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.5. Discriminant de K_r

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

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

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

et

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

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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $u_r \geq 2$:

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

— *Dans le cas où* $p = 2$ et $u_r = 2$:

$$2^{2^r} \prod_{1 \le i \le r} \prod_{m_{i-1} < j \le m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

— *Dans le cas où* $p = 2$ et $u_r \geqq 3$:

$$2^{2^{l-1}((r-l+2)2^{r-l+1}-1)} \prod_{1 \le i \le r} \prod_{m_{i-1} < j \le m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

Supposons tout d'abord $u_r = 0$. Désignons par A l'anneau des entiers de K_r. Pour tout j de 1 à m_r soit $p_j A = \prod_{1 \leqq v \leqq g_j} \mathfrak{p}_{jv}^{e_j}$ la décomposition de $p_j A$ dans K_r et soit f_j le degré résiduel de p_j dans K_r. Les p_j étant les seuls nombres premiers ramifiés dans K_r et leurs indices de ramification e_j étant premiers à p_j, la différente δ de K_r sur Q est:

$$\delta = \prod_{1 \le j \le m_r} \prod_{1 \le v \le g_j} \mathfrak{p}_{jv}^{e_j - 1}$$

Le déterminant D_f, de K_r sur Q, est donc $D = N_{K_r/Q}(\delta)$ et comme $N_{K_r/Q}(\mathfrak{p}_{jv}) = p_j^f$ on obtient:

$$D = \prod_{1 \le j \le m_r} p_j^{f_j g_j (e_j - 1)}$$

qui s'écrit également:

$$D = \prod_{1 \le i \le r} \prod_{m_{i-1} < j \le m_i} p_j^{f_j g_j (e_j - 1)} .$$

Si $m_{i-1} < j \leqq m_i$, alors $e_j = p^{r-i+1}$ d'après la proposition II.2 et comme $e_j f_j g_j = p^r$, on obtient le résultat annoncé.

Supposons maintenant p impair et $u_r \geqq 2$.
Dans ce cas u_r et l sont liés par la relation $u_r = r - l + 2$. On notera toujours D le discriminant de K_r sur Q et on introduit la décomposition $\delta = \delta_0 \delta_1 \dots \delta_{m_r}$ de la différente de K_r sur Q, en idéaux: $\delta_0, \delta_1, \dots \delta_{m_r}$, tels que $D_0 = N_{K_r/Q}(\delta_0)$ soit une puissance de p et tels que $D_j = N_{K_r/Q}(\delta_j)$ soit une puissance de p_j. D s'écrira alors $D = D_0 D_1 \dots D_{m_r}$. Le calcul de $D_1 D_2 \dots D_{m_r}$ s'effectue comme dans la démonstration précédente. Pour calculer D_0, on introduit la différente δ' de $\Omega(n_r)$ sur K_r décomposée de la même façon en $\delta' = \delta_0' \delta_1' \dots \delta_{m_r}'$ et $D'' = D_0'' D_1'' \dots D_{m_r}''$ le discriminant de $\Omega(n_r)$ sur Q.
La formule de transitivité sur les différentes donne:

$$D_0'' = N_{\Omega(n_r)/Q}(\delta_0 \delta_0') = N_{\Omega(n_r)/Q}(\delta_0') \, N_{K_r/Q}(\delta_0^{[\Omega(n_r):K_r]})$$

d'où

$$D_0'' = N_{\Omega(n_r)/Q}(\delta_0')\, D_0^{\frac{\varphi(n_r)}{p^r}}$$

Calcul de $N_{\Omega(n_r)/Q}(\delta_0')$:

Soient A et A_Ω les anneaux d'entiers respectifs de K_r et $\Omega(n_r)$ et soit $pA = \prod_{1 \leq v \leq g} \mathfrak{p}_v^e$ la décomposition de pA dans K_r et f le degré résiduel de p dans K_r. Soient:

$\mathfrak{p}_v A_\Omega = \prod_{1 \leq v' \leq g'} \mathfrak{p}_{vv'}^{e'}$ la décomposition de $\mathfrak{p}_v A_\Omega$ dans $\Omega(n_r)$ et f' le degré résiduel de $\mathfrak{p}_v$ dans $\Omega(n_r)$. L'indice de ramification e de p dans K_r est p^{r-l+1} (proposition II.2) et puisque l'indice de ramification ee' de p dans $\Omega(n_r)$ est $\varphi(p^{u_r}) = (p-1)\,p^{r-l+1}$, on a donc $e' = p - 1$ et e' est premier à p. On en déduit que:

$$\delta_0' = \prod_{\substack{1 \leq v \leq g \\ 1 \leq v' \leq g'}} \mathfrak{p}_{vv'}^{p-2}$$

et comme $N_{\Omega(n_r)/Q}(\mathfrak{p}_{vv'}) = p^{ff'}$, on aura donc:

$$N_{\Omega(n_r)/Q}(\delta_0') = p^{ff'gg'(p-2)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}}$$

D'autre part on a $D_0'' = p^{\varphi(n_r)\left(r-l+2-\frac{1}{p-1}\right)}$ d'où l'égalité:

$$p^{\varphi(n_r)\left(r-l+2-\frac{1}{p-1}\right)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}}\, D_0^{\frac{\varphi(n_r)}{p^r}}$$

dont on extrait la valeur de D_0.

Dans le cas $p = 2$ et $u_r = 2$; gardant les mêmes notations on a $e' = 1$ et $\delta_0' = 1$. On utilise alors comme précédemment la valeur $D_0'' = 2^{\varphi(n_r)}$.

Supposons maintenant $p = 2$ et $u_r \geq 3$:

On garde les mêmes notations que précédemment. On a cette fois: $u_r = r - l + 3$ et l'indice de ramification ee' de 2 dans $\Omega(n_r)$ est maintenant 2^{r-l+2} d'où $e' = 2$. δ_0' ne peut donc être obtenue comme précédemment. On introduit un corps E compris entre K_r et $\Omega(n_r)$ de la façon suivante: reprenant les notations introduites dans la proposition I.3 *bis* posons:

$$h = a_0'^{\,2^{l-1}\frac{\alpha_0}{}}\, a_0 \qquad \text{et} \qquad S = \{h, 1\}.$$

h est d'ordre 2, S est donc un sous-groupe de $G(n_r)$. Dans le cas où $l = 1$, c'est-à-dire $u_r = r + 2$, il apparaît immédiatement que S est inclus dans S_r. Si $l \geq 2$, c'est-à-dire si $3 \leq u_r \leq r + 1$ on constate que:

$\left(\frac{\alpha_0'}{2^{l-1}}+1\right)\alpha_0 \equiv 0\,(2^r)$ et qu'il existe donc un entier β tel que:

$$\left(\frac{\alpha_0'}{2^{l-1}}+1\right)\alpha_0 + 2^r\beta = p_1 - 1\,.$$

D'où

$$h = (c_1^{\alpha_0'}a_0')^{\frac{\alpha_0}{2^{l-1}}}\; c_1^{\alpha_0}\, a_0\, c_1^{2^r\beta}$$

qui montre que S est inclus dans S_r. E désigne le corps fixe de S, E contient donc K_r.

Le groupe d'inertie de 2 dans $\Omega\,(n_r)$ est $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$, le groupe d'inertie de $\mathfrak{p}_{vv}$, sur E sera donc $T\left(n_r, \frac{n_r}{2^{u_r}}\right) \cap S = S$. $\mathfrak{p}_v$ n'est donc pas ramifié dans E et la différente de E sur K_r est première avec 2.

Si D' est le discriminant de E sur Q, et D_0' la plus grande puissance de 2 divisant D', on aura alors:

$$D_0' = N_{E/Q}(\delta_0) = N_{E/K_r}(D_0) = D_0^{\frac{\varphi(n_r)}{2^{r+1}}}$$

Il reste à calculer D_0'. Pour cela introduisons A_E l'anneau des entiers de E et ξ une racine primitive $(n_r)^{\text{eme}}$ de 1. A partir de l'égalité: $\xi^2 = -\xi^{h+1} + (\xi+\xi^h)\,\xi$, on constate par récurrence sur t que ξ^t peut toujours se mettre sous la forme $a + b\xi$, avec a et b dans A_E. Comme $\{1, \xi, \ldots \xi^{\varphi(n_r)-1}\}$ est une base des entiers de $\Omega\,(n_r)$ sur Z, on en déduit que $\{1, \xi\}$ est une base des entiers de $\Omega\,(n_r)$ sur A_E. Le polynome $X^2 - (\xi+\xi^h)\,X + \xi^{h+1}$ est le polynome minimal de ξ sur E et la différente δ'' de $\Omega\,(n_r)$ sur E sera donc l'idéal engendré par $\xi - \xi^h$.

La formule de transitivité sur les différentes appliquée entre Q, E et $\Omega\,(n_r)$ va donner:

$$D'' = D'^{[\Omega(n_r):E]}\, N_{\Omega(n_r)/Q}(\delta'') = D'^2\, N_{\Omega(n_r)/Q}(\delta'')$$

Pour obtenir la valeur de $N_{\Omega(n_r)/Q}(\delta'')$, montrons que ξ^{h-1} est une racine primitive $(2^{r-l+2})^{\text{eme}}$ de 1. En effet:

$h \in T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ donc $h - 1 \equiv 0\left(\frac{n_r}{2^{u_r}}\right)$ et d'autre part, h étant premier à 2, on a $h - 1 \equiv 0\,(2)$.

Mais $h-1 \not\equiv 0\,(4)$, sinon h appartiendrait à $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$ et ce sous-groupe est engendré par a_0'.

On a donc finalement

$$h-1 \equiv 0\left(\frac{n_r}{2^{r-l+2}}\right) \quad \text{et} \quad h-1 \not\equiv 0\left(\frac{n_r}{2^{r-l+1}}\right)$$

On en déduit que

$$N_{\Omega(2^{r-l+2})/Q}(1-\xi^{h-1}) = 2$$

et

$$N_{\Omega(n_r)/Q}(\delta'') = 2^{\frac{\varphi(n_r)}{2^{r-l+1}}}.$$

Comme D_0'' est égal à $2^{\varphi(n_r)(r-l+2)}$, on en déduit les égalités:

$$2^{\varphi(n_r)(r-l+2)} = D'^2 \,.\, 2^{\frac{\varphi(n_r)}{2^{r-l+1}}} = D_0^{\frac{\varphi(n_r)}{2^r}} \,.\, 2^{\frac{\varphi(n_r)}{2^{r-l+1}}}$$

D'où l'on déduit la valeur de D_0.

Proposition II.4.

> Le discriminant de K_r, extension cyclique de degré p^r sur Q, ne dépend que de la suite de corps cyclotomiques associée à K_r. Réciproquement, si deux extensions cycliques de degré p_r sur Q, ont même discriminant sur Q, alors leurs suites de corps cyclotomiques sont égales.

C'est une conséquence de la proposition II.3.

Précisons pour la réciproque, que si K_r est une extension cyclique de degré p^r sur Q (p premier, par exemple) et si l'on connaît son discriminant D sur Q, alors les nombres premiers divisant n_r sont exactement ceux qui divisent D. L'exposant de p_j dans la décomposition de D en facteurs premiers n'est pas divisible par p^i si et seulement si $j \leqq m_i$ c'est-à-dire si et seulement si p_j divise n_i. Ceci permet de préciser quels sont les diviseurs de n_i distincts de p. Si p ne divise pas D, on a $u_r = 0$ et alors tous les u_i sont nuls. Si p divise D, et comme $(r-l+2)\,p^{r-l+1} - \dfrac{p^{r-l+1}-1}{p-1} - 1$ est premier à p, on obtient, à partir de la valeur de l'exposant de p dans la décomposition de D, la valeur de l, donc la suite $(u_i)_{1 \leqq i \leqq r}$.