Zeitschrift: 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

Kapitel: I.2. Plus petit corps cyclotomique contenant une extension ABÉLIENNE DE DEGRÉ p^r SUR Q

Autor: Oriat, Bernard

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

$T\left(n, \frac{n}{p_i^{r_i - s_i}}\right)$. 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 $n = p^s p_1 p_2 \dots p_m$ 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.

Le théorème de Kronecker permet d'affirmer qu'il existe n' tel que $\Omega(n')$ contienne K. Soit $n' = p^u p_1^{u_1} \ldots p_m^{u_m}$ la décomposition de n' en facteurs premiers et soit S le sous-groupe de $G(n')$ constitué par les K-automorphismes.

1. Montrons que si $p_i \not\equiv 1\,(p)$, alors $K \subseteq \Omega\left(\dfrac{n'}{p_i^{u_i}}\right)$. Il est équivalent de montrer que $T\left(n', \dfrac{n'}{p_i^{u_i}}\right) \subseteq S$; soit $h \in T\left(n', \dfrac{n'}{p_i^{u_i}}\right)$, puisque $T\left(n', \dfrac{n'}{p_i^{u_i}}\right)$ est d'ordre $(p_i - 1)p_i^{u_i - 1}$, on aura donc: $h^{(p_i - 1)p_i^{u_i - 1}} = 1_{\Omega(n')}$ ($1_{\Omega(n')}$ désignant l'identité sur $\Omega(n')$). Si σ est la restriction de h à K, on aura également $\sigma^{(p_i - 1)p_i^{u_i - 1}} = 1_K$. D'autre part $\sigma^{p^r} = 1_K$ puisque K est de degré p^r sur Q. Comme $(p_i - 1)\, p_i^{u_i - 1}$ et p^r sont premiers entre eux, on en déduit que $\sigma = 1_K$ et $h \in S$.

2. Montrons que si $p_i \equiv 1\,(p)$, alors $K \subseteq \Omega\left(\dfrac{n'}{p^{u_i - 1}}\right)$. Cela revient à démontrer que $T\left(n', \dfrac{n'}{p_i^{u_i - 1}}\right) \subseteq S$.

Soit $h \in T\left(n', \dfrac{n'}{p_i^{u_i - 1}}\right)$, puisque ce sous-groupe est d'ordre $p_i^{u_i - 1}$, on aura donc $h^{p^{u_i - 1}} = 1_{\Omega(n')}$. D'où, σ étant la restriction de h à K, $\sigma^{p_i^{u_i - 1}} = 1_K$. D'autre part $\sigma^{p^r} = 1_K$ pour la même raison que précédemment. Comme $p_i^{u_i - 1}$ et p^r sont premiers entre eux, $\sigma = 1_K$ et $h \in S$.

3. Montrons que $s \leqq r + 1$, c'est-à-dire, montrons que si $u \geqq r + 2$ alors $K \subseteq \Omega\left(\dfrac{n'}{p^{u-r-1}}\right)$.

En effet si $u \geqq r + 2$, $T\left(n', \dfrac{n'}{p^{u-r-1}}\right) = T\left(n', \dfrac{n'}{p^u}\right)^{((p-1)p^r)}$. Tout élément $h \in T\left(n', \dfrac{n'}{p^{u-r-1}}\right)$ est donc une puissance $(p^r)^{\text{eme}}$. Il en est de même de la restriction de h à K qui est l'identité de K, puisque K est de degré p^r sur Q. On a donc $T\left(n', \dfrac{n'}{p^{u-r-1}}\right) \subseteq S$.

4. Montrons enfin que $s \neq 1$.

Pour cela, montrons que si $u = 1$, alors $K \subseteq \Omega\left(\dfrac{n'}{p}\right)$. Si $u = 1$, alors

$T\left(n', \frac{n'}{p}\right)$ a pour ordre $p - 1$ et comme $p - 1$ est premier à p^r, on en déduit $T\left(n', \frac{n'}{p}\right) \subseteq S$.

PROPOSITION I.1 *bis.*

Soit r un entier positif et K une extension abélienne de degré 2^r sur Q, $\Omega(n)$ le plus petit corps cyclotomique contenant K. Alors n est de la forme $n = 2^s p_1 p_2 \dots p_m$ et vérifie la condition

— $0 \leqq s \leqq r + 2$.

— Les p_i sont des nombres premiers impairs distincts.

La démonstration est analogue à la précédente. Pour montrer que $s \leqq r + 2$, on constate que si $u \geqq r + 3$ et si $n' = 2^u p_1^{u_1} \dots p_m^{u_m}$, alors

$$T\left(n', \frac{n'}{2^{u-r-2}}\right) = T\left(n', \frac{n'}{2^u}\right)^{2^r}.$$

I.3. SUITE DE CORPS CYCLOTOMIQUES ASSOCIÉE A UNE EXTENSION CYCLIQUE K_r

DÉFINITION:

Soit K_r une extension cyclique de degré p^r (p premier) sur Q. Pour i entre 1 et r soit K_i l'unique sous-corps de K_r de degré p^i sur Q. Soit $\Omega(n_i)$ le plus petit corps cyclotomique contenant K_i. On appellera « suite de corps cyclotomiques associée à K_r » la suite des r corps $\Omega(n_i)$.

PROPOSITION I.2.

Soit r un entier positif et p un nombre premier impair. Soit K_r une extension cyclique de degré p^r sur Q. Soit $(\Omega(n_i))_{1 \leqq i \leqq r}$ la suite de corps cyclotomiques associée à K_r.
Alors les n_i vérifient les conditions suivantes:

I.2.A. Pour tout i de 1 à r, la décomposition de n_i en facteurs premiers est $n_i = p^{u_i} p_1 \dots p_{m_i}$; la suite $(m_i)_{1 \leqq i \leqq r}$ est non décroissante. La suite $(u_i)_{1 \leqq i \leqq r}$ est non décroissante, éventuellement nulle.