ACTA ARITHMETICA
XXIII (1973)

Approximation algorithmique du groupe des classes de certains corps cubiques cycliques

par

M. N. Gras, N. Moser et J. J. Payan (St. Martin d'Hères, France)

I. Rappels et notations. Soit K une extension cubique cyclique de $\boldsymbol{Q}$. Nous noterons A l'anneau des entiers de K, et σ un générateur du groupe de Galois G de $K/\boldsymbol{Q}$. On sait que le discriminant de K est de la forme $81m^2$ ou m^2, (suivant que $3\,\boldsymbol{Z}$ se ramifie dans $A/\boldsymbol{Z}$ ou non), avec m produit de nombres premiers deux à deux distincts et congrus à 1 modulo 3. A $K/\boldsymbol{Q}$ est associé un élément unique de $\boldsymbol{Q}(\sqrt{-3})$, $\varphi = \dfrac{a+b\sqrt{-3}}{2}$ (a et b entiers de même parité), possédant les propriétés suivantes:

$$m = N_{\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}}(\varphi) = \frac{a^2+3b^2}{4},$$

$$a \equiv 1(3) \quad \text{et } b > 0,$$

$$b \not\equiv 0(3) \text{ si } 3\,\boldsymbol{Z} \text{ est ramifié}, \quad b \equiv 0(3) \text{ sinon},$$

$$K\boldsymbol{Q}(\sqrt{-3}) = \boldsymbol{Q}(\sqrt{-3})(\sqrt[3]{a}) \quad \text{où } a = m\varphi.$$

Lorsque $K/\boldsymbol{Q}$ est modérément ramifiée, A est un $\boldsymbol{Z}[G]$-module libre; soit θ un générateur de trace -1 du $\boldsymbol{Z}[G]$-module A (θ est ainsi défini à la conjugaison près). Alors

$$\operatorname{Irr}(\theta, \boldsymbol{Q}) = F(X) = X^3 + X^2 + \tfrac{1}{3}(1-m)X - \tfrac{1}{27}[m(3+a)-1].$$

Dans le cas où $K/\boldsymbol{Q}$ est sauvagement ramifiée, A n'est pas $\boldsymbol{Z}[G]$-libre. Cependant, si θ est une racine du polynôme irréductible sur $\boldsymbol{Q}$

$$F(X) = X^3 - 3mX - ma,$$

$\{1, \theta^\sigma, \theta^{\sigma^2}\}$ est une $\boldsymbol{Z}$-base de A. Dans les deux cas, nous appellerons F le polynôme fondamental de K. (Pour avoir des justifications, consulter par exemple [1] et [5].)

Nous nous intéressons à ceux des corps K pour lesquels $\{1, 0, \theta^2\}$ est une $\boldsymbol{Z}$-base de A. Un calcul facile du discriminant de F montre que cette

condition est réalisée si et seulement si $m = \frac{a^2+27}{4}$ (resp. $m = \frac{a^2+3}{4}$) lorsque $K/\mathbf{Q}$ est modérément ramifiée (resp. sauvagement ramifiée).

Remarques. 1) Parmi les corps de discriminant m^2 (resp. $81m^2$), il y en a au plus un pour lequel $\{1, \theta, \theta^2\}$ est une $\mathbf{Z}$-base de A; il correspond à $\varphi = \frac{a+3\sqrt{-3}}{2}$ (resp. $\varphi = \frac{a+\sqrt{-3}}{2}$).

2) Il est bien connu que si $\Delta_{K/\mathbf{Q}} = m^2$ avec $m = \frac{1+27b^2}{4}$, A admet une $\mathbf{Z}$-base de la forme $\{1, \vartheta, \vartheta^2\}$ avec ϑ donné par $\mathrm{Irr}(\vartheta, \mathbf{Q}) = X^3 - mX - mb$.

3) Les m de la forme $m = \frac{a^2+27}{4}$ sont représentés par le trinôme u^2+3u+9, pour u congru à -1 modulo 3. Ceux de la forme $m = \frac{a^2+3}{4}$ peuvent s'écrire u^2+u+1, avec u congru à 0 modulo 3.

K étant un corps où $\{1, \theta, \theta^2\}$ est une $\mathbf{Z}$-base de A, θ^σ et θ^{σ^2} sont des combinaisons $\mathbf{Z}$-linéaires de 1, θ, θ^2. Nous poserons $\theta^\sigma = S_1(\theta)$ et $\theta^{\sigma^2} = S_2(\theta)$ avec S_1 et S_2 éléments de $\mathbf{Z}[X]$, de degré inférieur ou égal à 2. Nous fixerons le générateur σ de G en posant

$$S_1(X) = X^2 - \frac{a-1}{6}X - \frac{4m+a+7}{18},$$

$$S_2(X) = -S_1(X) - X - 1$$

si $K/\mathbf{Q}$ est modérément ramifiée, et

$$S_1(X) = -X^2 + \frac{a+1}{2}X - 2m,$$

$$S_2(X) = -S_1(X) - X$$

si $K/\mathbf{Q}$ est sauvagement ramifiée.

Enfin, nous noterons $\mathscr{K}$ le groupe des classes de K.

II. Approximation de $\mathscr{K}$. Soit $\mathfrak{p}$ un idéal premier de A, de degré résiduel égal à 1, divisant le nombre premier p. Les nombres rationnels n qui vérifient $\theta - n \in \mathfrak{p}$ forment une progression arithmétique de raison p; un tel n s'appellera une racine de $\mathfrak{p}$.

Delone et Faddeev ont montré que toute classe d'idéaux fractionnaires de K contient au moins un idéal entier $\mathfrak{a}$ dont la norme vérifie $N\mathfrak{a} < \frac{4}{27}\sqrt{\Delta_{K/\mathbf{Q}}}$ (cf. [2]). Si $\mathfrak{p}$ divise un tel idéal $\mathfrak{a}$, il est clair que $\mathfrak{p}$ admet au moins une racine dans l'intervalle $\left]-\frac{2}{27}\sqrt{\Delta_{K/\mathbf{Q}}}, \frac{2}{27}\sqrt{\Delta_{K/\mathbf{Q}}}\right[$.

Nous utiliserons les résultats suivants:

Propriété 1. *Soit n un entier rationnel. Si un idéal premier $\mathfrak{p}$ de A divise $\theta - n$, alors $\mathfrak{p}$ est de degré résiduel égal à 1. De plus, si $\mathfrak{p} = \mathfrak{p}^\sigma$, $\theta - n$ n'est pas divisible par $\mathfrak{p}^2$, et si $\mathfrak{p} \neq \mathfrak{p}^\sigma$, $\theta - n$ n'est divisible ni par $\mathfrak{p}^\sigma$, ni par $\mathfrak{p}^{\sigma^2}$.*

Démonstration. La première assertion résulte de l'hypothèse $\{1, \theta, \theta^\sigma\}$ ou $\{1, \theta^\sigma, \theta^{\sigma^2}\}$ $\mathbf{Z}$-base de A, la seconde de $A = \mathbf{Z}[\theta]$.

Corollaire. *Si $F(n) = p_1^{n_1} \dots p_r^{n_r}$, où les p_i sont premiers et deux à deux distincts, alors $(\theta - n) = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$, où $\mathfrak{p}_i$ désigne un diviseur premier de (p_i) dans A.*

Propriété 2. *Si n est une racine de $\mathfrak{p}$, les racines de $\mathfrak{p}^\sigma$ (resp. $\mathfrak{p}^{\sigma^2}$) forment la progression arithmétique de raison p contenant $S_2(n)$ (resp. $S_1(n)$).*

Démonstration. Comme $\theta - c \in \mathfrak{p}$, $\theta^\sigma - S_1(c) \in \mathfrak{p}$ et $\theta^{\sigma^2} - S_2(c) \in \mathfrak{p}$. Il en résulte que $\theta - S_1(c) \in \mathfrak{p}^{\sigma^2}$ et que $\theta - S_2(c) \in \mathfrak{p}^\sigma$.

Ordonnons alors totalement l'ensemble E des entiers n tels que $|n| < \frac{2}{27}\sqrt{\Delta_{K/\mathbf{Q}}}$. Soit p un nombre premier divisant au moins une valeur de $F(n)$ pour $n \in E$; nous noterons $\mathfrak{p}_p$ celui des idéaux premiers au dessus de p qui divise $\theta - n$ pour la plus petite valeur de n telle que $p \mid F(n)$. Il est clair que si p divise $F(n')$ pour $n' \in E$, $\mathfrak{p}_p$ divisera $\theta - n'$ (resp. $\mathfrak{p}_p^\sigma$ divisera $\theta - n'$, resp. $\mathfrak{p}_p^{\sigma^2}$ divisera $\theta - n'$), suivant que $n' \equiv n \pmod p$ (resp. $n' \equiv S_2(n) \bmod p$, resp. $n' \equiv S_1(n) \bmod p$).

Définissons maintenant un groupe abélien $\mathscr{G}$ par les générateurs $\mathrm{Cl}\mathfrak{p}_p$, $\mathrm{Cl}\mathfrak{p}_p^\sigma$, $\mathrm{Cl}\mathfrak{p}_p^{\sigma^2}$, (où p parcourt l'ensemble des nombres premiers vérifiant $p < \frac{4}{27}\sqrt{\Delta_{K/\mathbf{Q}}}$ et divisant une valeur $F(n)$ pour $n \in E$), et les relations

$$\mathrm{Cl}\mathfrak{p}_p \mathrm{Cl}\mathfrak{p}_p^\sigma \mathrm{Cl}\mathfrak{p}_p^{\sigma^2} = 1$$

et

$$(\mathrm{Cl}\mathfrak{p}_{p_1}^{\sigma^{i_1}})^{\lambda_1} \dots (\mathrm{Cl}\mathfrak{p}_{p_r}^{\sigma^{i_r}})^{\lambda_r} = 1$$

(ces dernières relations proviennent des égalités $F(n) = p_1^{i_1}, \dots, p_r^{i_r}$; les indices $i_1, \dots, i_r$ prennent les valeurs 0, 1, ou 2, déterminées grâce à la propriété 2). Nous pouvons énoncer:

Propriété 3. *$\mathscr{K}$ est un quotient de $\mathscr{G}$.*

Il en résulte que les invariants de $\mathscr{K}$ sont des diviseurs des invariants de $\mathscr{G}$.

III. Résultats numériques. Ils illustrent non trivialement le théorème de [4] suivant lequel le nombre de classes de K est une norme d'entier de $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$. C'est par ordinateur que nous les avons obtenus, avec l'aide de Lyliane Bouvier que nous remercions vivement.

Nous les avons rassemblés dans deux tableaux, en distinguant le cas modérément ramifié du cas sauvagement ramifié. Dans la troisième colonne figurent les idéaux entiers dont les classes engendrent $\mathscr{G}$, dans

$K/\mathbf{Q}$ modérément ramifiée, $\sqrt{A_{K/\mathbf{Q}}} < 2500$.

m	$F(X)=X^3-X^2$	Invariants de $\mathscr{G}$	Générateurs de $\mathscr{G}$	Invariants de $\mathscr{X}$
7	$-2X-1$	1	—	1* (a)
13	$-4X+1$	1	—	1* (a)
19	$-6X-7$	1	—	1* (a)
37	$-12X+11$	1	—	1* (a)
79	$-26X+41$	1	—	1* (a)
97	$-32X-79$	1	—	1* (a)
139	$-46X+103$	1	—	1* (a)
163	$-54X-169$	2, 2	Clp_5, Clp_5^σ	2, 2* (b)
7·31	$-72X+209$	3	Clp_7	3 (a)
13·19	$-82X-311$	3	Clp_{13}	3 (a)
313	$-104X+371$	7	Clp_5	7 (c)
349	$-116X-517$	2, 2	Clp_{11}, Clp_{11}^σ	2, 2* (b)
7·61	$-142X+601$	3, 3	Clp_7, Clp_{61}	3 (a)
7·67	$-156X-799$	3	Clp_7	3 (a)
13·43	$-186X+911$	3	Clp_{13}	3 (a)
607	$-202X-1169$	2, 2	Clp_7, Clp_7^σ	2, 2* (b)
709	$-236X+1313$	2, 2	Clp_{13}, Clp_{13}^σ	2, 2 (b)
7·109	$-254X-1639$	2, 2, 3	Clp_{41}, Clp_{41}^σ, Clp_7	2, 2, 3 (a) (b)
877	$-292X+1819$	7	Clp_{11}	7 (c)
937	$-312X-2221$	2, 2	Clp_{23}, Clp_{23}^σ	2, 2 (b)
1063	$-354X+2441$	13	Clp_5	13 (c)
1129	$-376X-2927$	7	Clp_{19}	7 (c)
7·181	$-422X+3191$	3, 3, 3	Clp_7, Clp_{17}, Clp_{181}	3, 3 (d)
13·103	$-446X-3769$	3, 3	Clp_{11}, Clp_{11}^σ	3, 3 (d)
1489	$-496X+4081$	19	Clp_7	19 (c)
1567	$-522X-4759$	7	Clp_{19}	7 (c)
7·13·19	$-576X+5123$	3, 3	Clp_7, Clp_{13}	3, 3 (a)
1987	$-662X+6329$	7, ∞, ∞	Clp_{29}, Clp_{251}, $\mathrm{Clp}_{251}^\sigma$	7 (c)
31·67	$-692X-7231$	2, 2, 3	Clp_{89}, Clp_{89}^σ, $(\mathrm{Clp}_7)^2$	2, 2, 3 (a) (b)
31·73	$-754X+7711$	3, 7	$(\mathrm{Clp}_5)^7$, $(\mathrm{Clp}_5)^3$	3, 7 (c)
7·337	$-786X-8737$	3, 3, 3	Clp_{61}, Clp_{61}^σ, Clp_{337}	3, 3 (d)

$K/\mathbf{Q}$ sauvagement ramifiée, $\sqrt{A_{K/\mathbf{Q}}} < 2500$.

m	$F(X)=X^3$	Invariants de $\mathscr{G}$	Générateurs de $\mathscr{G}$	Invariants de $\mathscr{X}$
7	$-21X+35$	3	Clp_3	3* (a)
13	$-39X-91$	3	Clp_3	3* (a)
31	$-93X+341$	3	Clp_3	3 (a)
43	$-129X-559$	3	Clp_3	3 (a)
73	$-219X+1241$	3, 3	Clp_{11}, Clp_{11}^σ	3, 3 (d)
7·13	$-273X-1729$	3, 3	Clp_3, Clp_7	3, 3 (a)
7·19	$-399X+3059$	3, 3	Clp_3, Clp_7	3, 3 (a)
157	$-471X-3925$	2, 2, 3	$(\mathrm{Clp}_5)^3$, $(\mathrm{Clp}_5^\sigma)^3$, Clp_3	2, 2, 3 (a) (b)
211	$-633X+6119$	2, 2, 3	Clp_{107}, $\mathrm{Clp}_{107}^\sigma$, Clp_3	2, 2, 3 (a) (b)
241	$-723X-7471$	2, 2, 3	Clp_{17}, Clp_{17}, Clp_3	2, 2, 3 (a) (b)

*: Résultat déjà connu.

(a): 3^{t-1} divise $\mathrm{Card}\mathscr{X}$ où t désigne le nombre de facteurs premiers distincts du discriminant. (Classes Ambiges.)

(b): 4 divise $\mathrm{Card}\mathscr{X}$. (Cf. [5], généralisable au cas où m est produit de plusieurs facteurs premiers.)

(c): programme mis au point par M. N. Gras pour déterminer le nombre de classes. (Article à paraître.)

(d): $\mathscr{G}$ est un 3-groupe. (Cf. [3].)

l'ordre où l'on a donné les invariants. Dans la dernière colonne figure la structure de $\mathscr{X}$, dans les cas où nous avons pu conclure; les indices renvoient aux arguments utilisés.

Remarque. On peut conclure directement dans le cas des corps de discriminant 13×103 et 7×337 que $\mathscr{X} \simeq \mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}$. En effet dans chacun de ces cas, il existe un p avec Clp_p et Clp_p^σ générateurs de $\mathscr{G}$ isomorphe à $\mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}$, et une relation $\mathfrak{p}_p\mathfrak{p}_p^{2\sigma} \sim \mathfrak{p}_{p_1}$, où p_1 divise $\Delta_{K/\mathbf{Q}}$. On se sert alors de „l'unicité" de la relation de dépendance entre les classes ambiges (voir [6]).

Les exemples les plus intéressants nous paraissent correspondre à

$$m = 313 \quad \text{nombre de classes } 7,$$
$$m = 1063 \quad \text{nombre de classes } 13,$$
$$m = 1489 \quad \text{nombre de classes } 19.$$

La remarque suivante montre que ces exemples fournissent des extensions de $\mathbf{Q}$ de degré 7, 13 ou 19, et de discriminant „petit".

Remarque. Soit K un corps cubique de discriminant q^2, où q est premier, et de nombre de classes égal à p, avec p premier ($p \equiv 1 \bmod 3$). L'extension abélienne non ramifiée maximale N de K est cyclique de degré p sur K, et galoisienne non abélienne sur Q; soit alors L une extension intermédiaire de N/Q de degré p. On voit facilement que l'idéal premier q au-dessus de q dans K se décompose dans N/K; la considération des groupes de décomposition de ses diviseurs premiers dans N montre que $\Delta_{L/Q} = q^{\frac{2(p-1)}{3}}$. Il en résulte que pour $q = 313$, $p = 7$, nous avons obtenu une extension de degré 7 dont le discriminant, égal à 313^4, s'intercale entre les discriminants 43^6 et 7^{12} des extensions cycliques de degré 7, A_1 non ramifiée en dehors de 43 et A_2 non ramifiée en dehors de 7. Pour $q = 1489$, l'extension de degré 19 et de discriminant 1489^{12} est de discriminant inférieur à celui de toute extension cyclique de degré 19 puisque le plus petit d'entre eux est 191^{18}.

Bibliographie

[1] A. Chatelet, *Arithmétique des corps abéliens du troisième degré*, Ann. ENS 63 (1946), p. 109–160.

[2] Delone et Fadeev, *The theory of irrationalities of the third degree*, (AMS 1964).

[3] G. Gras, *Sur le groupe des classes des extensions cycliques de degré l de Q*, Séminaire de Théorie des Nombres, Univ. de Grenoble, 1971–72.

[4] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abhandlungen der Deutschen Akademie der Wissenschaften zu Berlin, 1948, n° 2.

[5] M. N. Gras-Montouchet, *Sur le nombre de classes du sous-corps cubique cyclique de $Q(x)$ $p \equiv 1 \bmod 3$*, Proc. Japan. Academy 47 (6) (1971).

[6] J. J. Payan, *Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur Q, ou sur un corps quadratique imaginaire*, (à paraître).

INSTITUT DE MATHÉMATIQUES PURES
St. Martin d'Hères, France

Reçu le 1. 4. 1972 (280)

ACTA ARITHMETICA
XXIII (1973)

On the transcendence of certain power series of algebraic numbers

by

P. L. Cijsouw (Amsterdam) and R. Tijdeman (Leiden)

1. Introduction. Let $\sigma(z) = \sum_{k=0}^{\infty} a_k z^{e_k}$ be a power series with complex coefficients a_k, convergence radius $R > 0$ and sufficiently rapidly increasing integers e_k. H. Cohn, [2], constructed certain transcendental numbers using such gap series. He proved that under certain conditions $\sigma(\theta)$ is transcendental for every algebraic argument θ with $0 < |\theta| < R$, if the coefficients a_k of σ be rationals. Or, equivalently, $\sigma(\theta)$ is algebraic with $0 < |\theta| < R$, implies that θ is transcendental. Baron and Braune, [1], used the same method with the assumption that the coefficients a_k of σ are algebraic integers of degree s_k. They proved that $\sigma(\theta)$ is transcendental for every algebraic θ with $0 < |\theta| < R$ under the following conditions:

(i) $D^{-k} < \overline{|a_k|} < D^k$ for some $D \geqslant 1$ and all k,

(ii) $\lim_{k\to\infty} e_k T_k^2 / e_{k+1} = 0$, where $T_k = \prod_{i=0}^{k} s_i$.

It was noted that these conditions imply $R = 1$.

In this paper we will improve and generalise the result of Baron and Braune using a more suitable auxiliary inequality. As a special case of a more general result we will prove the following property for gap series $\sigma(\theta)$ with algebraic integral coefficients a_k of degree s_k: $\sigma(\theta)$ is transcendental for algebraic θ with $0 < |\theta| < R$ under the conditions:

(i) $\overline{|a_k|} \leqslant D^{e_k}$ for some $D \geqslant 1$ and all k,

(ii) $\lim_{k\to\infty} e_k S_k / e_{k+1} = 0$, where S_k is the degree of the field obtained by adjoining $a_0, a_1, \ldots, a_k$ to the field of the rationals.

2. Formulation of results. We denote the conjugates of an algebraic number α of degree s by $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(s)}$. Further, $\overline{|\alpha|} = \max_{i=1,\ldots,s} |\alpha^{(i)}|$. We mention the inequalities $\overline{|\alpha+\beta|} \leqslant \overline{|\alpha|} + \overline{|\beta|}$ and $\overline{|\alpha\beta|} \leqslant \overline{|\alpha|} \cdot \overline{|\beta|}$, for arbitrary algebraic numbers α and β. The *height* of an algebraic number α is defined as the maximum absolute value of the coefficients of its minimal