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: I.9. Conditions d'inclusion de K_r dans $K_{r'}$

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

choix d'un sous-groupe S_r. Il suffit alors de chercher le nombre de valeurs que peuvent prendre les α_j vérifiant cette condition, I.3.A et I.3.B.

PROPOSITION I.5 *bis*.

Etant donnée une suite de corps cyclotomiques $(\Omega(n_i))_{1 \leqq i \leqq r}$ vérifiant les conditions I.2.A *bis* et I.2.B *bis*, le nombre d'extensions K_r, de degré 2^r sur Q, cycliques sur Q, admettant comme suite de corps cyclotomiques associée, la suite $(\Omega(n_i))_{1 \leqq i \leqq r}$ est:

— *Dans le cas où* $3 \leqq u_r \leqq r + 1$:

$$2^{r-l+1}\, 2^{(r-1)(m_1-1)} \prod_{2 \leq i \leq r} 2^{(r-i)(m_i - m_{i-1})}$$

— *Dans le cas où* $u_r = r + 2$, en posant $m_0 = 0$:

$$2 \prod_{1 \leq i \leq r} 2^{(r-i)(m_i - m_{i-1})}$$

— *Dans le cas où* $u_r = 0$ ou 2:

$$2^{(r-1)(m_1-1)} \prod_{2 \leq i \leq r} 2^{(r-i)(m_i - m_{i-1})}$$

I.9. CONDITIONS D'INCLUSION DE K_r DANS $K_{r'}$

PROPOSITION I.6.

Soit K_r une extension cyclique de degré p^r sur Q (p premier impair). Soit $(\Omega(n_i))_{1 \leqq i \leqq r}$ la suite de corps cyclotomiques associée à K_r et soit r' un entier strictement supérieur à r.

Il existe une extension $K_{r'}$ cyclique de degré $p^{r'}$ sur Q, contenant K_r, si et seulement si la suite $(\Omega(n_i))_{1 \leqq i \leqq r}$ vérifie la condition:

I.6.A : Pour tout i de 1 à r et tout $j \leqq m_i$, $p_j \equiv 1 \; (p^{r'-i+1})$.

Compte tenu de I.2.B, la condition I.6.A est nécessaire.

Pour montrer qu'elle est suffisante, construisons une extension $K_{r'}$ contenant K_r.

Plaçons-nous dans le cas où $2 \leqq u_r \leqq r$ et posons $n'_i = n_i$ pour $1 \leqq i \leqq r$ et $n'_i = p^{i-r} n_r$ pour $r < i \leqq r'$. La suite $(\Omega(n'_i))_{1 \leqq i \leqq r'}$ vérifie alors les conditions I.2.A et I.2.B.

Soit π la surjection de $G(n'_{r'})$ sur $G(n_r)$ qui à toute classe modulo $n'_{r'}$ fait correspondre la classe modulo n_r qui la contient. C'est aussi l'application qui à tout automorphisme de $\Omega(n'_{r'})$ fait correspondre sa restriction à $\Omega(n_r)$.

Soient $b_0', c_1', c_2', \ldots c_{m_r}'$ des générateurs des sous-groupes

$$T\left(n_{r'}', \frac{n_{r'}'}{p^{u_{r'}}}\right), T\left(n_{r'}', \frac{n_{r'}'}{p_1}\right), \ldots T\left(n_{r'}', \frac{n_{r'}'}{p_{m_r}}\right)$$

et soit

$$b_0 = \pi(b_0'), c_1 = \pi(c_1'), \ldots c_{m_r} = \pi(c_{m_r}').$$

Alors $b_0, c_1, \ldots c_{m_r}$ sont des générateurs de

$$T\left(n_r, \frac{n_r}{p^{u_r}}\right), T\left(n_r, \frac{n_r}{p_1}\right), \ldots T\left(n_r, \frac{n_r}{p_{m_r}}\right).$$

Soit S_r le sous-groupe de $G(n_r)$ admettant K_r comme corps fixe. D'après la proposition I.3, il existe $\alpha_0, \alpha_2, \ldots \alpha_{m_r}$ vérifiant I.3.A et I.3.B et tels que S_r soit engendré par:

$$\{ c_1^{p^r}, c_1^{\alpha_0} b_0, c_1^{\alpha_j} c_j ; 2 \leqq j \leqq m_r \}.$$

Soit $S_{r'}'$ le sous-groupe de $G(n_{r'}')$ engendré par: $\{ c_1'^{p^{r'}}, c_1'^{\alpha_0} b_0', c_1'^{\alpha_j} c_j' ; 2 \leqq j \leqq m_r \}$ et soit $K_{r'}$ le sous-corps de $\Omega(n_{r'}')$ corps fixe de $S_{r'}'$. D'après la proposition I.4, $K_{r'}$ est une extension cyclique de degré $p^{r'}$ de Q.

D'autre part, on vérifie que $\pi(S_{r'}') \subset S_r$ qui prouve que $K_{r'}$ contient K_r.

Remarque : On a construit, en fait, plusieurs extensions $K_{r'}'$ contenant K_r. S_r étant donné, les α_i ne sont déterminés que modulo p^r et si l'on remplace α_i par α_i' tel que $\alpha_i \equiv \alpha_i' (p^r)$ et $\alpha_i \not\equiv \alpha_i' (p^{r'})$ on obtiendra un autre sous-groupe $S_{r'}'$.

Dans le cas où $u_r = r + 1$, la démonstration est analogue.

Dans le cas où $u_r = 0$, on pose simplement $n_i' = n_r$ pour tout i entre r et r' et l'application π est alors l'identité.

PROPOSITION I.6 *bis*.

Soit K_r une extension cyclique de degré 2^r sur Q, $(\Omega(n_i))_{1 \leqq i \leqq r}$ la suite de corps cyclotomiques associée à K_r et soit r' un entier strictement supérieur à r. Il existe une extension $K_{r'}$ cyclique de degré $2^{r'}$ sur Q, contenant K_r si et seulement si:

I.6.A bis : Pour tout i de 1 à r et tout $j \leqq m_i$, $p_j \equiv 1 \ (2^{r'-i+1})$.

I.6.B bis : K_r est réelle.

I.6.A *bis* s'obtient à partir de I.2.B *bis*.

D'autre part il est nécessaire que K_r soit réelle car: $(-1)^2 = 1 \in S_r$, implique, d'après le lemme I.1, $-1 \in S_i$ pour tout $i < r'$. Donc tous les sous-corps stricts de $K_{r'}$ sont réels.

Pour démontrer la réciproque, on peut remarquer que:

si $u_r = 0$, -1 se décompose dans les sous-groupes $T\left(n_r, \frac{n_r}{p_j}\right)$ de la façon suivante:

$$-1 = \prod_{1 \leq j \leq m_r} c_j^{\frac{p_j - 1}{2}}.$$

On déduit de la condition I.6.A *bis* que si $j \leqq m_i$, alors $\frac{p_j - 1}{2} \equiv 0\ (2^{r-i+1})$ et compte tenu du lemme I.2 *bis*, $c_j^{\frac{p_j-1}{2}} \in S_r$. Donc $-1 \in S_r$ et K_r est réelle.

Donc si $u_r = 0$, I.6.B *bis* est une conséquence de I.6.A *bis* et on démontre l'existence de $K_{r'}$ comme précédemment.

Si maintenant $u_r \geqq 2$, -1 se décompose dans $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ et $T\left(n_r, \frac{n_r}{p_j}\right)$ sous la forme:

$$-1 = a_0 \prod_{1 \leq j \leq m_r} c_j^{\frac{p_j - 1}{2}}.$$

La condition I.6.A *bis* implique donc comme précédemment, que $c_j^{\frac{p_j-1}{2}} \in S_r$ d'où $-a_0 \in S_r$.

Si $u_r = 2$, $a_0 \notin S_r$ (lemme I.2 *bis*) donc les conditions I.6.A *bis* et I.6.B *bis* sont incompatibles.

Si $u_r \geqq 3$, les conditions I.6.A *bis* et I.6.B *bis* impliquent donc $a_0 \in S_r$, d'où $\alpha_0 \equiv 0\ (2^r)$.

On termine la démonstration comme précédemment.

Chapitre II

DÉCOMPOSITION, RAMIFICATION, DISCRIMINANT

II.1. Rappels

Soient K et K' deux corps de nombres, K' étant abélien sur K. Soient A et A' leurs anneaux d'entiers respectifs et $\mathfrak{p}$ un idéal premier de A. $\mathfrak{p}A'$ se décompose en idéaux premiers de A' sous la forme: $\mathfrak{p}A' = (\prod_{1 \leqq v \leqq g} \mathfrak{p}_v)^e$