Astérisque

S. IYANAGA

Construction de corps de nombres algébriques avec les groupes des classes d'idéaux de types donnés

Astérisque, tome 147-148 (1987), p. 301-306

<http://www.numdam.org/item?id=AST_1987__147-148__301_0>

Société Mathématique de France
Astérisque 147-148 (1987), p. 301-306.

Construction de corps de nombres algébriques avec les groupes des classes d'idéaux de types donnés

par S. Iyanaga

Nous appellerons <u>corps</u> un corps de nombres algébriques de degré fini $n \geq 2$, c'est-à-dire $k = Q(\theta)$, où θ est une racine d'un polynôme irréductible $f(x) \in Z[x]$ de degré $n = [k: Q] \geq 2$. Parmi les n conjugués de k, r_1 sont réels, $2r_2$ imaginaires. $k^\times$ est le groupe multiplicatif des éléments non nuls de k, $U = U(k)$ le groupe des unités de k, $W = W(k)$ le sous-groupe (fini) de U des racines de 1. On sait que U/W forme un groupe abélien libre à $r = r_1+r_2-1$ générateurs. $\mathcal{J}$ désigne le groupe multiplicatif des idéaux de k, $\mathcal{P} \cong k^\times/U$ le sous-groupe de $\mathcal{J}$ des idéaux principaux, $\mathcal{H} = \mathcal{J}/\mathcal{P}$ le groupe (fini) des classes d'idéaux, ou <u>groupe des classes</u> de k. Son cardinal $|\mathcal{H}| = h = h(k)$ est le <u>nombre des classes</u> de k.

On envisage le problème de construire les corps k de certains types (e.g. de degré donné) dont les groupes des classes doivent satisfaire à certaines conditions (e.g. $\mathcal{H} \supset (Z/mZ)^\nu$, où m, ν sont des nombres naturels donnés, signifiant que $\mathcal{H}$ doit contenir un sous-groupe isomorphe à $(Z/mZ)^\nu$; ou bien plus simplement $m|h$.)

Nagell [8] (1922) a démontré qu'il y a une infinité de corps quadratiques imaginaires avec $m|h$ pour m arbitrairement donné. Yamamoto [16] (1970) a démontré qu'on obtient la même conclusion pour les corps quadratiques réels. Azuhata-Ichimura [1] (1984) ont construit une infinité de corps de degré n, avec $m|h$, m, n étant arbitrairement donnés; plus précisément tels que $\mathcal{H} \supset (Z/mZ)^{r_2}$ de sorte que ce résultat contient le théorème de Nagell, mais non pas celui de Yamamoto. Dans sa thèse soutenue récemment, Nakano [11] a réussi à renforcer ce résultat: l'exposant r_2 peut se remplacer par r_2+1, d'où s'ensuit le théorème de Yamamoto. En fait, il a montré, en analysant les démonstrations de Yamamoto [16] et d'Azuhata-

Ichimura [1], que leurs résultats peuvent être déduits des deux Lemmes suivants, assez faciles à établir, sur $k = Q(\theta)$:

(Les notations n, r, U, W, $\mathcal{J}$, f, m etc. expliquées ci-dessus sont utilisées dans la suite dans les mêmes sens. De plus, on notera $\mathcal{L} = \mathcal{L}(m)$ l'ensemble des diviseurs premiers de m et posera $M = \prod_{\ell \in \mathcal{L}} \ell^{1+\mathrm{Ord}_\ell(|W|)}$. $\left(\frac{*}{*}\right)_\ell$ désignera le symbole de résidu de la ℓ-ième puissance.)

Lemme 1. Soit $s > r$, et supposons qu'il y ait s éléments $\alpha_1, \cdots, \alpha_s$ de $k^\times$ tels que

(i) $(\alpha_i) \in \mathcal{J}^m$, $i = 1, 2, \ldots, s$,

(ii) $\alpha_1, \ldots, \alpha_s$ sont (mutliplicativement) indépendants dans $k^\times / Wk^{\times \ell}$ pour tout $\ell \in \mathcal{L}$.

Alors on a $\mathcal{H} \supset (Z/mZ)^{s-r}$.

Lemme 2. Supposons qu'il y ait 2s éléments $A_1, \ldots, A_s$, $C_1, \ldots, C_s$ de Z tels que $f(A_i) = \pm C_i^m$, $(f'(A_i), C_i) = 1$, $i = 1, \ldots, s$. Posons $\theta - A_i = \alpha_i$. Alors $\alpha_1, \ldots, \alpha_s$ satisfont à (i).

Supposons de plus qu'il y ait s nombres premiers $p_1, \ldots, p_s$ et $t \in Z$ tels que $p_i \equiv 1 \pmod{M}$, $f(t) \equiv 0 \pmod{p_i}$, $f'(t) \not\equiv 0 \pmod{p_i}$, $i = 1, \ldots, s$ et

$$\left(\frac{t-A_j}{p_i}\right)_\ell = 1 \quad \text{pour } i \neq j, \qquad \left(\frac{t-A_i}{p_i}\right)_\ell \neq 1.$$

Alors $\alpha_1, \ldots, \alpha_s$ satisfont à (ii).

Ces Lemmes ramènent notre problème de construction de k à celui de f satisfaisant aux conditions du Lemme 2. Nakano résout ce dernier de façon ingénieuse, quoique pas très simple. Au lieu d'entrer dans les détails de démonstration, nous donnons ici les formulations exactes du résultat principal ainsi que de plusieurs autres conséquences de ces Lemmes.

On affirme dans tous les théorèmes qui suivent l'existence d'une infinité de corps k qui ont une propriété (P) dont les groupes de classes $\mathcal{H}$ ont une propriété (Q). On donnera (P), (Q) pour chacun de ces Théorèmes.

Théorème 1. On se donne n, r_1, r_2 tels que $n = r_1 + 2r_2 \geq 2$, et

$m \geq 2$ arbitrairement.

(P) $(k: Q) = n$ et r_1, r_2 sont les nombres des conjugués réels et imaginaires de k.

$$(Q) \quad \mathcal{H} \supset (Z/mZ)^{r_2+1}.$$

Pour démontrer ce théorème, on utilise un polynôme irréducible $f \in Z[x]$ de la forme

$$(*) \quad f(x) = \prod_{i=0}^{n-1} (x-A_i) + C^m, \quad A_0, \cdots, A_{n-1}, C \in Z$$

ayant juste r_1 racines réelles, tel que $f(B) = D^m$ pour certains $B, D \in Z$, où $A_0, \cdots, A_{n-1}, B, C, D$ doivent satisfaire à certaines congruences. On pose $\alpha_i = \theta - A_i$, $i = 1, \cdots, n-1$, $\alpha_n = \theta - B$ pour une racine θ de f et vérifie que $\alpha_1, \cdots, \alpha_n$ satisfont à des conditions (i), (ii) du Lemme 1.

Un polynôme du type (*) a été utilisé en fait d'abord par Ishida [6] pour démontrer l'existence d'une infinité de corps de degré premier p tels que $\mathcal{H} \supset (Z/2Z)^{p-1}$. Ichimura [5] a généralisé ce résultat pour le cas de degré général n (impair) au lieu de degré premier. Nakano [11], [12] obtient en poursuivant la même méthode:

Théorème 2. (P) Comme dans le Théorème 1, n étant impair.

$$(Q) \quad \mathcal{H} \supset (Z/mZ)^{r_2+1} + (Z/2Z)^{r_2+\frac{r_1-1}{2}}.$$

Prenant en particulier $m = 2$, (Q) devient

$$\mathcal{H} \supset (Z/2Z)^{2r_2+\frac{r_1+1}{2}}.$$

On retrouve le résultat de [5] renforcé en faisant $r_1 = 1$.

Nakano [10] étudie le 2-rang des corps purs $k = Q(\sqrt[n]{a})$, $a \in Z$. Si n est pair, la théorie classique des genres du corps quadratique implique que le 2-rang de $\mathcal{H}$ est au moins ρ, où $\rho+1$ est le nombre des nombres premiers p tels que $v_p(a)$ sont impairs, où $v_p(a)$ désigne l'exposant de la puissance de p qui divise exactement a. Soit donc n impair, Utilisant un polynôme de la forme

$$f(x) = x^n - (y^n + z^2), \ y, z \in Z$$

où y, z doivent être convenablement choisis, Nakano démontre:

Théorème 3. Soient $n \geq 2$ impair, donné arbitrairement et $n = \prod_{i=1}^{s} p_i^{e_i}$ sa décomposition canonique. On pose $\Delta = \prod_{i=1}^{s} (e_i+1)-1$ (le nombre des diviseurs propres de n).

(P) $k = Q(\sqrt[3]{a})$, $a \in Z$. (Q) $\mathcal{H} \supset (Z/2Z)^{3\Delta}$.

Le résultat avec l'exposant 2Δ au lieu de 3Δ se trouve démontré dans [10], [11]. Il a été amélioré depuis.

Dans [9], [11], Nakano démontre le théorème suivant en utilisant un polynôme $f(x) = x^3-(y^{3m}+z^{3m})$, y, $z \in Z$ convenablement choisis:

Théorème 4. (P) $k = Q(\sqrt[3]{a})$, $a \in Z$, (Q) $m|h$.

et dans [13], [11] le théorème suivant qui renforce le résultat de Uchida [14].

Théorème 5. (P) k/Q cubique et cyclique, (Q) $\mathcal{H} \supset (Z/mZ)^2$.

Le travail classique de Yamamoto [16], d'où beaucoup de méthodes utilisées dans les travaux cités tirent leur origine, contient aussi un résultat sur le 3-rang des corps quadratiques, qui a été renforcé par Craig [2], [3] en employant un polynôme symétrique $x^2+y^2+z^2-2(yz+zx+xy)$ de trois variables x, y, z. En modifiant cette méthode, Nakano a démontré:

Théorème 6. (P) $k = Q(\sqrt[3]{a})$, $a \in Z$, (Q) $\mathcal{H} \supset (Z/2Z)^6$.

Ce résultat n'a pas encore été publié.

Pour un nombre premier ℓ et un groupe abélien fini G, désignons par G_ℓ la ℓ-partie de G, c'est-à-dire le sous-groupe de G dont chaque élément a une puissance de ℓ pour ordre. Les Théorèmes 3, 6 concernant $\mathcal{H}_\ell$ avec $\ell \nmid n = (k: Q)$, tandis que la "théorie du corps de genres" initiée par Ishida [7], ainsi que Gras [4], a pour objet $\mathcal{H}_\ell$ avec $\ell|n$. Yahagi [15] l'étudie aussi; celui-ci démontre en particulier ce résultat remarquable:

Théorème 7. Soit G_ℓ un ℓ-groupe abélien fini donné.

(P) (k: Q) = l'exposant de G_ℓ, k|Q cyclique, (Q) $\mathcal{H}_\ell \cong G_\ell$.

BIBLIOGRAPHIE

[1] T. Azuhata & H. Ichimura, On the divisibility problem of the class numbers of algebraic number fields, J. Fac. Sc. Univ. Tokyo, 30 (1984), 579-585.

[2] M. Craig, A type of class groups for imaginary quadratic fields, Acta Arith., 22 (1973), 449-459.

[3] M. Craig, A construction for irregular discriminants, Osaka J. Math. 14 (1977), 365-402.

[4] G. Gras, Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, Ann. Inst. Fourier 23, no.3 (1973), 1-48.

[5] H. Ichimura, On 2-rank of the ideal class groups of totally real number fields, Proc. Japan Acad. 58A (1982), 329-332.

[6] M. Ishida, On 2-rank of the ideal class groups of algebraic number fields, J. reine ang. Math. 273 (1975), 165-169.

[7] M. Ishida, The genus fields of algebraic number fields, LNM Springer 555 (1976).

[8] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Hamburg 1 (1922), 140-150.

[9] S. Nakano, Class numbers of pure cubic fields, Proc. Japan Acad. 59A (1983), 263-265.

[10] S. Nakano, On the 2-rank of the ideal class groups of pure number fields, Arch. Math. 42 (1984), 53-57.

[11] S. Nakano, On ideal class groups of algebraic number fields, Thesis, Gakushuin Univ. (1985).

[12] S. Nakano, On ideal class groups of algebraic number fields, J. reine ang. Math. 358 (1985), 61-75.

[13] S. Nakano, Ideal class groups of cubic cyclic fields, to appear in Acta Arith.

[14] K. Uchida, Class numbers of cubic cyclic fields, J. Math. Soc. Japan 26 (1974), 447-453.

[15] O. Yahagi, Construction of number fields with prescribed ℓ-class groups, Tokyo J. Math. 1 (1978), 275-283.

[16] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970), 57-76.

Addendum (Avril 1986). La démonstration du Théorème 3 utilise, comme celle du Théorème 6, le polynôme de Craig. Elle a été publiée

dans [17]. L'auteur doit au rapporteur la connaissance du résultat suivant démontré par Mestre [18] en utilisant l'arithmétique des courbes elliptiques:

Théorème 8. (P) $(k: Q) = 2$. (Q) $\mathcal{H} \supset (\mathbb{Z}/5\mathbb{Z})^2$ ou $\mathcal{H} \supset (\mathbb{Z}/7\mathbb{Z})^2$.

(Dans le cas où k est imaginaire, ce résultat est contenu dans le Théorème 1.)

[17] S. Nakano, On the construction of pure number fields of odd degrees with large 2-class groups, Proc. Japan Acad. 62A (1986), 61-64.

[18] Jean François Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. reine angew. Math. 343 (1983), 23-35.

Shokichi IYANAGA
12-4 Otsuka 6-chome
Bunkyo-ku, Tokyo 112 Japan