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.1. Rappels et notations
DOI: https://doi.org/10.5169/seals-45361

Q. J'ai montré que si une extension K_r ne vérifie pas ces conditions, on peut toujours obtenir une base d'entiers de K_r en complétant une base des entiers de K_{r-1}, sous-corps de K_r de degré p^{r-1}, avec $\varphi(p^r)$ conjugués d'un même entier.

Je tiens à exprimer ma profonde reconnaissance à M. le professeur Châtelet pour l'attention constante qu'il a manifestée à cette étude et pour les nombreux conseils qu'il m'a donnés.

Je remercie vivement M. le professeur Parizet qui a bien voulu examiner ce travail et faire partie du jury.

Je remercie également M. le professeur Bantegnie pour ses encouragements et M. le professeur Hellegouarch pour les entretiens qu'il a bien voulu m'accorder lors du commencement de ce travail.

Chapitre Premier

SUITE DE CORPS CYCLOTOMIQUES ASSOCIÉE A UNE EXTENSION CYCLIQUE DE DEGRÉ p^r SUR Q

I.1. Rappels et notations

Le corps des rationnels sera noté Q. Si n est un entier positif et ξ une racine primitive n^{eme} de 1, $Q(\xi)$ est le n^{eme} corps cyclotomique et sera noté $\Omega(n)$. Le degré, $[\Omega(n): Q]$, de $\Omega(n)$ sur Q est $\varphi(n)$, φ est l'indicateur d'Euler. Si n est impair, on a $\Omega(n) = \Omega(2n)$; c'est le seul cas où $\Omega(n) = \Omega(n')$ avec $n \neq n'$.

$\frac{Z}{n}$ désigne l'anneau des classes résiduelles modulo n et $\left(\frac{Z}{n}\right)^*$ est l'ensemble des classes résiduelles modulo n, premières avec n. C'est aussi le groupe multiplicatif des éléments inversibles de $\frac{Z}{n}$.

$\Omega(n)$ est une extension abélienne de Q. On notera $G(n)$ son groupe de Galois. A tout automorphisme σ de $\Omega(n)$ correspond un élément de $\left(\frac{Z}{n}\right)^*$,

a, défini par $\sigma(\xi) = \xi^a$. Cette correspondance est un isomorphisme de groupes ne dépendant pas du choix de la racine primitive n^{eme}: ξ. On confondra par la suite les groupes $G(n)$ et $\left(\frac{Z}{n}\right)^*$ (cf. [1] chapitre VI).

Définition et propriétés des sous-groupes $T(n, d)$

Soit d un entier divisant n. On posera:

$T(n, d) = \{ h, h \in \left(\frac{Z}{n}\right)^*, h \equiv 1\,(d) \}$. $T(n, d)$ est le noyau de l'application de $\left(\frac{Z}{n}\right)^*$ sur $\left(\frac{Z}{d}\right)^*$ faisant correspondre à toute classe h modulo n, la classe h', modulo d, contenant h. C'est donc un sous-groupe de $\left(\frac{Z}{n}\right)^*$, d'ordre $\frac{\varphi(n)}{\varphi(d)}$.

Tout élément de $T(n, d)$ laisse invariant $\xi^{\frac{n}{d}}$ qui est une racine primitive d^{eme} de 1. Le sous-corps de $\Omega(n)$, corps fixe de $T(n, d)$ est donc $\Omega(d)$.

Soient d et d' deux entiers divisant n.

On a: $$T(n, d) \cap T(n, d') = T(n, PPCM(d, d'))$$

et $$T(n, d) \,.\, T(n, d') = T(n, PGCD(d, d')).$$

La première égalité est immédiate. On peut s'assurer de la deuxième en constatant d'une part que: $T(n, d) \,.\, T(n, d') \subseteq T(n, PGCD(d, d'))$ et que d'autre part l'égalité: $\varphi(d)\,\varphi(d') = \varphi(PPCM(d, d'))\,\varphi(PGCD(d, d'))$ et l'isomorphisme: $\frac{T(n, d) \cdot T(n, d')}{T(n, d)} \cong \frac{T(n, d')}{T(n, d) \cap T(n, d')}$ permettent de conclure que $T(n, d) \,.\, T(n, d')$ et $T(n, PGCD(d, d'))$ ont le même nombre d'éléments.

On déduit de cela que:

$$\Omega(n) \cap \Omega(n') = \Omega(PGCD(n, n'))$$

et

$$\Omega(n) \cdot \Omega(n') = \Omega(PPCM(n, n')).$$

En effet $\Omega(n)$ et $\Omega(n')$ sont inclus dans $\Omega(nn')$. Le sous-groupe de $G(nn')$ formé des $\Omega(n)$-automorphismes est $T(nn', n)$. Le sous-groupe de $G(nn')$ formé des $\Omega(n) \cap \Omega(n')$-automorphismes est $T(nn', n) \,.\, T(nn', n')$

et de même le sous-groupe des $\Omega(n)\,.\,\Omega(n')$-automorphismes est $T(nn', n) \cap T(nn', n')$. Ceci permet de parler du plus petit corps cyclotomique contenant une extension abélienne de Q.

Structure des groupes $\left(\frac{Z}{n}\right)^*$

Soit $n = p_1^{r_1} \ldots p_m^{r_m}$ la décomposition de n en facteurs premiers. Alors $\left(\frac{Z}{n}\right)^*$ est produit direct des sous-groupes $T\left(n, \frac{n}{p_i^{r_i}}\right)$, i variant de 1 à m.

En effet:

$$\prod_{1 \leqq i \leqq m} T\left(n, \frac{n}{p_i^{r_i}}\right) = T\left(n, PGCD\left(\frac{n}{p_i^{r_i}}\right)\right) = T(n, 1) = \left(\frac{Z}{n}\right)^*$$

et

$$T\left(n, \frac{n}{p_j^{r_j}}\right) \cap \prod_{i \neq j} \left(T\left(n, \frac{n}{p_i^{r_i}}\right)\right) = T\left(n, \frac{n}{p_j^{r_j}}\right) \cap T(n, p_j^{r_j}) = T(n, n) = 1\,.$$

Précisons que si h est un élément de $\left(\frac{Z}{n}\right)^*$ et si $h = h_1 h_2 \ldots h_m$ est sa décomposition dans les sous-groupes $T\left(n, \frac{n}{p_i^{r_i}}\right)$, c'est-à-dire si $h_i \in T\left(n, \frac{n}{p_i^{r_i}}\right)$ on a alors $h \equiv h_i\,(p_i^{r_i})$.

L'application θ_i de $T\left(n, \frac{n}{p_i^{r_i}}\right)$ sur $\left(\frac{Z}{p_i^{r_i}}\right)^*$ qui à tout élément h de $T\left(n, \frac{n}{p_i^{r_i}}\right)$ fait correspondre la classe h' de $\left(\frac{Z}{p_i^{r_i}}\right)^*$ contenant h est un isomorphisme et sa restriction à $T\left(n, \frac{n}{p_i^{r_i - s_i}}\right)$ a pour image $T(p_i^{r_i}, p_i^{s_i})$ pour tout s_i compris entre 0 et r_i.

Rappelons que si p est impair $\left(\frac{Z}{p^r}\right)^*$ est cyclique.

Si p_i est impair et si h appartient à $T\left(n, \frac{n}{p_i^{r_i}}\right)$, pour tout s_i compris entre 1 et r_i, $h^{(p_i - 1)p_i^{s_i - 1}}$ est congru à 1 modulo $p_i^{s_i}$, donc appartient à

$T\left(n, \frac{n}{p_i^{r_i - s_i}}\right)$. Comme d'autre part $T\left(n, \frac{n}{p_i^{r_i}}\right)$ est cyclique, $T\left(n, \frac{n}{p_i^{r_i - s_i}}\right)$ et $T\left(n, \frac{n}{p_i^{r_i}}\right)^{((p_i - 1)\, p_i^{s_i - 1})}$ *) possèdent le même nombre d'éléments. $T\left(n, \frac{n}{p_i^{r_i - s_i}}\right)$ est donc l'ensemble des puissances $((p_i - 1)\, p_i^{s_i - 1})^{\text{eme}}$ d'éléments de $T\left(n, \frac{n}{p_i^{r_i}}\right)$.

Rappelons que si $r \geqq 3$, $\left(\frac{Z}{2^r}\right)^*$ est produit direct de $\{-1, 1\}$ et de $T(2^r, 4)$. Si $p_i = 2$, $r_i \geqq 3$, posons $a_0 = \theta_i^{-1}(-1)$; $T\left(n, \frac{n}{2^{r_i}}\right)$ est produit direct de $\{a_0, 1\}$ et de $T\left(n, \frac{n}{2^{r_i - 2}}\right)$ qui est cyclique. Pour tout s_i entre 3 et r_i, $T\left(n, \frac{n}{2^{r_i - s_i}}\right)$ est alors l'ensemble des puissances $(2^{s_i - 2})^{\text{eme}}$ d'éléments de $T\left(n, \frac{n}{2^{r_i}}\right)$. C'est aussi l'ensemble des puissances $(2^{s_i - 2})^{\text{eme}}$ d'éléments de $T\left(n, \frac{n}{2^{r_i - 2}}\right)$.

I.2. Plus petit corps cyclotomique contenant une extension abélienne de degré p^r sur Q

Proposition I.1.

Soit r un entier positif, p un nombre premier impair, K une extension abélienne de degré p^r sur Q, $\Omega(n)$ le plus petit corps cyclotomique contenant K. Alors n est de la forme $n = p^s p_1 p_2 \ldots p_m$ et vérifie les conditions:

— $0 \leqq s \leqq r + 1$.

— $s \neq 1$.

— Les p_i sont des nombres premiers distincts et congrus à 1 modulo p.

*) $G^{(n)}$ désigne le sous-groupe de G formé des puissances n^{eme} d'éléments de G.