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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **15.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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: $\dfrac{T(n, d) \cdot T(n, d')}{T(n, d)} \cong \dfrac{T(n, d')}{T(n, d) \cap T(n, d')}$ 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 $n = p_1^{r_1} \dots p_m^{r_m}$ 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 $h = h_1 h_2 \dots h_m$ 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 $n = p^s p_1 p_2 \dots p_m$ 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 $n' = p^u p_1^{u_1} \dots p_m^{u_m}$ 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 $K \subseteq \Omega\left(\frac{n'}{p_i^{u_i}}\right)$. Il est équivalent de montrer que $T\left(n', \frac{n'}{p_i^{u_i}}\right) \subseteq S$; soit $h \in T\left(n', \frac{n'}{p_i^{u_i}}\right)$, puisque $T\left(n', \frac{n'}{p_i^{u_i}}\right)$ 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 $K \subseteq \Omega\left(\frac{n'}{p^{u_i - 1}}\right)$. Cela revient à démontrer que $T\left(n', \frac{n'}{p_i^{u_i-1}}\right) \subseteq S$.

Soit $h \in T\left(n', \frac{n'}{p_i^{u_i-1}}\right)$, 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 $K \subseteq \Omega\left(\frac{n'}{p^{u-r-1}}\right)$.

En effet si $u \geqq r + 2$, $T\left(n', \frac{n'}{p^{u-r-1}}\right) = T\left(n', \frac{n'}{p^u}\right)^{((p-1)p^r)}$. Tout élément $h \in T\left(n', \frac{n'}{p^{u-r-1}}\right)$ 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 $T\left(n', \frac{n'}{p^{u-r-1}}\right) \subseteq S$.

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

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

— $0 \leq s \leq r + 2$.

— 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 $n' = 2^u p_1^{u_1} \dots p_m^{u_m}$, 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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $n_i = p^{u_i} p_1 \dots p_{m_i}$; 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 $j \leqq m_i$ 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 $1 \leqq i \leqq r$, 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 $l \geqq 2$, 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 $S_i \nsupseteq T\left(n_r, \frac{n_r}{p_j}\right)$ D'après le lemme I.1, ceci implique que $S_r \nsupseteq T\left(n_r, \frac{n_r}{p_j}\right)^{(p^{r-i})}$ 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 $u_l \leqq 3$. Si $l = 1$ c'est une conséquence immédiate de la proposition I.1 *bis*. Si $l \geqq 2$, 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 $T\left(n_r, \dfrac{n_r}{p^{u_r}}\right)$ et $T\left(n_r, \dfrac{n_r}{p_j}\right)$ j variant de 1 à m_r.

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

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

PROPOSITION I.3.

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

— *Dans le cas ou* $2 \leq u_r \leq r$, il existe des nombres α_j, pour $j = 0$ et $2 \leq j \leq m_r$, tels que S_r soit engendré par:

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

α_0 vérifie la condition:

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

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

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

— *Dans le cas ou* $u_r = r + 1$, il existe des nombres α_j, pour $1 \leq j \leq m_r$, tels que S_r soit engendré par: $\{ b_0^{p^r}, b_0^{\alpha_j} c_j ; 1 \leq j \leq m_r \}$. Les α_j, pour $1 \leq j \leq m_r$, vérifient la condition I.3.B.

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

Démontrons tout d'abord le lemme suivant:

LEMME I.2.

— Si $u_r \neq 0$, $b_0^{p^{r-l+1}} \in S_r$ et $b_0^{p^{r-l}} \notin S_r$.

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

Supposons par exemple $2 \leq u_r \leq r$. On aura alors, d'après la condition I.2.A: $u_r = r - l + 2$ et $2 \leq l \leq r$. Il découle de la définition de l que

$$K_{l-1} \subseteq \Omega\left(\frac{n_r}{p^{u_r}}\right) \quad \text{et} \quad K_l \nsubseteq \Omega\left(\frac{n_r}{p^{u_r}}\right),$$

c'est-à-dire:

$$S_{l-1} \supseteq T\left(n_r, \frac{n_r}{p^{u_r}}\right) \quad \text{et} \quad S_l \not\supseteq T\left(n_r, \frac{n_r}{p^{u_r}}\right).$$

D'où $b_0 \in S_{l-1}$ et $b_0 \notin S_l$ et l'on obtient le résultat en utilisant le lemme I.1.

De même, si $m_{i-1} < j \leq m_i$ alors $K_{i-1} \subseteq \Omega\left(\frac{n_r}{p_j}\right)$ et $K_i \nsubseteq \Omega\left(\frac{n_r}{p_j}\right)$. D'où $T\left(n_r, \frac{n_r}{p_j}\right) \subseteq S_{i-1}$ et $T\left(n_r, \frac{n_r}{p_j}\right) \nsubseteq S_i$. Ce qui équivaut encore à $c_j \in S_{i-1}$ et $c_j \notin S_i$.

Démonstration de la proposition I.3

Soit $\{e_0, e_1, \dots e_{m_r}\}$ une base du Z-module Z^{m_r+1} et μ l'application Z-linéaire de Z^{m_r+1} sur $G(n_r)$ telle que $\mu(e_0) = b_0$ et $\mu(e_i) = c_i$ pour tout i entre 1 et m_r.

Pour tout sous-groupe S de $G(n_r)$, les groupes-quotients de Z^{m_r+1} par $\mu^{-1}(S)$ d'une part et de G par S d'autre part sont isomorphes. Posons $H_r = \mu^{-1}(S_r)$ et cherchons une base $\{f_0, f_1, \dots f_{m_r}\}$ de H_r aussi simple que possible.

Les conditions du lemme I.2 sont équivalentes à:

— $p^{r-l+1}e_0 \in H_r$ et $p^{r-l}e_0 \notin H_r$.

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

On peut préciser de plus, que $2 \leq l$ implique n_1 premier à p et comme on ne peut avoir $n_1 = 1$, p_1 divise donc n_1 et $m_1 \geq 1$. On aura donc $p^r e_1 \in H_r$ et $p^{r-1}e_1 \notin H_r$.

Cherchons une base de H_r: $\{f_0, f_1, \dots f_{m_r}\}$ telle que la matrice de $(f_1, f_0, f_2, \dots f_{m_r})$ par rapport à $(e_1, e_0, e_2, \dots e_{m_r})$ soit triangulaire c'est-à-dire:

$$f_1 = a_{11}\, e_1$$
$$f_j = \sum_{0 \leq k \leq j} a_{kj}\, e_k$$

On a

$$\operatorname{Det} A = \prod_{0 \leq j \leq m_r} |a_{jj}| = \operatorname{Card}\left(\frac{Z^{m_r+1}}{H_r}\right) = \operatorname{Card}\frac{G(n_r)}{S_r} = p_r\,.$$

Donc a_{11} divise p^r et comme d'autre part $p^{r-1}e_1 \notin H_r$, on en déduit que $|a_{11}| = p^r$ et $|a_{jj}| = 1$ pour tout j différent de 1.

On peut donc choisir $a_{11} = p^r$, $a_{jj} = 1$ et f_j de la forme $f_j = \alpha_j e_1 + e_j$ pour tout j différent de 1.

Si $m_{i-1} < j \leq m_i$, multipliant l'égalité $f_j = \alpha_j e_1 + e_j$, par p^{r-i+1} ou p^{r-i}, on constate que $\alpha_j p^{r-i+1} e_1 \in H_r$ et $\alpha_j p^{r-i} e_1 \notin H_r$. D'où $\alpha_j \equiv 0\,(p^{i-1})$ et $\alpha_j \not\equiv 0\,(p^i)$. On obtient de même $\alpha_0 \equiv 0\,(p^{l-1})$ et $\alpha_0 \not\equiv 0\,(p^l)$.

L'ensemble des $\mu(f_j)$, j de 0 à m_r, est un système de générateurs de S_r.

Dans les autres cas, on procède de la même façon: si $u_r = r + 1$, on a $l = 1$, $b_0^{p^r} \in H_r$ et $b_0^{p^{r-1}} \notin H_r$. On place donc b_0 en premier, c'est-à-dire que l'on cherche une base $(f_0, f_1, \dots f_{m_r})$ de H_r telle que la matrice A de $(f_0, f_1, \dots f_{m_r})$ par rapport à $(e_0, e_1, e_2 \dots e_{m_r})$ soit triangulaire.

Remarque: S_r n'est pas en général, produit direct des sous-groupes cycliques engendrés par chacun des générateurs obtenus.

I.5. Construction d'extensions cycliques K_r de degré p^r sur Q dans le cas où p est impair

Proposition I.4.

Réciproquement, soient p un nombre premier impair, r un entier positif $(\Omega(n_i))_{1 \leq i \leq r}$ une suite de corps cyclotomiques vérifiant les conditions I.2.A et I.2.B.

— *Si* $2 \leq u_r \leq r$, soient des nombres α_0, vérifiant la condition I.3.A, et α_j, pour $2 \leq j \leq m_r$, vérifiant la condition I.3.B. Soit S_r le sous-groupe de $G(n_r)$ engendré par: $\{ c_1^{p^r}, c_1^{\alpha_0} b_0, c_1^{\alpha_j} c_j ; 2 \leq j \leq m_r \}$.

— *Si* $u_r = r + 1$, soient des nombres α_j, pour $1 \leq j \leq m_r$, vérifiant la condition I.3.B et soit S_r le sous-groupe de $G(n_r)$ engendré par: $\{ b_0^{p^r}, b_0^{\alpha_j} c_j ; 1 \leq j \leq m_r \}$.

— *Si* $u_r = 0$, soient des nombres α_j, pour $2 \leq j \leq m_r$, vérifiant la condition I.3.B et soit S_r le sous-groupe de $G(n_r)$ engendré par: $\{ c_1^{p^r}, c_1^{\alpha_j} c_j ; 2 \leq j \leq m_r \}$.

Soit enfin, K_r le sous-corps de $\Omega(n_r)$, corps fixe de S_r. Alors:

K_r est une extension cyclique sur Q, de degré p^r. La suite de corps cyclotomiques associée à K_r est la suite $(\Omega(n_i))_{1 \leq i \leq r}$.

Supposons $2 \leq u_r \leq r$, utilisons à nouveau l'application μ de Z^{m_r+1} sur $G(n_r)$ définie dans la démonstration précédente. Soit H_r le sous-module de Z^{m_r+1} ayant pour base: $(f_0, f_1, \dots f_{m_r})$ avec $f_1 = p^r e_1$, et $f_j = \alpha_j e_1 + e_j$ pour tout j différent de 1. On a $\mu(H_r) = S_r$ et d'autre part les conditions I.3.A et I.3.B impliquent que:

— $p^{r-l+1} e_0 \in H_r$ et $p^{r-l} e_0 \notin H_r$.

— 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

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

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 $\{p^ie_1, f_0, f_2, \ldots f_{m_r}\}$, 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 α_0, α_0', α_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 $0 \leq j \leq m_r$, tels que S_r soit engendré par: $\{ a_0'^{\alpha_0} a_0, a_0'^{\alpha_j} c_j ; 1 \leq j \leq m_r \}$.

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

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

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

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

On démontre tout d'abord le lemme suivant:

LEMME I.2 *bis*

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

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

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

En effet si $u_r \geq 3$, 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 $(\Omega(n_i))_{1 \leq i \leq r}$ une suite de corps cyclotomiques vérifiant les conditions I.2.A *bis* et I.2.B *bis*.

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

le sous-groupe de $G(n_r)$ engendré par:

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

— *Si* $u_r = r + 2$, soient des nombres $\alpha_0 \equiv 0\,(2^{r-1})$ et α_j, pour $1 \leq j \leq m_r$ vérifiant I.3.B *bis*. Soit S_r le sous-groupe de $G(n_r)$ engendré par: $\{ a_0'^{\alpha_0} a_0, a_0'^{\alpha_j} c_j ; 1 \leq j \leq m_r \}$.

— *Si* $u_r = 2$, soient des nombres α_j, pour $2 \leq j \leq m_r$, vérifiant I.3.B *bis*. Soit S_r le sous-groupe de $G(n_r)$ engendré par:

$$\{ c_1^{2^{r-1}} a_0, c_1^{\alpha_j} c_j ; 2 \leq j \leq m_r \}.$$

— *Si* $u_r = 0$, soient des nombres α_j, pour $2 \leq j \leq m_r$, vérifiant I.3.B *bis*. Soit S_r le sous-groupe de $G(n_r)$ engendré par:

$$\{ c_1^{2^r}, c_1^{\alpha_j} c_j ; 2 \leq j \leq m_r \}.$$

Soit enfin, K_r le sous-corps de $\Omega(n_r)$, corps fixe de S_r. Alors: K_r est une extension cyclique sur Q, de degré 2^r. La suite de corps cyclotomiques associée à K_r est la suite $(\Omega(n_i))_{1 \leq i \leq r}$.

I.8. Nombre d'extensions associées a une même suite de corps cyclotomiques

Proposition I.5.

Soit p un nombre premier impair et $(\Omega(n_i))_{1 \leq i \leq r}$ une suite de corps cyclotomiques vérifiant les conditions I.2.A et I.2.B. Le nombre d'extensions K_r de degré p^r sur Q, cycliques sur Q, admettant la suite $(\Omega(n_i))_{1 \leq i \leq r}$ comme suite de corps cyclotomiques associée est:

— *Dans le cas où* $2 \leq u_r \leq r$:

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

— *Dans le cas où* $u_r = r + 1$, et en posant $m_0 = 0$:

$$\prod_{1 \leq i \leq r} \varphi(p^{r-i+1})^{m_i - m_{i-1}}$$

— *Dans le cas où* $u_r = 0$:

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

Si par exemple, $2 \leq u_r \leq r$, on peut remplacer dans le système de générateurs de S_r donné en I.3, $c_1^{\alpha_0} b_0$ par $c_1^{\alpha_0 + k_0 p^r} b_0$, $c_1^{\alpha_2} c_2$ par $c_1^{\alpha_2 + k_2 p^r} c_2$, ... et choisir ainsi des α_i, compris entre 0 et p^r. Vérifiant cette condition supplémentaire, les valeurs de α_i sont alors déterminées de façon unique par le

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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $(\Omega(n_i))_{1 \leq i \leq r}$ est:

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

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

— *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 $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $(\Omega(n_i))_{1 \leq i \leq r}$ vérifie la condition:

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

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 $2 \leq u_r \leq r$ et posons $n'_i = n_i$ pour $1 \leq i \leq r$ et $n'_i = p^{i-r} n_r$ pour $r < i \leq r'$. La suite $(\Omega(n'_i))_{1 \leq i \leq r'}$ 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 $b'_0, c'_1, c'_2, \dots c'_{m_r}$ des générateurs des sous-groupes

$$T\left(n'_{r'}, \frac{n'_{r'}}{p^{u'_{r'}}}\right), T\left(n'_{r'}, \frac{n'_{r'}}{p_1}\right), \dots T\left(n'_{r'}, \frac{n'_{r'}}{p_{m_r}}\right)$$

et soit

$$b_0 = \pi(b'_0), c_1 = \pi(c'_1), \dots c_{m_r} = \pi(c'_{m_r}).$$

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

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

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

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

Soit $S'_{r'}$ le sous-groupe de $G(n'_{r'})$ engendré par: $\{c_1'^{p^{r'}}, c_1'^{\alpha_0} b'_0, c_1'^{\alpha_j} c'_j; 2 \leq j \leq m_r\}$ 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, $(\Omega(n_i))_{1 \leq i \leq r}$ 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 $j \leq m_i$, $p_j \equiv 1\ (2^{r'-i+1})$.
>
> *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 $j \leq m_i$, 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 $u_r \geq 2$, -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 $u_r \geq 3$, 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: $\mathfrak{p}A' = (\prod_{1 \leq v \leq g} \mathfrak{p}_v)^e$