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.6. Système de générateurs de S_r. Cas où p=2

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

— Si $m_{i-1} < j \leqq m_i$ alors $p^{r-i+1} e_j \in H_r$ et $p^{r-i} e_j \notin H_r$.

On en déduit tout d'abord que $(p-1)\, p^{r-l+1} e_0 \in H_r$ et compte tenu de la condition I.2.B $(p_j - 1)\, e_j \in H_r$ pour $1 \leqq j \leqq m_r$. Le noyau de μ qui a pour base: $\{(p-1)\, p^{r-l+1} e_0, (p_1 - 1)\, e_1, \ldots (p_{m_r} - 1)\, e_{m_r}\}$ est donc contenu dans H_r.

On a donc $H_r = \mu^{-1}(S_r)$ et $\dfrac{Z^{m_r+1}}{H_r}$ est isomorphe à $\dfrac{G(n_r)}{S_r}$.

Le degré de K_r sur Q est donc égal à

$$\operatorname{Card}\left(\frac{G(n_r)}{S_r}\right) = \operatorname{Card}\left(\frac{Z^{m_r+1}}{H_r}\right) = p^r.$$

Comme $p^{r-1} e_1 \notin H_r$, $\dfrac{Z^{m_r+1}}{H_r}$ est donc un groupe cyclique. K_r est donc cyclique sur Q.

Soient H_i les sous-modules de Z^{m_r+1} ayant pour bases $\{p^i e_1, f_0, f_2, \ldots f_{m_r}\}$, i de 1 à r. Soient S_i les sous-groupes de $G(n_r)$ définis par $S_i = \mu(H_i)$ et K_i les sous-corps de $\Omega(n_r)$ corps fixes de chacun des S_i.

Pour tout i de 1 à r, H_i contient H_r, donc K_i est un sous-corps de K_r. L'indice de H_r dans H_i est p^{r-i}, donc K_i est le sous-corps de K_r de degré p^i sur Q.

On a $p^{r-l+1} e_0 \in H_r$ et $p^{r-l} e_0 \notin H_r$. D'où $b_0^{p^{r-l+1}} \in S_r$ et $b_0^{p^{r-l}} \notin S_r$. Donc $b_0^{(p-1)p^{r-l}} \notin S_r$, $T\left(n_r, \dfrac{n_r}{p}\right) \nsubseteq S_r$ d'où $K_r \nsubseteq \Omega\left(\dfrac{n_r}{p}\right)$.

De même si $m_{i-1} < j \leqq m_i$, on a alors $c_j^{p^{r-i+1}} \in S_r$ et $c_j^{p^{r-i}} \notin S_r$, et compte tenu du lemme I.1, $c_j \in S_{i-1}$ et $c_j \notin S_i$, c'est-à-dire:

$$K_{i-1} \subseteq \Omega\left(\frac{n_r}{p_j}\right) \quad \text{et} \quad K_i \nsubseteq \Omega\left(\frac{n_r}{p_j}\right)$$

$(\Omega(n_i))_{1 \leqq i \leqq r}$ est donc la suite de corps cyclotomiques associée à K_r.

Dans les cas $u_r = 0$ et $u_r = r + 1$, la démonstration est analogue.

I.6. Système de générateurs de S_r. Cas où $p = 2$

Si K_r est une extension de degré 2^r sur Q, cyclique sur Q, on peut de la même façon donner un système de générateurs du sous-groupe S_r de $G(n_r)$.

On notera comme précédemment c_j un générateur de $T\left(n_r, \frac{n_r}{p_j}\right)$.

Si $u_r = 0$, $G(n_r)$ est produit direct des sous-groupes $T\left(n_r, \frac{n_r}{p_j}\right)$ j variant de 1 à m_r.

Si $u_r \geqq 2$, a_0 désigne l'élément de $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ tel que $a_0 \equiv -1\,(2^{u_r})$.

Si $u_r = 2$, a_0 engendre $T\left(n_r, \frac{n_r}{4}\right)$ et $G(n_r)$ est produit direct de $T\left(n_r, \frac{n_r}{4}\right)$ et des sous-groupes $T\left(n_r, \frac{n_r}{p_j}\right)$, j de 1 à m_r.

Si $u_r \geqq 3$, $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ est produit direct de $\{a_0, 1\}$ et de $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$.

On notera a_0' un générateur de $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$. $G(n_r)$ est alors produit direct des sous-groupes cycliques:

$$\{a_0, 1\}, \quad T\left(n_r, \frac{n_r}{2^{u_r-2}}\right), \quad \text{et} \quad T\left(n_r, \frac{n_r}{p_j}\right),$$

j variant de 1 à m_r.

PROPOSITION I.3 *bis*

Soit K_r une extension cyclique de degré 2^r sur Q, et soit $(\Omega(n_i))_{1 \leqq i \leqq r}$ la suite de corps cyclotomiques associée à K_r.

— *Dans le cas où* $3 \leqq u_r \leqq r+1$, il existe des nombres $\alpha_0, \alpha_0', \alpha_j$, pour $2 \leqq j \leqq m_r$, tels que S_r soit engendré par:

$$\{ c_1^{2^r}, c_1^{\alpha_0} a_0, c_1^{\alpha_0'} a_0', c_1^{\alpha_j} c_j ; 2 \leqq j \leqq m_r \}.$$

α_0 vérifie la condition: $\alpha_0 \equiv 0\,(2^{r-1})$.

α_0' vérifie la condition:

I.3.A bis : $\alpha_0' \equiv 0\,(2^{l-1})$ et $\alpha_0' \not\equiv 0\,(2^l)$.

Les α_j, pour $2 \leqq j \leqq m_r$, vérifient la condition:

I.3.B bis : Si $m_{i-1} < j \leqq m_i$, alors $\alpha_j \equiv 0\,(2^{i-1})$ et $\alpha_j \not\equiv 0\,(2^i)$.

— *Dans le cas où* $u_r = r + 2$, il existe des nombres α_j, pour $0 \leqq j \leqq m_r$, tels que S_r soit engendré par: $\{ a_0'^{\alpha_0} a_0, a_0'^{\alpha_j} c_j ; 1 \leqq j \leqq m_r \}$.

α_0 vérifie la condition: $\alpha_0 \equiv 0 \, (2^{r-1})$.

Les α_j, pour $1 \leqq j \leqq m_r$, vérifient la condition I.3.B *bis*.

— *Dans le cas où* $u_r = 2$, il existe des nombres α_j, pour $2 \leqq j \leqq m_r$, vérifiant la condition I.3.B *bis* et tels que S_r soit engendré par: $\{ c_1^{2^{r-1}} a_0, c_1^{\alpha_j} c_j ; 2 \leqq j \leqq m_r \}$.

— *Dans le cas où* $u_r = 0$, il existe des nombres α_j, pour $2 \leqq j \leqq m_r$, vérifiant la condition I.3.B *bis* et tels que S_r soit engendré par: $\{ c_1^{2^r}, c_1^{\alpha_j} c_j ; 2 \leqq j \leqq m_r \}$.

On démontre tout d'abord le lemme suivant:

LEMME I.2 *bis*

— Dans le cas où $u_r \geqq 3$, $a_0'^{2^{r-l+1}} = 1$ et $a_0'^{2^{r-l}} \notin S_r$.

— Dans le cas où $u_r = 2$, $a_0 \notin S_r$.

— Si $m_{i-1} < j \leqq m_i$ alors $c_j^{2^{r-i+1}} \in S_r$ et $c_j^{2^{r-i}} \notin S_r$.

En effet si $u_r \geqq 3$, la condition I.2.A *bis* implique $u_r = r - l + 3$. 2^{r-l+1} est donc de l'ordre de a_0 et d'autre part, si $a_0'^{2^{r-l}} \in S_r$, alors:

$$\left(T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)\right)^{(2^{r-l})} = T\left(n_r, \frac{n_r}{2}\right) \subseteq S_r \, .$$

D'où $K_r \subseteq \Omega\left(\frac{n_r}{2}\right)$ et $\Omega\,(n_r)$ ne serait pas le plus petit corps cyclotomique contenant K_r. De même si $u_r = 2$ et $a_0 \in S_r$ alors on aurait $K_r \subseteq \Omega\left(\frac{n_r}{4}\right)$.

Le reste de la démonstration est identique à la démonstration de I.3.

I.7. CONSTRUCTION D'EXTENSIONS CYCLIQUES DE DEGRÉ 2^r SUR Q

PROPOSITION I.4 *bis*

Réciproquement, soit r un entier positif et $(\Omega\,(n_i))_{1 \leqq i \leqq r}$ une suite de corps cyclotomiques vérifiant les conditions I.2.A *bis* et I.2.B *bis*.

— *Si* $3 \leqq u_r \leqq r + 1$, soient des nombres: $\alpha_0 \equiv 0 \, (2^{r-1})$, α_0', vérifiant I.3.A *bis*, α_j, pour $2 \leqq j \leqq m_r$, vérifiant I.3.B *bis*. Soit S_r