier

$$\frac{\varphi_2}{\varphi_1} = \frac{\varphi_1 + \sigma\varphi_1}{\varphi_1} = 1 + \frac{\sigma\varphi_1}{\varphi_1} \in U_K.$$

Ecrivons que $N_{K/k}(\varphi_2/\varphi_2) \in U_k$. K/k étant sauvagement ramifiée en $\mathfrak{p}$, on sait (voir [10] chap. V § 3 lemme 5) que

$$N_{K/k}\left(1 + \frac{\sigma\varphi_1}{\varphi_1}\right) \equiv 1 + \mathrm{Tr}_{K/k}\frac{\sigma\varphi_1}{\varphi_1} + N_{K/k}\frac{\sigma\varphi_1}{\varphi_1} \bmod \mathrm{Tr}_{K/k} A_K$$

d'où $N_{K/k}(\varphi_2/\varphi_1) \equiv 2 \bmod \mathrm{Tr}_{K/k} A_K$, c'est-à-dire $N_{K/k}(\varphi_2/\varphi_1) \equiv 2 \bmod \mathfrak{p}$. Si k distinct de $\mathbf{Q}(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-3})$ on obtient $\pm 1 \equiv 2 \bmod \mathfrak{p}$ ce qui est impossible. Si $k = \mathbf{Q}(\sqrt{-1})$ (resp $k = \mathbf{Q}(\sqrt{-3})$) on a $N_{K/k}\varphi_2/\varphi_1$ racine quatrième (resp sixième) de l'unité. Cela implique $p = 5$ dans le premier cas, $p = 7$ dans le second.

Exemple 2. Ce théorème donne la possibilité d'exhiber facilement des corps pour lesquels la »bonne» relation entre classes ambiges est vérifiée, où il n'y a pas de diviseurs communs extraordinaires et où A_K n'est pas monogène. C'est notamment le cas de l'extension cyclique de degré 5 sur $\mathbf{Q}$ et de conducteur 5^2 et de l'extension cyclique de degré 7 sur $\mathbf{Q}$ et de conducteur 7^2.

La remarque suivante montre qu'il n'y a pas d'obstacle dû au degré dans le cas modéré.

Remarque 5. Si $2p + 1$ est premier, posons alors $2p + 1 = l$, le corps K de discriminant l^{p-1} a un anneau d'entiers monogène. Il suffit pour le voir de remarquer que K est le sous-corps réel maximal de $\mathbf{Q}(\zeta) = \mathbf{Q}^{(l)}$ où ζ racine primitive l-ième de l'unité et de vérifier que $A_K = \mathbf{Z}[\zeta + \zeta^{-1}]$.

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

La propriété suivante indique avec un peu plus de précision la complexité du problème dans le cas modéré:

Proposition 6. *Pour que A_K soit monogene, il faut et il suffit que l'idéal $\mathfrak{P}_1 \ldots \mathfrak{P}_t$ soit principal et possède une base φ vérifiant*

i) $\mathrm{Tr}_{K/k}\varphi = 0$;
ii) *pour* $i = 1, 2, \ldots, (p-3)/2$, $(1 + \sigma + \sigma^2 + \ldots + \sigma^i)\varphi A_K = \mathfrak{P}_1 \ldots \mathfrak{P}_t$.

Démonstration. La condition nécessaire résulte de la proposition 5. Inversement soit φ vérifiant i) et ii): la ramification modérée entraîne $H^1(G, A_K) = 0$ d'où l'existence d'un θ de A_K tel que $\varphi = \theta - \sigma\theta$; la condition ii) entraîne $(\theta - \sigma^{i+1}\theta)A_K = \mathfrak{P}_1 \ldots \mathfrak{P}_t$ pour $i = 1, \ldots, (p-3)/2$. L'égalité $1 - \sigma^j = -\sigma^j(1 - \sigma^{p-j})$ montre alors que $(\theta - \sigma^i\theta)A_K = \mathfrak{P}_1 \ldots \mathfrak{P}_t$ pour $i = 1, 2, \ldots, p-1$ d'où $\Delta(\theta) = (\mathfrak{p}_1 \ldots \mathfrak{p}_t)^{p-1}$.

Remarque 6. Supposons la relation $\mathfrak{P}_1 \ldots \mathfrak{P}_t \sim 1$ vérifiée et notons φ_0 une base de cet idéal et posons $\sigma\varphi_0/\varphi_0 = u_0$, u_0 est une unité de norme 1. On sait que l'application Φ_{u_0} qui à un entier α de K associe

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

est A_k-linéaire de rang 1. Son noyau $\operatorname{Ker}\Phi_{u_0}$ est donc un sous A_k-module de rang $p-1$ de A_K. La condition i) (qui est d'ailleurs la seule dans le cas $p = 3$) est équivalente à $\operatorname{Ker}\Phi_{u_0} \cap U_K \neq \phi$.

Remarque 7 (J. MARTINET). Si $k = \mathbf{Q}$ et si toute unité de norme 1 est totalement positive alors $\operatorname{Ker}\Phi_{u_0} \cap U_K = \phi$ et A_K n'est pas monogène. (On sait grâce à [1] que le nombre de classes de K est alors pair et on trouve dans [7] un exemple de cette situation, à savoir $p = 3$, $\Delta_{K/\mathbf{Q}} = 1009^2$).

J'ai eu de fructueuses conversations avec Francoise Bertrandias et Nicole Moser pendant l'élaboration de ce travail. Je les en remercie.

Références

1. ARMITAGE, J. V. and FRÖLICH, A., Class numbers and unit signatures. *Mathematica* 14 (1967), 94–98.
2. CARLITZ, L., On abelian fields. *Trans. Amer. Math. Soc.* 35 (1933), 122–136.
3. CHEVALLEY, C., Sur la théorie du corps de classes dans les corps finis et dans les corps locaux. *J. Fac. Sci. Univ. Tokyo* 2 (1933), Chap. IV, 393–406.
4. GRAS, G., Groupes de ramification – Application à la théorie de Kummer. *Sém. Théorie Nombres Univ. Grenoble*, 1969–70.
5. —»— Sur le l-groupe des classes d'une extension cyclique de degré l. *Sém. Théorie Nombres Univ. Grenoble*, 1971–72.
6. HASSE, H., *Zahlentheorie.* Akademie-Verlag, Berlin, 1963.
7. MONTOUCHET-GRAS, M. N., *Sur le nombre de classes du sous-corps cubique de* $\mathbf{Q}^p$ $(p \equiv 1$ (3)). Thèse, Grenoble, 1971.
8. MARTINET, J., A propos de classes d'idéaux. *Sém. Théorie Nombres Univ. Bordeaux*, 1971–72.
9. NAGELL, T., Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique. *Ark. Mat.* 6 (1966), 269–289.
10. PAYAN, J. J., Ordres monogène des corps cycliques de degré premier. *Sém. Théorie Nombres Univ. Grenoble*, 1971–72.
11. SERRE, J. P., *Corps locaux.* Hermann, Paris, 1962.

Received May 4, 1973

J. J. Payan
Université Scientifique et Médicale de Grenoble
Institut de Mathématiques Pures
Boite Postale 116
F-38 SAINT-MARTIN-D'HÉRES
France