**Zeitschrift:** L'Enseignement Mathématique

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

**Band:** 18 (1972)

**Heft:** 1: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** ÉTUDE ARITHMÉTIQUE DES CORPS CYCLIQUES DE DEGRE p' SUR LE CORPS DES NOMBRES RATIONNELS

**Autor:** Oriat, Bernard

**Kapitel:** II.3. DÉCOMPOSITION D'UN NOMBRE q PREMIER, NON RAMIFIÉ DANS $K_r$

**DOI:** https://doi.org/10.5169/seals-45361

Alors le corps d'inertie de $p$ dans $\Omega(n)$ est $\Omega(n')$ et son groupe d'inertie $T(n, n')$.

Soit $\pi$ l'application canonique de $G(n)$ sur $G({}^{K}/_{Q})$ qui à tout automorphisme de $\Omega(n)$ fait correspondre sa restriction à $K$. $\pi$ a pour noyau $G({}^{\Omega(n)}/_{K})$ et comme $\Omega(n)$ est le plus petit corps cyclotomique contenant $K$, on a donc:

$$\Omega(n') \not\supseteq K \quad \text{c'est-à-dire} \quad T(n, n') \not\subseteq G({}^{\Omega(n)}/_{K}) .$$

$\pi\big(T(n, n')\big)$ qui est le groupe d'inertie de $p$ dans $K$, n'est donc pas réduit à l'identité et $p$ se ramifie dans $K$.

## II.3. Décomposition d'un nombre $q$ premier, non ramifié dans $K_r$

$K_r$ désigne une extension cyclique de degré $p^r$ sur $Q$ ($p$ premier) et $(\Omega(n_i))_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée. Les notations restent les mêmes qu'au premier chapitre. $q$ est un nombre premier non ramifié dans $K_r$, c'est-à-dire d'après le lemme précédent, premier avec $n_r$.

Si $p$ est impair et suivant que $u_r = 0$ ou $u_r \geqq 2$,

soit
$$q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$
ou
$$q \equiv b_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r) ,$$

la décomposition de $q$ dans $G(n_r)$.

On posera alors:

— Si
$$2 \leqq u_r \leqq r : V(q) = \alpha_0\beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

— Si
$$u_r = r + 1 : V(q) = \sum_{1 \leq j \leq m_r} \alpha_j\beta_j - \beta_0$$

— Si
$$u_r = 0 : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

De même si $p = 2$ et suivant que $u_r = 0$, ou $u_r = 2$, ou $u_r \geqq 3$, soit

$$q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} (n_r) \qquad \text{ou} \qquad q \equiv a_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$

ou

$$q \equiv a_0^{\beta_0} {a'_0}^{\beta'_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$

la décomposition de $q$ dans $G(n_r)$. On posera alors:

— Si

$$3 \leqq u_r \leqq r+1 : V(q) = \alpha_0\beta_0 + \alpha'_0\beta'_0 + \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

— Si

$$u_r = r+2 \quad : V(q) = \sum_{0 \leq j \leq m_r} \alpha_j\beta_j - \beta'_0$$

— Si

$$u_r = 2 \quad : V(q) = 2^{r-1}\beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

— Si

$$u_r = 0 \quad : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

Proposition II.1.

Soient $K_r$ une extension cyclique de degré $p^r$ sur $Q$ et $q$ un nombre premier, ne divisant pas $n_r$. Alors la décomposition de $q$ en idéaux premiers de $K_r$ est de la forme:

$$q = \prod_{1 \leq v \leq g_q} \mathfrak{q}_v$$

et $g_q$ est le $PGCD$ de $p^r$ et de $V(q)$.

Le groupe de décomposition de $q$ dans $\Omega(n_r)$ est le sous-groupe de $G(n_r)$ engendré par la classe de $q$ modulo $n_r$ et la restriction de $q$, considéré comme automorphisme de $\Omega(n_r)$, à $K_r$ engendre le groupe de décomposition de $q$ dans $K_r$.

Le degré résiduel $f_q$ de $q$ dans $K_r$ est donc l'ordre de $q\,S_r$ dans $\dfrac{G(n_r)}{S_r}$. Supposons par exemple $p$ impair et $2 \leqq u_r \leqq r$ et considérons alors:

$$\begin{aligned} s &= (c_1^{\alpha_0} b_0)^{\beta_0} (c_1^{\alpha_2} c_2)^{\beta_2} \ldots (c_1^{\alpha_{m_r}} c_{m_r})^{\beta_{m_r}} \\ &= b_0^{\beta_0} c_1^{V(q)+\beta_1} c_2^{\beta_2} \ldots c_{m_r}^{\beta_{m_r}} \end{aligned}$$

D'après la proposition I.3, $s \in S_r$ et l'on a modulo $n_r$:

$$sq^{-1} = c_1^{V(q)}.$$

$f_q$ est donc égal à l'ordre de $c_1^{V(q)}\,S_r$ dans $\dfrac{G(n_r)}{S_r}$ et comme l'ordre de $c_1 S_r$

est $p^r$ (lemme I.2), on a donc:

$$f_q = \frac{p^r}{PGCD\left(p^r, V(q)\right)}$$

et

$$g_q = PGCD\left(p^r, V(q)\right).$$

## II.4. Indice de ramification dans une extension $K_r$

Proposition II.2.

Soient $K_r$ une extension cyclique de degré $p^r$ sur $Q$ et $\left(\Omega(n_i)\right)_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée à $K_r$. Pour tout $i$ de 1 à $r$ et tout $j$ tel que $m_{i-1} < j \leq m_i$, l'indice de ramification de $p_j$ dans $K_r$ est $p^{r-i+1}$.
Si $u_r \neq 0$, l'indice de ramification de $p$ dans $K_r$ est $p^{r-l+1}$.

Soit $j$ tel que $m_{i-1} < j \leq m_i$. $p_j$ divise donc $n_i$ et ne divise pas $n_{i-1}$. C'est-à-dire que $p_j$ se ramifie dans $\Omega(n_i)$ et ne se ramifie pas dans $\Omega(n_{i-1})$. D'après le lemme II.1, ceci implique que $p_j$ se ramifie dans $K_i$ et ne se ramifie pas dans $K_{i-1}$. $K_{i-1}$ est donc le corps d'inertie de $p_j$ dans $K_r$ et l'indice de ramification de $p_j$ dans $K_r$ est égal à: $[K_r : K_{i-1}]$.

De même si $u_r \neq 0$, $K_{l-1}$ est le corps d'inertie de $p$ dans $K_r$.

## II.5. Discriminant de $K_r$

Proposition II.3.

$K_r$ est une extension cyclique de degré $p^r$ sur $Q$ et $\left(\Omega(n_i)\right)_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée. Le discriminant de $K_r$ sur $Q$ est:

— *Dans le cas où* $u_r = 0$:

$$\prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{p^{i-1}(p^{r-i+1}-1)}$$

— *Dans le cas où* $p$ est impair et $u_r \geq 2$:

$$p^{p^{l-1}\left((r-l+2)p^{r-l+1} - \frac{p^{r-l+1}-1}{p-1} - 1\right)} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{p^{i-1}(p^{r-i+1}-1)}$$