**Zeitschrift:** L'Enseignement Mathématique

**Herausgeber:** Commission Internationale de l'Enseignement Mathématique

**Band:** 20 (1974)

**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

**Autor:** Archinard, Gabriel

**Kapitel:** Chapitre 2. — Indice d'un nombre de $O_k$

**DOI:** https://doi.org/10.5169/seals-46902

*Démonstration* Ces formules s'obtiennent immédiatement en prenant les discriminants des bases canoniques par la formule (1.6).

Corollaire 1.5 Soit $p_1, p_2, \ldots, p_r$, $r$ nombres premiers différents de 1, distincts et congrus à 1 (mod 3). Alors il existe $2^{r-1}$ corps modérément ramifiés de discriminant $(p_1 p_2 \ldots p_r)^2$ et $2^r$ corps sauvagement ramifiés de discriminant $81\,(p_1 p_2 \ldots p_r)^2$.

Tous les corps cubiques cycliques ont leurs discriminants de cette forme, sauf un corps unique de discriminant 81.

Pour une démonstration du théorème 1.4 et du corollaire 1.5, on se reportera à [1], chapitre IV.

## Chapitre 2. — Indice d'un nombre de $O_K$

L'indice d'un nombre $\theta$ d'une extension finie $K/Q$ est le nombre $I(\theta) = \sqrt{\Delta(\theta)/\Delta_K}$, où $\Delta(\theta)$ est le discriminant de $\theta$ dans $K$ et $\Delta_K$ le discriminant de $K$ (cf. [3], chap. III, § 25 et [5]).

Comme au chapitre 1, $K/Q$ désigne dorénavant une extension cubique cyclique et on va utiliser une base canonique (déf. 1.6) pour calculer l'indice d'un élément quelconque de $O_K$.

*Lemme 2.1* Soit $\theta$ un élément primitif d'une base canonique de $K$. Alors, si $\varphi \in O_K$, il existe un nombre $\psi = X\theta + Y\sigma\theta \in O_K$ tel que $\psi - \varphi \in Z$ et $I(\psi) = I(\varphi)$.

*Démonstration* On considère le cas où $\theta$ est construit avec $(\alpha, 1)$, c'est-à-dire où $\alpha$ est unitaire positif. $\theta$, $\sigma\theta$ et $\sigma^2\theta$ forment une base d'entiers de $K$, donc $\varphi = X_0\theta + X_1\sigma\theta + X_2\sigma^2\theta$, avec $X_i \in Z$, $i = 1, 2, 3$. Soit $\psi = \varphi - X_2$; alors $I(\psi) = I(\varphi)$ et $\psi = (X_0 - X_2)\theta + (X_1 - X_2)\sigma\theta$, d'après $\theta + \sigma\theta + \sigma^2\theta = 1$. $\psi$ a la forme requise.

Les cas où $\alpha$ est unitaire négatif et où $K$ est non unitaire se démontrent de manière semblable. C.q.f.d.

Donc, pour obtenir les indices de tous les nombres de $O_K$, il suffit de considérer les nombres de la forme $X\theta + Y\sigma\theta$ où $X$ et $Y$ sont des entiers.

*Lemme 2.2* Soit $K$ le corps (modérément ramifié) engendré par l'entier canonique unitaire $\alpha = a_1 j + a_2 j^2$ et soit $\theta, \sigma\theta, \sigma^2\theta$ la base canonique construite avec $\alpha$. Alors, si $\psi = X\theta + Y\sigma\theta$, $\pm I(\psi)$ est égal à:

$$(2.1) \qquad \frac{a_1 - a_2}{3} X^3 + a_2 X^2 Y - a_1 X Y^2 + \frac{a_1 - a_2}{3} Y^3 .$$

On donne la démarche de la démonstration pour le cas où $\alpha$ est unitaire positif.

$\theta$, $\sigma\,\theta$ et $\sigma^2\,\theta$ formant, dans ce cas, une base des entiers de $K$, on exprime $\psi^2 = X^2\,\theta^2 + 2\,X\,Y\,\theta\,\sigma\,\theta + Y^2\,(\sigma\theta)^2$ comme combinaison linéaire de $\theta$, $\sigma\,\theta$, $\sigma^2\,\theta$ à l'aide des formules (1.7) et (1.8), en tenant compte de $S = \theta + \sigma\,\theta + \sigma^2\,\theta = 1$. 1, $\psi$ et $\psi^2$ étant exprimés comme combinaisons linéaires de $\theta$, $\sigma\,\theta$ et $\sigma^2\,\theta$, l'indice $\pm\,I(\psi)$ est le déterminant de la matrice des coefficients de ces combinaisons. Le calcul donne le résultat annoncé.

La même technique permet de démontrer le lemme suivant:

*Lemme 2.3* Soit $K$ le corps (sauvagement ramifié) engendré par l'entier canonique non unitaire $\alpha = a_1\,j + a_2\,j^2$ et soit 1, $\theta$, $\sigma\,\theta$ la base canonique construite avec $\alpha$. Alors, si $\psi = X\,\theta + Y\,\sigma\,\theta$, $\pm\,I(\psi)$ est égal à:

$$(2.2) \qquad (a_1 - a_2)\,X^3 + 3a_2X^2Y - 3a_1XY^2 + (a_1 - a_2)\,Y^3\,.$$

De ces lemmes découlent aisément la propriété suivante:

*Propriété 2.1* Soit $K$ le corps engendré par l'entier canonique $\alpha = a_1\,j + a_2\,j^2$ et soit $\theta \neq 1$ un des éléments non nuls d'une base canonique de $K$. Alors, une condition nécessaire et suffisante pour que $O_K = Z\,[\theta]$ est

(2.3) $\qquad a_1 - a_2 = \pm\,3$, si $K/Q$ est modérément ramifiée

(2.4) $\qquad a_1 - a_2 = \pm\,1$, si $K/Q$ est sauvagement ramifiée.

*Remarque 2.1* Des formules (2.1) et (2.2), on déduit aisément des équations diophantiennes qui sont résolubles si et seulement si l'anneau des entiers des corps correspondants sont monogènes.

*Définition 2.2* Si un entier divise $I(\varphi)$ pour tous les nombres $\varphi \in O_K$, on dit que c'est un diviseur commun des indices de $K$, ou un diviseur commun extraordinaire des discriminants de $K$.

D'après le critère de Hensel ([3], chap. III, § 25), seul 2 peut être diviseur commun des indices d'une extention cubique de $Q$.

La propriété suivante donne une condition nécessaire et suffisante pour qu'il en soit ainsi dans une extention cubique cyclique de $Q$.

*Propriété 2.2* Soit $K$ le corps engendré par l'entier canonique $\alpha = a_1\,j + a_2\,j^2$. Alors, 2 est diviseur commun des indices de $K$ si et seulement si $a_1 - a_2$ est pair.

*Démonstration* D'après les lemmes 2.1, 2.2 et 2.3, l'indice d'un nombre quelconque $\psi$ de $O_K$ est de la forme (2.1) ou (2.2), avec $X$ et $Y$ entiers rationnels.

Ces formes s'écrivent respectivement:

$$I(\psi) = \frac{a_1 - a_2}{3}(X^3 - 3X^2Y + Y^3) + a_1XY(X - Y)$$

et

$$I(\psi) = (a_1 - a_2)(X^3 - 3X^2Y + Y^3) + 3a_1XY(X - Y).$$

On voit que $I(\psi)$ est pair, pour tous $X$ et $Y$ entiers rationnels si et seulement si $a_1 - a_2$ est pair. C.q.f.d.

*Exemple 2.1* Soit $K$ le corps engendré par $\alpha = 5j - j^2$. On a $\alpha\alpha' = 31$ et $\alpha - 1 = 6j$, donc $\alpha$ est canonique unitaire et $K = Q(\theta)$, où $\theta$ est zéro du polynôme $X^3 - X^2 - 10X + 8$. Les 3 zéros de ce polynôme forment une base canonique de $K$ et $\Delta_K = 31^2$.

La condition du théorème 2.2 étant satisfaite, 2 est diviseur commun des indices de $K$.

*Remarque 2.2* Si 2 est diviseur commun des indices de $K$, $O_K$ n'est pas monogène; mais on verra, au chapitre 4, qu'il existe des corps $K$ où 2 n'est pas diviseur commun des indices et où $O_K$ n'est pas monogène.

## Chapitre 3. — Les nombres cubiques cycliques $\theta$ pour lesquels $Z[\theta]$ est l'anneau des entiers de $Q(\theta)$

Soit $\theta$ un nombre cubique cyclique construit avec $(\beta, S)$ (cf. théorème 1.1). On cherche des conditions pour que l'anneau des entiers de $Q(\theta)$ soit $Z[\theta]$.

*Lemme 3.1* Soit $\theta$ un nombre cubique cyclique, construit avec $(\beta, S)$, tel que $Z[\theta]$ soit l'anneau des entiers de $Q(\theta)$. Alors $\beta = \frac{b+d}{c}j + \frac{b}{c}j^2$, où $d$ est égal à 1 ou à 3 et où $b$ et $c$ sont des entiers rationnels premiers entre eux.

*Démonstration* Soit $\beta = b_1 j + b_2 j^2$. $b_1$ et $b_2$ sont des nombres rationnels. $1, \theta, \theta^2$ étant une base d'entiers de $Q(\theta)$, on a

$$\frac{\Delta(1, \theta, \sigma\theta)}{\Delta(1, \theta, \theta^2)} \in Z.$$