I.3. Suite de corps cyclotomiques associée a une extension cyclique K_r

$T\left(n', \frac{n'}{p}\right)$ 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 $n = 2^s p_1 p_2 \ldots p_m$ et vérifie la condition

— $0 \leq s \leq r+2$.

— Les p_i sont des nombres premiers impairs distincts.

La démonstration est analogue à la précédente. Pour montrer que $s \leq r+2$, on constate que si $u \geq r+3$ et si $n' = 2^u p_1^{u_1} \ldots p_m^{u_m}$, 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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $n_i = p^{u_i} p_1 \ldots p_{m_i}$; la suite $(m_i)_{1 \leq i \leq r}$ est non décroissante. La suite $(u_i)_{1 \leq i \leq r}$ est non décroissante, éventuellement nulle.

Si les u_i ne sont pas tous nuls, soit l le plus petit entier tel que $u_l \neq 0$. On a alors $u_l = 2$ et $u_{i+1} = u_i + 1$ pour tout i entre l et $r-1$.

I.2.B. Si $j \leq m_i$ alors $p_j \equiv 1 \ (p^{r-i+1})$.

Démontrons tout d'abord le

LEMME I.1.

Soit K une extension abélienne de Q. K_r un sous-corps de K de degré p^r sur Q, cyclique sur Q; pour $1 \leq i \leq r$, soit K_i l'unique sous-corps de K_r de degré p^i sur Q.
Soit σ un automorphisme de K. Alors pour tout i entre 1 et r, σ^{p^i} est un K_r-automorphisme si et seulement si σ est un K_{r-i}-automorphisme.

Notons S_i le sous-groupe de $G(K/Q)$ (groupe de Galois de K sur Q), formé des K_i-automorphismes. Soit $\sigma \in S_{r-i}$; S_r est d'indice p^i dans S_{r-i} donc $\sigma^{p^i} \in S_r$. Réciproquement, si $\sigma^{p^i} \in S_r$, alors la restriction de σ à K_r, $\sigma \mid K_r$, est un élément d'ordre inférieur ou égal à p^i dans $G(K_r/Q)$. Puisque ce groupe est cyclique d'ordre p^r, $\sigma \mid K_r$ est une puissance $(p^{r-i})^{\text{eme}}$ et $\sigma \in S_{r-i}$.

Démonstration de la proposition I.2

S_i désigne maintenant le sous-groupe de $G(n_r)$ formé des K_i-automorphismes.

Condition I.2.A. D'après la proposition I.1, les n_i sont de la forme $n_i = p^{u_i} p_1 \dots p_{m_i}$. Puisque $K_i \subset K_{i+1}$, alors $\Omega(n_i) \subseteq \Omega(n_{i+1})$ et n_i divise n_{i+1}. Les suites (u_i) et (m_i) sont donc non décroissantes.

Supposons que les u_i ne soient pas tous nuls et montrons que $u_l = 2$. Si aucun des u_i n'est nul, c'est-à-dire si $l = 1$ alors $u_l = 2$ est une conséquence immédiate de la proposition I.1. Si $l \geq 2$, on a donc

$$u_{l-1} = 0 \quad \text{et} \quad K_{l-1} \subseteq \Omega(p_1 p_2 \dots p_{m_r})$$

c'est-à-dire

$$S_{l-1} \supseteq T(n_r, p_1 p_2 \dots p_{m_r}) .$$

Soit $h \in T(n_r, p^2 p_1 p_2 \dots p_{m_r})$; h est une puissance $((p-1)p)^{\text{eme}}$ d'un élément τ de $T(n_r, p_1 p_2 \dots p_{m_r})$. Or $\tau \in S_{l-1}$ et d'après le lemme I.1, $\tau^p \in S_l$ donc $h \in S_l$.

On a donc

$$T(n_r, p^2 p_1 p_2 \dots p_{m_r}) \subseteq S_l$$

d'où

$$K_l \subseteq \Omega(p^2 p_1 \dots p_{m_r}) \quad \text{et} \quad u_l \leqq 2 .$$

D'autre part, d'après la proposition I.1, $u_l \neq 0$ implique $u_l \geqq 2$.

Supposons $u_i \geqq 2$ et montrons que $u_{i+1} = u_i + 1$. Cette égalité équivaut aux deux relations

$$K_{i+1} \nsubseteq \Omega(p^{u_i} p_1 p_2 \dots p_{m_r})$$

et

$$K_{i+1} \subseteq \Omega(p^{u_i+1} p_1 p_2 \dots p_{m_r})$$

Première relation :

Supposons que

$$K_{i+1} \subseteq \Omega(p^{u_i} p_1 p_2 \dots p_{m_r})$$

c'est-à-dire

$$S_{i+1} \supseteq T(n_r, p^{u_i} p_1 p_2 \dots p_{m_r}) .$$

Soit

$$h \in T(n_r, p^{u_i-1} p_1 p_2 \dots p_{m_r}) .$$

Comme $u_i \geqq 2$, $h^p \in T(n_r, p^{u_i} p_1 p_2 \dots p_{m_r})$ d'où $h^p \in S_{i+1}$ et $h \in S_i$ d'après le lemme I.1. Ceci prouverait que $K_i \subseteq \Omega(p^{u_i-1} p_1 p_2 \dots p_{m_r})$, ce qui contredit la définition de u_i.

Deuxième relation :

On a

$$K_i \subseteq \Omega(p^{u_i} p_1 p_2 \dots p_{m_r})$$

d'où

$$S_i \supseteq T(n_r, p^{u_i} p_1 p_2 \dots p_{m_r})$$

et

$$S_i^{(p)} \supseteq T(n_r, p^{u_i} p_1 p_2 \dots p_{m_r})^{(p)} = T(n_r, p^{u_i+1} p_1 p_2 \dots p_{m_r})$$

D'autre part d'après le lemme I.1: $S_{i+1} \supseteq S_i^{(p)}$.
On a donc:

$$S_{i+1} \supseteq T(n_r, p^{u_i+1} p_1 p_2 \dots p_{m_r})$$

et

$$K_{i+1} \subseteq \Omega(p^{u_i+1} p_1 p_2 \cdots p_{m_r})$$

Condition I.2.B. Si $j \leq m_i$, alors $K_i \nsubseteq \Omega\left(\frac{n_r}{p_j}\right)$ c'est-à-dire $S_i \not\supseteq T\left(n_r, \frac{n_r}{p_j}\right)$ D'après le lemme I.1, ceci implique que $S_r \not\supseteq T\left(n_r, \frac{n_r}{p_j}\right)^{(p^{r-i})}$ et comme $S_r \supseteq T\left(n_r, \frac{n_r}{p_j}\right)^{(p^r)}$ on en déduit que $T\left(n_r, \frac{n_r}{p_j}\right)^{(p^{r-i})}$ contient strictement $T\left(n_r, \frac{n_r}{p_j}\right)^{(p^r)}$. Or $T\left(n_r, \frac{n_r}{p_j}\right)$ est un groupe cyclique d'ordre $p_j - 1$ et $T\left(n_r, \frac{n_r}{p_j}\right)^{(p^v)}$ est d'ordre $\frac{p_j - 1}{PGCD(p_j - 1, p^v)}$.

On a donc:

$$PGCD(p_j - 1, p^r) > PGCD(p_j - 1, p^{r-i})$$

d'où

$$p_j \equiv 1 \,(p^{r-i+1})$$

PROPOSITION I.2 *bis.*

Soit r un entier positif et K_r une extension cyclique de degré 2^r sur Q. Soit $(\Omega(n_i))_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée à K_r. Alors les n_i vérifient les conditions suivantes:

I.2.A bis. Pour tout i de 1 à r, la décomposition de n_i en facteurs premiers est $n_i = 2^{u_i} p_1 p_2 \ldots p_{m_i}$; la suite des $(m_i)_{1 \leq i \leq r}$ est non décroissante. La suite des u_i est non décroissante, éventuellement nulle. Si les u_i ne sont pas tous nuls, soit l le plus petit entier tel que $u_l \neq 0$:

— si $l = r$ alors $u_l = 2$ ou 3.

— si $l < r$ alors $u_l = 3$ et $u_{i+1} = u_i + 1$ pour tout i tel que $r > i \geq l$.

I.2.B bis. Si $j \leq m_i$ alors $p_j \equiv 1 \,(2^{r-i+1})$.

Montrons que $u_l \leqslant 3$. Si $l = 1$ c'est une conséquence immédiate de la proposition I.1 *bis*. Si $l \geqslant 2$, soit $h \in T(n_r, 2^3 p_1 \dots p_{m_r})$. h est le carré d'un élément $\tau \in T(n_r, p_1 \dots p_{m_r})$.
Or $S_{l-1} \supseteq T(n_r, p_1 \dots p_{m_r})$, donc $\tau \in S_{l-1}$ et $h \in S_l$ d'après le lemme I.1. D'où:

$$T(n_r, 2^3 p_1 \dots p_{m_r}) \subseteq S_l \quad \text{et} \quad K_l \subseteq \Omega(2^3 p_1 \dots p_{m_r}).$$

Montrons que si $l < r$, alors $u_l = 3$.
En effet supposons $u_l = 2$, alors $K_l \subseteq \Omega(2^2 p_1 \dots p_{m_r})$ c'est-à-dire $S_l \supseteq T(n_r, 2^2 p_1 \dots p_{m_r})$. Or $T(n_r, p_1 \dots p_{m_r})$ est produit direct de $T(n_r, 2^2 p_1 \dots p_{m_r})$ et d'un sous-groupe $\{1, a_0\}$ d'ordre 2. On a donc $a_0^2 = 1$ et $a_0^2 \in S_{l+1}$. D'où $a_0 \in S_l$ d'après le lemme I.1. D'où:

$$T(n_r, p_1 \dots p_{m_r}) \subseteq S_l \quad \text{et} \quad K_l \subseteq \Omega(p_1 \dots p_{m_r})$$

ce qui contredit la définition de l.

Pour montrer que $u_{i+1} = u_i + 1$ pour tout i entre l et $r - 1$, on utilise comme précédemment l'égalité:

$$T(n_r, 2^{u_i} p_1 \dots p_{m_r})^{(2)} = T(n_r, 2^{u_i+1} p_1 \dots p_{m_r})$$

La démonstration de la condition I.2.B *bis* est analogue à celle de la condition I.2.B.

I.4. Système de générateurs de S_r. Cas où p est impair

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

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.

b_0 désignera un générateur de $T\left(n_r, \frac{n_r}{p^{u_r}}\right)$ et pour tout j entre 1 et m_r, c_j un générateur de $T\left(n_r, \frac{n_r}{p_j}\right)$.