

**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  
**DOI:** <https://doi.org/10.5169/seals-45361>

### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 22.01.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# ÉTUDE ARITHMÉTIQUE DES CORPS CYCLIQUES DE DEGRÉ $p^r$ SUR LE CORPS DES NOMBRES RATIONNELS

par Bernard ORIAT

## TABLE DES MATIÈRES

### CHAPITRE PREMIER. — *Suite de corps cyclotomiques associée à une extension cyclique de degré $p^r$ sur $Q$ .*

I.1.	Rappels et notations . . . . .	59
I.2.	Plus petit corps cyclotomique contenant une extension abélienne de degré $p^r$ sur $Q$ . . . . .	62
I.3.	Suite de corps cyclotomiques associée à une extension cyclique $K_r$ . . . . .	64
I.4.	Système de générateurs de $S_r$ . Cas où $p$ est impair . . .	68
I.5.	Construction d'extensions cycliques $K_r$ de degré $p^r$ sur $Q$ dans le cas où $p$ est impair . . . . .	71
I.6.	Système de générateurs de $S_r$ . Cas où $p = 2$ . . . . .	72
I.7.	Construction d'extensions cycliques de degré $2^r$ sur $Q$ .	74
I.8.	Nombre d'extensions associées à une même suite de corps cyclotomiques . . . . .	75
I.9.	Conditions d'inclusion de $K_r$ dans $K_{r'}$ . . . . .	76

### CHAPITRE II. — *Décomposition, Ramification, Discriminant.*

II.1.	Rappels . . . . .	78
II.2.	Nombres premiers ramifiés dans une extension abélienne sur $Q$ . . . . .	80
II.3.	Décomposition d'un nombre $q$ premier, non ramifié dans $K_r$ .	81
II.4.	Indice de ramification dans une extension $K_r$ . . . . .	83
II.5.	Discriminant de $K_r$ . . . . .	83

### CHAPITRE III. — *Bases d'entiers.*

III.1.	Rappels . . . . .	88
III.2.	Bases d'entiers dans les corps cyclotomiques . . . . .	88
III.3.	Conditions pour qu'une extension abélienne de $Q$ possède une base d'entiers normale . . . . .	90
III.4.	Bases d'entiers dans les extensions $K_r$ . . . . .	94
III.5.	Exemple . . . . .	98



## INTRODUCTION

Ce travail a pour objet l'étude arithmétique des extensions cycliques de degré une puissance d'un nombre premier sur le corps des rationnels, considérées comme sous-corps d'un corps cyclotomique. Le théorème de Kronecker (dont on pourra trouver une démonstration dans *Algebraic Number Theory*, J. W. S. Cassels et A. Fröhlich; chapitre VII, J. T. Tate; Academic Press) montre en effet que toute extension abélienne du corps des nombres rationnels est incluse dans un corps cyclotomique.

L'étude des extensions abéliennes du corps des nombres rationnels a déjà été traitée par plusieurs auteurs, en particulier H. W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*; *Jour. reine angew. Math.* 209, pp. 54-71 (1962).

Le présent travail n'a pas pour but de démontrer des résultats essentiellement originaux, mais de donner un exposé aussi élémentaire que possible des propriétés les plus importantes.

J'ai supposé connu et j'ai utilisé sans les citer explicitement des résultats concernant les propriétés élémentaires des groupes abéliens finis et la théorie de Galois dans les extensions abéliennes finies. Dans le premier chapitre, j'ai rappelé et employé la décomposition de  $\left(\frac{\mathbb{Z}}{n}\right)^*$  en produit direct de groupes cycliques (théorème chinois). Les propriétés des corps cyclotomiques utilisées ont été mentionnées au début de chaque chapitre.

Dans le premier chapitre, j'ai associé à toute extension  $K_r$  cyclique de degré  $p^r$  sur  $\mathbb{Q}$ , la suite des plus petits corps cyclotomiques contenant respectivement chaque sous-corps de  $K_r$ . J'ai établi les conditions que doit vérifier une telle suite et réciproquement, j'ai obtenu toutes les extensions  $K_r$  dont cette suite est la suite associée.

Dans le deuxième chapitre, j'ai montré que la donnée d'une suite de corps cyclotomiques associée à une extension  $K_r$  est équivalente à la donnée du discriminant de  $K_r$  sur  $\mathbb{Q}$  et j'ai calculé la valeur de ce discriminant.

Dans le troisième chapitre, j'ai énoncé des conditions équivalentes d'existence de bases d'entiers normales dans les extensions abéliennes sur

$Q$ . 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  $\xi$  une racine primitive  $n^{\text{ème}}$  de 1,  $Q(\xi)$  est le  $n^{\text{ème}}$  corps cyclotomique et sera noté  $\Omega(n)$ . Le degré,  $[\Omega(n):Q]$ , de  $\Omega(n)$  sur  $Q$  est  $\varphi(n)$ ,  $\varphi$  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  $\sigma$  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  $n^{\text{eme}}$ :  $\xi$ . 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  $d^{\text{eme}}$  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:  $T(n, d) \cap T(n, d') = T(n, \text{PPCM}(d, d'))$

et  $T(n, d) \cdot T(n, d') = T(n, \text{PGCD}(d, d'))$ .

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

On déduit de cela que:

$$\Omega(n) \cap \Omega(n') = \Omega(\text{PGCD}(n, n'))$$

et

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

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  $T(nn', n) \cdot T(nn', n')$

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

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

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

En effet :

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

et

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

Précisons que si  $h$  est un élément de  $\left(\frac{\mathbb{Z}}{n}\right)^*$  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

$$h_i \in T\left(n, \frac{n}{p_i^{r_i}}\right) \text{ on a alors } h \equiv h_i (p_i^{r_i}).$$

L'application  $\theta_i$  de  $T\left(n, \frac{n}{p_i^{r_i}}\right)$  sur  $\left(\frac{\mathbb{Z}}{p_i^{r_i}}\right)^*$  qui à tout élément  $h$  de  $T\left(n, \frac{n}{p_i^{r_i}}\right)$  fait correspondre la classe  $h'$  de  $\left(\frac{\mathbb{Z}}{p_i^{r_i}}\right)^*$  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  $\left(\frac{\mathbb{Z}}{p^r}\right)^*$  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  $r \geq 3$ ,  $\left(\frac{\mathbb{Z}}{2^r}\right)^*$  est produit direct de  $\{-1, 1\}$  et de  $T(2^r, 4)$ . Si  $p_i = 2$ ,  $r_i \geq 3$ , 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 $\mathcal{Q}$

### PROPOSITION I.1.

Soit  $r$  un entier positif,  $p$  un nombre premier impair,  $K$  une extension abélienne de degré  $p^r$  sur  $\mathcal{Q}$ ,  $\Omega(n)$  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:

—  $0 \leq s \leq r + 1$ .

—  $s \neq 1$ .

— 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  $n^{\text{eme}}$  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  $\sigma$  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  $K \subseteq \Omega\left(\frac{n'}{p_i^{u_i - 1}}\right)$ . 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  $h^{p_i^{u_i - 1}} = 1_{\Omega(n')}$ . D'où,  $\sigma$  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  $s \leq r + 1$ , c'est-à-dire, montrons que si  $u \geq r + 2$  alors  $K \subseteq \Omega\left(\frac{n'}{p^{u - r - 1}}\right)$ .

En effet si  $u \geq r + 2$ ,  $T\left(n', \frac{n'}{p^{u - r - 1}}\right) = T\left(n', \frac{n'}{p^u}\right)^{((p - 1)p^r)}$ . Tout élément  $h \in T\left(n', \frac{n'}{p^{u - r - 1}}\right)$  est donc une puissance  $(p^r)^{\text{ème}}$ . 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  $j \leq m_i$  alors  $p_j \equiv 1 \pmod{p^{r-i+1}}$ .

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  $\sigma$  un automorphisme de  $K$ . Alors pour tout  $i$  entre 1 et  $r$ ,  $\sigma^{p^i}$  est un  $K_r$ -automorphisme si et seulement si  $\sigma$  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  $\sigma$  à  $K_r$ ,  $\sigma|_{K_r}$ , est un élément d'ordre inférieur ou égal à  $p^i$  dans  $G(K_r/Q)$ . Puisque ce groupe est cyclique d'ordre  $p^r$ ,  $\sigma|_{K_r}$  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  $\tau$  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

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

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

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

$$K_{i+1} \not\subseteq \Omega(p^{u_i} p_1 p_2 \dots p_{m_r})$$

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  $u_i \geq 2$ ,  $h^p \in T(n_r, p^{u_i} p_1 p_2 \dots p_{m_r})$  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

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

*Condition I.2.B.* Si  $j \leq m_i$ , alors  $K_i \not\subseteq \Omega\left(\frac{n_r}{p_j}\right)$  c'est-à-dire

$S_i \not\subseteq T\left(n_r, \frac{n_r}{p_j}\right)$  D'après le lemme I.1, ceci implique que

$S_r \not\subseteq T\left(n_r, \frac{n_r}{p_j}\right)^{(p^{r-i})}$  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

$$\frac{p_j - 1}{\text{PGCD}(p_j - 1, p^v)}.$$

On a donc:

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

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  $\mathcal{Q}$ . 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  $n_i = 2^{u_i} p_1 p_2 \dots p_{m_i}$ ; 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  $u_l \leq 3$ . Si  $l = 1$  c'est une conséquence immédiate de la proposition I.1 bis. Si  $l \geq 2$ , 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  $T\left(n_r, \frac{n_r}{p_j}\right)$ .

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  $\alpha_j$ , pour  $j = 0$  et  $2 \leq j \leq m_r$ , tels que  $S_r$  soit engendré par:

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

$\alpha_0$  vérifie la condition:

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

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

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

— Dans le cas ou  $u_r = r + 1$ , il existe des nombres  $\alpha_j$ , 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  $\alpha_j$ , pour  $1 \leq j \leq m_r$ , vérifient la condition I.3.B.

— Dans le cas ou  $u_r = 0$ , il existe des nombres  $\alpha_j$ , 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  $\alpha_j$ , 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

$$K_{l-1} \subseteq \Omega\left(\frac{n_r}{p^{u_r}}\right) \quad \text{et} \quad K_l \not\subseteq \Omega\left(\frac{n_r}{p^{u_r}}\right),$$

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  $K_i \not\subseteq \Omega\left(\frac{n_r}{p_j}\right)$ .

D'où  $T\left(n_r, \frac{n_r}{p_j}\right) \subseteq S_{i-1}$  et  $T\left(n_r, \frac{n_r}{p_j}\right) \not\subseteq S_i$ . 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  $\mu$  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 :

$$\begin{aligned} f_1 &= a_{11} e_1 \\ f_j &= \sum_{0 \leq k \leq j} a_{kj} e_k \end{aligned}$$

On a

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

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  $\alpha_0$ , vérifiant la condition I.3.A, et  $\alpha_j$ , 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  $\alpha_j$ , 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  $\alpha_j$ , 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  $\mu$  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  $m_{i-1} < j \leq m_i$  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  $1 \leq j \leq m_r$ . Le noyau de  $\mu$  qui a pour base:  $\{(p-1)p^{r-l+1}e_0, (p_1-1)e_1, \dots, (p_{m_r}-1)e_{m_r}\}$  est donc contenu dans  $H_r$ .

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

Le degré de  $K_r$  sur  $Q$  est donc égal à

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

Comme  $p^{r-1}e_1 \notin H_r$ ,  $\frac{Z^{m_r+1}}{H_r}$  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  $\{p^i e_1, f_0, f_2, \dots, f_{m_r}\}$ ,  $i$  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  $b_0^{(p-1)p^{r-l}} \notin S_r$ ,  $T\left(n_r, \frac{n_r}{p}\right) \notin S_r$  d'où  $K_r \not\subseteq \Omega\left(\frac{n_r}{p}\right)$ .

De même si  $m_{i-1} < j \leq m_i$ , 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:

$$K_{i-1} \subseteq \Omega\left(\frac{n_r}{p_j}\right) \quad \text{et} \quad K_i \not\subseteq \Omega\left(\frac{n_r}{p_j}\right)$$

$(\Omega(n_i))_{1 \leq i \leq r}$  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  $u_r \geq 2$ ,  $a_0$  désigne l'élément de  $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$  tel que  $a_0 \equiv -1 \pmod{2^{u_r}}$ .

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  $u_r \geq 3$ ,  $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$  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  $(\Omega(n_i))_{1 \leq i \leq r}$  la suite de corps cyclotomiques associée à  $K_r$ .

— Dans le cas où  $3 \leq u_r \leq r + 1$ , il existe des nombres  $\alpha_0, \alpha'_0, \alpha_j$ , pour  $2 \leq j \leq m_r$ , tels que  $S_r$  soit engendré par:

$$\{c_1^{2^r}, c_1^{\alpha_0} a_0, c_1^{\alpha'_0} a'_0, c_1^{\alpha_j} c_j; 2 \leq j \leq m_r\}.$$

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

$\alpha'_0$  vérifie la condition:

$$I.3.A \text{ bis: } \alpha'_0 \equiv 0 \pmod{2^{l-1}} \text{ et } \alpha'_0 \not\equiv 0 \pmod{2^l}.$$

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

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



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

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

Les  $\alpha_j$ , 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  $\alpha_j$ , 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  $\alpha_j$ , 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:

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

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:  $\alpha_0 \equiv 0 \pmod{2^{r-1}}$ ,  $\alpha_0'$ , vérifiant I.3.A bis,  $\alpha_j$ , 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  $\alpha_0 \equiv 0 \pmod{2^{r-1}}$  et  $\alpha_j$ , 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  $\alpha_j$ , 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  $\alpha_j$ , 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  $\alpha_i$ , compris entre 0 et  $p^r$ . Vérifiant cette condition supplémentaire, les valeurs de  $\alpha_i$  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  $\alpha_j$  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  $j \leq m_i$ ,  $p_j \equiv 1 \pmod{p^{r'-i+1}}$ .

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  $\pi$  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  $\alpha_i$  ne sont déterminés que modulo  $p^r$  et si l'on remplace  $\alpha_i$  par  $\alpha'_i$  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  $\pi$  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  $\frac{p_j-1}{2} \equiv 0 \pmod{2^{r-i+1}}$

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  $\alpha_0 \equiv 0 \pmod{2^r}$ .

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:  $\mathfrak{p}A' = \left( \prod_{1 \leq v \leq g} \mathfrak{p}_v \right)^e$

et pour tout  $v$  de 1 à  $g$ ,  $\frac{A'}{p_v}$  a pour dimension  $f$  sur  $\frac{A}{p}$ .  $f$  est le degré résiduel de  $p_v$  sur  $K$  et  $e$  l'indice de ramification de  $p_v$  sur  $K$  (ou de  $p$  dans  $K'$ ). On a les relations:

$$efg = [K':K] \quad \text{et} \quad N_{K'/K}(p_v) = p^f.$$

Les  $p_v$ ,  $1 \leq v \leq g$ , sont exactement les idéaux premiers de  $A'$  contenant  $p$ .

Soit  $G(K'/K)$  le groupe de Galois de  $K'$  sur  $K$ . L'ensemble des  $\sigma$  de  $G(K'/K)$  tel que  $\sigma(p_v) = p_v$  est un sous-groupe de  $G(K'/K)$  ne dépendant pas de  $v$  et appelé groupe de décomposition de  $p_v$  sur  $K$  (ou de  $p$  dans  $K'$ ). Son cardinal est égal à  $ef$ . S'il est égal à 1, on dit que  $p$  se décompose complètement dans  $K'$ .

L'ensemble des  $\sigma$  de  $G(K'/K)$  tel que  $\sigma(x) - x$  appartienne à  $p_v$  pour tout  $x$  de  $A'$ , est un sous-groupe de  $G(K'/K)$  ne dépendant pas de  $v$  et appelé groupe d'inertie de  $p_v$  sur  $K$  (ou de  $p$  dans  $K'$ ).

Son cardinal est égal à  $e$ .  $p$  est dit ramifié dans  $K'$  si  $e \geq 2$  ([1] chapitre 5; [2] chapitre 5).

Soit  $K''$  un corps de nombres, contenant  $K'$  et abélien sur  $K$ , et soit  $A''$  son anneau d'entiers. Si  $p_v A''$  se décompose en idéaux premiers de  $A''$  sous la forme:  $p_v A'' = (\prod_{1 \leq v' \leq g'} p_{vv'})^{e'}$  et si  $f'$  désigne le degré résiduel de  $p_{vv'}$  sur  $K'$ , les quantités  $e'$ ,  $g'$ ,  $f'$  sont les mêmes pour tout  $v$  entre 1 et  $g$ . L'indice de ramification de  $p$  dans  $K''$  est  $ee'$  et son degré résiduel  $ff'$ . Si  $D$  est le groupe de décomposition de  $p_{vv'}$  sur  $K$  et  $\pi$  l'application de  $G(K''/K)$  sur  $G(K'/K)$  qui à tout automorphisme de  $K''$  fait correspondre sa restriction à  $K'$ , alors  $D \cap G(K''/K')$  est le groupe de décomposition de  $p_{vv'}$  sur  $K'$  et  $\pi(D)$  est le groupe de décomposition de  $p_v$  sur  $K$ . On a un résultat analogue avec les groupes d'inertie ([3] chapitre 1).

On appelle corps de décomposition de  $p$  dans  $K'$  le sous-corps de  $K'$  laissé invariant par les éléments du groupe de décomposition de  $p$  dans  $K'$ . C'est le plus grand corps, compris entre  $K$  et  $K'$ , dans lequel  $p$  se décompose complètement. De même le corps d'inertie de  $p$  dans  $K'$  est le sous-corps de  $K'$  laissé invariant par les éléments du groupe d'inertie de  $p$  dans  $K'$ . C'est le plus grand corps compris entre  $K$  et  $K'$ , dans lequel  $p$  ne se ramifie pas ([4] chapitre 2).

*Différente*: L'ensemble des  $x$  de  $K'$  tels que  $Tr_{K'/K}(xA') \subseteq A$ , est un idéal fractionnaire de  $K'$  dont l'inverse est la différentielle de  $K'$  sur  $K$  notée  $\delta_{K'/K}$ . Elle est engendrée par les  $F'(x)$ , où  $x$  parcourt  $A'$  et  $F$  désigne le polynome minimal de  $x$  sur  $K$ . Si  $p_1 \dots p_m$  sont les idéaux de  $A'$  ramifiés sur  $K$ , alors:

$$\delta_{K'/K} = \prod_{1 \leq v \leq m} p_v^{h_v}.$$

Si  $e_v$  est l'indice de ramification de  $p_v$  sur  $K$  on a:  $h_v \geq e_v - 1$  et  $h_v = e_v - 1$  si et seulement si  $e_v$  est premier avec la caractéristique du corps  $\frac{A'}{p_v}$ . Le discriminant de  $K'$  sur  $K$  est  $N_{K'/K}(\delta_{K'/K})$  et on a la formule de transitivité:  $\delta_{K''/K} = \delta_{K''/K'} \delta_{K'/K}$  ([2] chapitre 4, [5] chapitre 3).

*Corps cyclotomiques*: Dans un corps cyclotomique  $\Omega(p^s)$ , ( $p$  premier)  $p$  est leur seul nombre premier ramifié et:  $p = (1 - \xi)^{\varphi(p^s)}$ ,  $\xi$  désignant une racine primitive  $(p^s)^{\text{eme}}$  de 1, est la décomposition de  $p$  en idéaux premiers de  $\Omega(p^s)$ .

$p$  est ramifié dans un corps cyclotomique  $\Omega(n)$  si et seulement si  $p$  divise  $n$ . Si  $n$  s'écrit:  $n = p^s n'$  avec  $n'$  premier avec  $p$ , alors le corps d'inertie de  $p$  dans  $\Omega(n)$  est  $\Omega(n')$  et l'indice de ramification de  $p$  dans  $\Omega(n)$  est  $\varphi(p^s)$ . Si  $q$  est premier avec  $n$ , la classe de  $q$  modulo  $n$  est l'automorphisme de Frœbenius, et elle engendre dans  $G(n)$  le groupe de décomposition de  $q$  dans  $\Omega(n)$ . Le degré résiduel de  $q$  dans  $\Omega(n)$  est donc le plus petit entier  $f$  tel que:  $q^f \equiv 1 (n)$ .

Si  $\xi$  est une racine primitive  $n^{\text{eme}}$  de 1,  $\{1, \xi, \dots, \xi^{\varphi(n)-1}\}$  est une base de l'anneau des entiers de  $\Omega(n)$  sur  $Z$ . Le discriminant de  $\Omega(n)$  sur  $Q$  est:

$$\frac{n^{\varphi(n)}}{\prod p^{\frac{\varphi(n)}{p-1}}}$$

ce dernier produit étant étendu à tous les nombres premiers  $p$  divisant  $n$  ([5] chapitre 4).

## II.2. NOMBRES PREMIERS RAMIFIÉS DANS UNE EXTENSION ABÉLIENNE DE $Q$

### LEMME II.1.

Soient  $K$  une extension abélienne de  $Q$  et  $\Omega(n)$  le plus petit corps cyclotomique contenant  $K$ . Alors un nombre premier  $p$  se ramifie dans  $K$  si et seulement s'il divise  $n$ .

Si  $p$  est ramifié dans  $K$ , alors il est ramifié dans tout surcorps de  $K$ , donc dans  $\Omega(n)$  et il divise  $n$ .

Réciproquement, si  $p$  divise  $n$ , posons  $n = p^s n'$ , avec  $n'$  premier avec  $p$ .

Alors le corps d'inertie de  $p$  dans  $\Omega(n)$  est  $\Omega(n')$  et son groupe d'inertie  $T(n, n')$ .

Soit  $\pi$  l'application canonique de  $G(n)$  sur  $G(K/Q)$  qui à tout automorphisme de  $\Omega(n)$  fait correspondre sa restriction à  $K$ .  $\pi$  a pour noyau  $G(\Omega(n)/K)$  et comme  $\Omega(n)$  est le plus petit corps cyclotomique contenant  $K$ , on a donc :

$$\Omega(n') \not\subseteq K \quad \text{c'est-à-dire} \quad T(n, n') \not\subseteq G(\Omega(n)/K).$$

$\pi(T(n, n'))$  qui est le groupe d'inertie de  $p$  dans  $K$ , n'est donc pas réduit à l'identité et  $p$  se ramifie dans  $K$ .

### II.3. DÉCOMPOSITION D'UN NOMBRE $q$ PREMIER, NON RAMIFIÉ DANS $K_r$

$K_r$  désigne une extension cyclique de degré  $p^r$  sur  $Q$  ( $p$  premier) et  $(\Omega(n_i))_{1 \leq i \leq r}$  la suite de corps cyclotomiques associée. Les notations restent les mêmes qu'au premier chapitre.  $q$  est un nombre premier non ramifié dans  $K_r$ , c'est-à-dire d'après le lemme précédent, premier avec  $n_r$ .

Si  $p$  est impair et suivant que  $u_r = 0$  ou  $u_r \geq 2$ ,

$$\text{soit} \quad q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}}(n_r)$$

$$\text{ou} \quad q \equiv b_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}}(n_r),$$

la décomposition de  $q$  dans  $G(n_r)$ .

On posera alors :

— Si

$$2 \leq u_r \leq r : V(q) = \alpha_0 \beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$$

— Si

$$u_r = r + 1 : V(q) = \sum_{1 \leq j \leq m_r} \alpha_j \beta_j - \beta_0$$

— Si

$$u_r = 0 : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$$

De même si  $p = 2$  et suivant que  $u_r = 0$ , ou  $u_r = 2$ , ou  $u_r \geq 3$ , soit

$$q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}}(n_r) \quad \text{ou} \quad q \equiv a_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}}(n_r)$$

ou

$$q \equiv a_0^{\beta_0} a_0' \beta_0' c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}}(n_r)$$



la décomposition de  $q$  dans  $G(n_r)$ . On posera alors:

- Si  $3 \leq u_r \leq r + 1 : V(q) = \alpha_0 \beta_0 + \alpha'_0 \beta'_0 + \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$
- Si  $u_r = r + 2 : V(q) = \sum_{0 \leq j \leq m_r} \alpha_j \beta_j - \beta'_0$
- Si  $u_r = 2 : V(q) = 2^{r-1} \beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$
- Si  $u_r = 0 : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$

# PROPOSITION II.1.

Soient  $K_r$  une extension cyclique de degré  $p^r$  sur  $Q$  et  $q$  un nombre premier, ne divisant pas  $n_r$ . Alors la décomposition de  $q$  en idéaux premiers de  $K_r$  est de la forme:

$$q = \prod_{1 \leq v \leq g_q} \mathfrak{q}_v$$

et  $g_q$  est le PGCD de  $p^r$  et de  $V(q)$ .

Le groupe de décomposition de  $q$  dans  $\Omega(n_r)$  est le sous-groupe de  $G(n_r)$  engendré par la classe de  $q$  modulo  $n_r$  et la restriction de  $q$ , considéré comme automorphisme de  $\Omega(n_r)$ , à  $K_r$  engendre le groupe de décomposition de  $q$  dans  $K_r$ .

Le degré résiduel  $f_q$  de  $q$  dans  $K_r$  est donc l'ordre de  $q$  dans  $\frac{G(n_r)}{S_r}$ . Supposons par exemple  $p$  impair et  $2 \leq u_r \leq r$  et considérons alors:

$$\begin{aligned} s &= (c_1^{\alpha_0} b_0)^{\beta_0} (c_1^{\alpha_2} c_2)^{\beta_2} \dots (c_1^{\alpha_{m_r}} c_{m_r})^{\beta_{m_r}} \\ &= b_0^{\beta_0} c_1^{V(q) + \beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} \end{aligned}$$

D'après la proposition I.3,  $s \in S_r$  et l'on a modulo  $n_r$ :

$$sq^{-1} = c_1^{V(q)}.$$

$f_q$  est donc égal à l'ordre de  $c_1^{V(q)} S_r$  dans  $\frac{G(n_r)}{S_r}$  et comme l'ordre de  $c_1 S_r$

est  $p^r$  (lemme I.2), on a donc:

$$f_q = \frac{p^r}{PGCD(p^r, V(q))}$$

et

$$g_q = PGCD(p^r, V(q)).$$

#### II.4. INDICE DE RAMIFICATION DANS UNE EXTENSION $K_r$ .

##### PROPOSITION II.2.

Soient  $K_r$  une extension cyclique de degré  $p^r$  sur  $Q$  et  $(\Omega(n_i))_{1 \leq i \leq r}$  la suite de corps cyclotomiques associée à  $K_r$ . Pour tout  $i$  de 1 à  $r$  et tout  $j$  tel que  $m_{i-1} < j \leq m_i$ , l'indice de ramification de  $p_j$  dans  $K_r$  est  $p^{r-i+1}$ .

Si  $u_r \neq 0$ , l'indice de ramification de  $p$  dans  $K_r$  est  $p^{r-l+1}$ .

Soit  $j$  tel que  $m_{i-1} < j \leq m_i$ .  $p_j$  divise donc  $n_i$  et ne divise pas  $n_{i-1}$ . C'est-à-dire que  $p_j$  se ramifie dans  $\Omega(n_i)$  et ne se ramifie pas dans  $\Omega(n_{i-1})$ . D'après le lemme II.1, ceci implique que  $p_j$  se ramifie dans  $K_i$  et ne se ramifie pas dans  $K_{i-1}$ .  $K_{i-1}$  est donc le corps d'inertie de  $p_j$  dans  $K_r$  et l'indice de ramification de  $p_j$  dans  $K_r$  est égal à:  $[K_r : K_{i-1}]$ .

De même si  $u_r \neq 0$ ,  $K_{l-1}$  est le corps d'inertie de  $p$  dans  $K_r$ .

#### II.5. DISCRIMINANT DE $K_r$ .

##### PROPOSITION II.3.

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

— Dans le cas où  $u_r = 0$ :

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

— Dans le cas où  $p$  est impair et  $u_r \geq 2$ :

$$p^{p^{l-1}((r-l+2)p^{r-l+1} - \frac{p^{r-l+1}-1}{p-1} - 1)} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{p^{i-1}(p^{r-i+1}-1)}$$

— Dans le cas où  $p = 2$  et  $u_r = 2$ :

$$2^{2^r} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

— Dans le cas où  $p = 2$  et  $u_r \geq 3$ :

$$2^{2^{l-1}((r-l+2)2^{r-l+1}-1)} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

Supposons tout d'abord  $u_r = 0$ . Désignons par  $A$  l'anneau des entiers de  $K_r$ . Pour tout  $j$  de 1 à  $m_r$  soit  $p_j A = \prod_{1 \leq v \leq g_j} \mathfrak{p}_{jv}^{e_j}$  la décomposition de  $p_j A$  dans  $K_r$  et soit  $f_j$  le degré résiduel de  $p_j$  dans  $K_r$ . Les  $p_j$  étant les seuls nombres premiers ramifiés dans  $K_r$  et leurs indices de ramification  $e_j$  étant premiers à  $p_j$ , la différentielle  $\delta$  de  $K_r$  sur  $Q$  est:

$$\delta = \prod_{1 \leq j \leq m_r} \prod_{1 \leq v \leq g_j} \mathfrak{p}_{jv}^{e_j-1}$$

Le déterminant  $D_f$  de  $K_r$  sur  $Q$ , est donc  $D = N_{K_r/Q}(\delta)$  et comme  $N_{K_r/Q}(\mathfrak{p}_{jv}) = p_j^{f_j}$  on obtient:

$$D = \prod_{1 \leq j \leq m_r} p_j^{f_j g_j (e_j - 1)}$$

qui s'écrit également:

$$D = \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{f_j g_j (e_j - 1)}.$$

Si  $m_{i-1} < j \leq m_i$ , alors  $e_j = p^{r-i+1}$  d'après la proposition II.2 et comme  $e_j f_j g_j = p^r$ , on obtient le résultat annoncé.

Supposons maintenant  $p$  impair et  $u_r \geq 2$ .

Dans ce cas  $u_r$  et  $l$  sont liés par la relation  $u_r = r - l + 2$ . On notera toujours  $D$  le discriminant de  $K_r$  sur  $Q$  et on introduit la décomposition  $\delta = \delta_0 \delta_1 \dots \delta_{m_r}$  de la différentielle de  $K_r$  sur  $Q$ , en idéaux:  $\delta_0, \delta_1, \dots, \delta_{m_r}$ , tels que  $D_0 = N_{K_r/Q}(\delta_0)$  soit une puissance de  $p$  et tels que  $D_j = N_{K_r/Q}(\delta_j)$  soit une puissance de  $p_j$ .  $D$  s'écrit alors  $D = D_0 D_1 \dots D_{m_r}$ . Le calcul de  $D_1 D_2 \dots D_{m_r}$  s'effectue comme dans la démonstration précédente. Pour calculer  $D_0$ , on introduit la différentielle  $\delta'$  de  $\Omega(n_r)$  sur  $K_r$  décomposée de la même façon en  $\delta' = \delta'_0 \delta'_1 \dots \delta'_{m_r}$  et  $D'' = D''_0 D''_1 \dots D''_{m_r}$  le discriminant de  $\Omega(n_r)$  sur  $Q$ .

La formule de transitivité sur les différentielles donne:

$$D''_0 = N_{\Omega(n_r)/Q}(\delta_0 \delta'_0) = N_{\Omega(n_r)/Q}(\delta'_0) N_{K_r/Q}(\delta_0^{[\Omega(n_r):K_r]})$$

d'où

$$D''_0 = N_{\Omega(n_r)/Q}(\delta'_0) D_0^{\frac{\varphi(n_r)}{p^r}}$$

Calcul de  $N_{\Omega(n_r)/Q}(\delta'_0)$ :

Soient  $A$  et  $A_\Omega$  les anneaux d'entiers respectifs de  $K_r$  et  $\Omega(n_r)$  et soit  $pA = \prod_{1 \leq v \leq g} p_v^e$  la décomposition de  $pA$  dans  $K_r$  et  $f$  le degré résiduel de  $p$  dans  $K_r$ . Soient:

$p_v A_\Omega = \prod_{1 \leq v' \leq g'} p_{vv'}^{e'}$  la décomposition de  $p_v A_\Omega$  dans  $\Omega(n_r)$  et  $f'$  le degré résiduel de  $p_v$  dans  $\Omega(n_r)$ . L'indice de ramification  $e$  de  $p$  dans  $K_r$  est  $p^{r-l+1}$  (proposition II.2) et puisque l'indice de ramification  $ee'$  de  $p$  dans  $\Omega(n_r)$  est  $\varphi(p^{u_r}) = (p-1)p^{r-l+1}$ , on a donc  $e' = p-1$  et  $e'$  est premier à  $p$ . On en déduit que:

$$\delta'_0 = \prod_{\substack{1 \leq v \leq g \\ 1 \leq v' \leq g'}} p_{vv'}^{p-2}$$

et comme  $N_{\Omega(n_r)/Q}(p_{vv'}) = p^{ff'}$ , on aura donc:

$$N_{\Omega(n_r)/Q}(\delta'_0) = p^{ff'gg'(p-2)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}}$$

D'autre part on a  $D''_0 = p^{\varphi(n_r)} \left( r-l+2 - \frac{1}{p-1} \right)$  d'où l'égalité:

$$p^{\varphi(n_r) \left( r-l+2 - \frac{1}{p-1} \right)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}} D_0^{\frac{\varphi(n_r)}{p^r}}$$

dont on extrait la valeur de  $D_0$ .

Dans le cas  $p = 2$  et  $u_r = 2$ ; gardant les mêmes notations on a  $e' = 1$  et  $\delta'_0 = 1$ . On utilise alors comme précédemment la valeur  $D''_0 = 2^{\varphi(n_r)}$ .

Supposons maintenant  $p = 2$  et  $u_r \geq 3$ :

On garde les mêmes notations que précédemment. On a cette fois:  $u_r = r - l + 3$  et l'indice de ramification  $ee'$  de 2 dans  $\Omega(n_r)$  est maintenant  $2^{r-l+2}$  d'où  $e' = 2$ .  $\delta'_0$  ne peut donc être obtenue comme précédemment. On introduit un corps  $E$  compris entre  $K_r$  et  $\Omega(n_r)$  de la façon suivante: reprenant les notations introduites dans la proposition I.3 bis posons:

$$h = a_0'^{\frac{\alpha_0}{2^{l-1}}} a_0 \quad \text{et} \quad S = \{h, 1\}.$$

$h$  est d'ordre 2,  $S$  est donc un sous-groupe de  $G(n_r)$ . Dans le cas où  $l = 1$ , c'est-à-dire  $u_r = r + 2$ , il apparaît immédiatement que  $S$  est inclus dans  $S_r$ . Si  $l \geq 2$ , c'est-à-dire si  $3 \leq u_r \leq r + 1$  on constate que:

$\left(\frac{\alpha'_0}{2^{l-1}} + 1\right) \alpha_0 \equiv 0 (2^r)$  et qu'il existe donc un entier  $\beta$  tel que:

$$\left(\frac{\alpha'_0}{2^{l-1}} + 1\right) \alpha_0 + 2^r \beta = p_1 - 1.$$

D'où

$$h = (c_1^{\alpha'_0} a'_0)^{\frac{\alpha_0}{2^{l-1}}} c_1^{\alpha_0} a_0 c_1^{2^r \beta}$$

qui montre que  $S$  est inclus dans  $S_r$ .  $E$  désigne le corps fixe de  $S$ ,  $E$  contient donc  $K_r$ .

Le groupe d'inertie de 2 dans  $\Omega(n_r)$  est  $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ , le groupe d'inertie de  $p_v$ , sur  $E$  sera donc  $T\left(n_r, \frac{n_r}{2^{u_r}}\right) \cap S = S$ .  $p_v$  n'est donc pas ramifié dans  $E$  et la différentielle de  $E$  sur  $K_r$  est première avec 2.

Si  $D'$  est le discriminant de  $E$  sur  $Q$ , et  $D'_0$  la plus grande puissance de 2 divisant  $D'$ , on aura alors:

$$D'_0 = N_{E/Q}(\delta_0) = N_{E/K_r}(D_0) = D_0^{\frac{\varphi(n_r)}{2^{r+1}}}$$

Il reste à calculer  $D'_0$ . Pour cela introduisons  $A_E$  l'anneau des entiers de  $E$  et  $\xi$  une racine primitive  $(n_r)^{\text{eme}}$  de 1. A partir de l'égalité:  $\xi^2 = -\xi^{h+1} + (\xi + \xi^h) \xi$ , on constate par récurrence sur  $t$  que  $\xi^t$  peut toujours se mettre sous la forme  $a + b\xi$ , avec  $a$  et  $b$  dans  $A_E$ . Comme  $\{1, \xi, \dots, \xi^{\varphi(n_r)-1}\}$  est une base des entiers de  $\Omega(n_r)$  sur  $Z$ , on en déduit que  $\{1, \xi\}$  est une base des entiers de  $\Omega(n_r)$  sur  $A_E$ . Le polynome  $X^2 - (\xi + \xi^h)X + \xi^{h+1}$  est le polynome minimal de  $\xi$  sur  $E$  et la différentielle  $\delta''$  de  $\Omega(n_r)$  sur  $E$  sera donc l'idéal engendré par  $\xi - \xi^h$ .

La formule de transitivité sur les différentielles appliquée entre  $Q$ ,  $E$  et  $\Omega(n_r)$  va donner:

$$D'' = D'^{[\Omega(n_r):E]} N_{\Omega(n_r)/Q}(\delta'') = D'^2 N_{\Omega(n_r)/Q}(\delta'')$$

Pour obtenir la valeur de  $N_{\Omega(n_r)/Q}(\delta'')$ , montrons que  $\xi^{h-1}$  est une racine primitive  $(2^{r-l+2})^{\text{eme}}$  de 1. En effet:

$h \in T\left(n_r, \frac{n_r}{2^{u_r}}\right)$  donc  $h - 1 \equiv 0 \left(\frac{n_r}{2^{u_r}}\right)$  et d'autre part,  $h$  étant premier à 2, on a  $h - 1 \equiv 0 (2)$ .

Mais  $h - 1 \not\equiv 0 (4)$ , sinon  $h$  appartiendrait à  $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$  et ce sous-groupe est engendré par  $a'_0$ .

On a donc finalement

$$h - 1 \equiv 0 \left( \frac{n_r}{2^{r-l+2}} \right) \quad \text{et} \quad h - 1 \not\equiv 0 \left( \frac{n_r}{2^{r-l+1}} \right)$$

On en déduit que

$$N_{\Omega(2^{r-l+2})/Q}(1 - \xi^{h-1}) = 2$$

et

$$N_{\Omega(n_r)/Q}(\delta'') = 2^{\frac{\varphi(n_r)}{2^{r-l+1}}}.$$

Comme  $D_0''$  est égal à  $2^{\varphi(n_r)(r-l+2)}$ , on en déduit les égalités:

$$2^{\varphi(n_r)(r-l+2)} = D_0'^2 \cdot 2^{\frac{\varphi(n_r)}{2^{r-l+1}}} = D_0 \frac{\varphi(n_r)}{2^r} \cdot 2^{\frac{\varphi(n_r)}{2^{r-l+1}}}$$

D'où l'on déduit la valeur de  $D_0$ .

#### PROPOSITION II.4.

Le discriminant de  $K_r$ , extension cyclique de degré  $p^r$  sur  $Q$ , ne dépend que de la suite de corps cyclotomiques associée à  $K_r$ . Réciproquement, si deux extensions cycliques de degré  $p_r$  sur  $Q$ , ont même discriminant sur  $Q$ , alors leurs suites de corps cyclotomiques sont égales.

C'est une conséquence de la proposition II.3.

Précisons pour la réciproque, que si  $K_r$  est une extension cyclique de degré  $p^r$  sur  $Q$  ( $p$  premier, par exemple) et si l'on connaît son discriminant  $D$  sur  $Q$ , alors les nombres premiers divisant  $n_r$  sont exactement ceux qui divisent  $D$ . L'exposant de  $p_j$  dans la décomposition de  $D$  en facteurs premiers n'est pas divisible par  $p^i$  si et seulement si  $j \leq m_i$  c'est-à-dire si et seulement si  $p_j$  divise  $n_i$ . Ceci permet de préciser quels sont les diviseurs de  $n_i$  distincts de  $p$ . Si  $p$  ne divise pas  $D$ , on a  $u_r = 0$  et alors tous les  $u_i$  sont nuls. Si  $p$  divise  $D$ , et comme  $(r-l+2)p^{r-l+1} - \frac{p^{r-l+1} - 1}{p - 1} - 1$  est premier à  $p$ , on obtient, à partir de la valeur de l'exposant de  $p$  dans la décomposition de  $D$ , la valeur de  $l$ , donc la suite  $(u_i)_{1 \leq i \leq r}$ .

## CHAPITRE III

### BASES D'ENTIERS

#### III.1. RAPPELS

##### *Bases d'entiers normales*

Soit  $K$  une extension abélienne de  $Q$ . On dit qu'un élément  $\theta$  de  $K$  engendre une base normale des entiers de  $K$  si l'anneau des entiers de  $K$  admet pour base, sur  $Z$ , l'ensemble des conjugués de  $\theta$ .

Si  $K$  possède une base d'entiers normale, engendrée par  $\theta$ , alors :

— Tout sous-corps  $L$  de  $K$  possède également une base d'entiers normale engendrée par  $Tr_{K/L}(\theta)$ .

En effet, tout entier  $x$  de  $L$ , s'écrit :

$$x = \sum_{\sigma \in G(K/Q)} \lambda_{\sigma} \sigma(\theta), \lambda_{\sigma} \text{ appartenant à } Z.$$

Puisque  $x$  est invariant par tout  $L$ -automorphisme de  $K$ , alors  $\lambda_{\sigma} = \lambda_{\sigma'}$ , pour tous  $\sigma$  et  $\sigma'$  situés dans la même classe modulo  $G(K/L)$ .

— La trace de  $\theta$  sur  $Q$  est égale à  $\pm 1$ .

En effet  $Z$  n'a pas d'autre base d'entiers que  $\{1\}$  ou  $\{-1\}$ .

##### *Corps cyclotomiques*

$\xi$  étant une racine primitive  $n^{\text{eme}}$  de 1, on notera  $\Phi_n(X)$  le  $n^{\text{eme}}$  polynome cyclotomique, c'est-à-dire le polynome minimal de  $\xi$  sur  $Q$ . On rappelle qu'on a la relation :  $X^n - 1 = \prod_{k|n} \Phi_k(X)$ .

Si  $n = p_1^{u_1} \dots p_m^{u_m}$  est la décomposition de  $n$  en facteurs premiers, on a :

$$\Phi_n(X) = \Phi_{p_1 \dots p_m} \left( X^{p_1^{u_1-1} \dots p_m^{u_m-1}} \right)$$

([6] chapitre 8).

#### III.2. BASES D'ENTIERS DANS LES CORPS CYCLOTOMIQUES

##### LEMME III.1.

Soit  $d$  un entier sans facteur carré et  $\xi$  une racine primitive  $d^{\text{eme}}$  de 1. On a alors  $Tr_{\Omega(d)/Q}(\xi) = (-1)^m$ ,  $m$  étant le nombre de facteurs premiers de  $d$ .

On peut raisonner par récurrence sur  $m$ , en utilisant:  $\Phi_d = \frac{X^d - 1}{\prod_{\substack{k|d \\ k \neq d}} \Phi_k}$ .

Pour tout diviseur  $k$  de  $d$  soit  $m_k$  le nombre de facteurs premiers de  $k$ . D'après l'hypothèse de récurrence, les  $\Phi_k$  sont de la forme:

$$X^{\varphi(k)} - (-1)^{m_k} X^{\varphi(k)-1} + \dots$$

et  $\prod_{\substack{k|d \\ k \neq d}} \Phi_k$  sera de la forme:

$$X^{\varphi(d)-d} - s X^{\varphi(d)-d-1} + \dots \quad \text{avec} \quad s = \sum_{\substack{k|d \\ k \neq d}} (-1)^{m_k}.$$

Comme le nombre de diviseurs  $k$  de  $d$ , possédant  $m_k$  facteurs premiers est  $C_m^{m_k}$ , on aura donc:

$$s = \sum_{0 \leq j \leq m-1} (-1)^j C_m^j = -(-1)^m.$$

$\Phi_d$  sera donc de la forme:

$$X^{\varphi(d)} - (-1)^m X^{\varphi(d)-1} + \dots$$

### LEMME III.2.

Soient  $n$  et  $d$  deux entiers tels que  $d$  soit sans facteur carré et premier avec  $n$ . Soit  $\xi$  une racine primitive  $(nd)^{\text{ème}}$  de 1. Soient  $F$  l'ensemble des racines primitives  $(nd)^{\text{ème}}$  de 1 et  $F''$  l'ensemble des  $\xi^b$  tels que:  $0 \leq b < \varphi(nd)$  et  $\text{PGCD}(b, n) \neq 1$ .

Alors le module engendré sur  $Z$  par  $F \cup F''$  est l'anneau des entiers de  $\Omega(nd)$ .

Comme  $\{1, \xi, \xi^2, \dots, \xi^{\varphi(nd)-1}\}$  est une base de l'anneau des entiers de  $\Omega(nd)$ , il suffit de montrer que si  $c$  est premier avec  $n$  et non premier avec  $d$ , alors  $\xi^c$  appartient au module engendré par  $F$ .

Soit  $v = \text{PGCD}(c, d)$ .  $\xi^{\frac{nd}{v}}$  est une racine primitive  $v^{\text{ème}}$  de 1 et  $v$  est sans facteur carré. D'après le lemme III.1, on a la relation:

$$\pm 1 = \sum_{\substack{0 < k < v \\ \text{PGCD}(k, v) = 1}} \xi^{\frac{ndk}{v}} \quad \text{d'où: } \xi^c = \pm \sum_{\substack{0 < k < v \\ \text{PGCD}(k, v) = 1}} \xi^{\frac{ndk}{v} + c}$$



On vérifie que  $\frac{ndk}{v} + c$  et  $nd$  sont premiers entre eux, c'est-à-dire que les  $\xi^{\frac{ndk}{v} + c}$  appartiennent à  $F$ .

LEMME III.3.

||  $\Omega(d)$  possède une base d'entiers normale si et seulement si  $d$  est sans facteur carré.

En effet si  $d$  est sans facteur carré, alors d'après le lemme III.2, appliqué à  $n = 1$ , les conjugués de  $\xi$ , racine primitive  $d^{\text{eme}}$  de 1, engendrent l'anneau des entiers de  $\Omega(d)$ . Comme ils sont en nombre égal à  $[\Omega(d):Q]$ , ils forment donc une base de l'anneau des entiers de  $\Omega(d)$ . Réciproquement soit  $p$  un nombre premier et  $\xi$  une racine primitive  $(p^2)^{\text{eme}}$  de 1. Comme  $\Phi_{p^2}(X) = \Phi_p(X^p)$ , on a  $Tr_{\Omega(p^2)/Q}(\xi) = 0$ . D'autre part:

$$Tr_{\Omega(p^2)/Q}(\xi^p) = p Tr_{\Omega(p)/Q}(\xi^p) = -p$$

et la trace de toute racine  $(p^2)^{\text{eme}}$  de 1, non primitive, est multiple de  $p$ . Ainsi la trace de tout entier de  $\Omega(p^2)$  est multiple de  $p$ , donc ne peut être égale à 1.  $\Omega(p^2)$  n'a pas de base d'entiers normale, non plus que tout sur-corps de  $\Omega(p^2)$ . En particulier  $\Omega(d)$  n'a pas de base d'entiers normale si  $d$  possède un facteur carré.

### III.3. CONDITIONS POUR QU'UNE EXTENSION ABÉLIENNE DE $Q$ POSSÈDE UNE BASE D'ENTIERES NORMALE

|| *Notation* : Si  $K$  est une extension cyclique sur  $Q$ ,  $\theta$  un élément de  $K$ ,  $\sigma$  un automorphisme de  $K$ ,  $t$  un entier positif,  $B(\theta, \sigma, t)$  désignera l'ensemble des  $t$  premiers conjugués successifs de  $\theta$  par  $\sigma$ , c'est-à-dire:

$$B(\theta, \sigma, t) = \{ \sigma^k(\theta), 0 \leq k < t \}$$

PROPOSITION III.1.

|| Soit  $K_r$  une extension cyclique de degré  $p^r$  sur  $Q$  ( $p$  premier). Soit  $\Omega(n_r)$  le plus petit corps cyclotomique contenant  $K_r$ . On suppose que  $u_r$  est différent de 0, que  $\xi$  est une racine primitive  $(n_r)^{\text{eme}}$  de 1 et  $B_{r-1}$  est une base de l'anneau des entiers de  $K_{r-1}$ . Soient  $\theta = \sum_{s \in S_r} \xi^s$  et  $\sigma$  un générateur de  $G(K_r/Q)$ .

Alors:

$B_{r-1} \cup B(\theta, \sigma, \varphi(p^r))$  est une base de l'anneau des entiers de  $K_r$ .

Soit  $g$  un automorphisme de  $\Omega(n_r)$  prolongeant  $\sigma$ . Les classes de  $G(n_r)$  modulo  $S_r$  sont  $g^k S_r$ ,  $0 \leq k < p^r$ .

Introduisons les ensembles suivants:

$F$  est l'ensemble des racines primitives  $n_r^{eme}$  de 1 c'est-à-dire:

$$F = \{ \xi^a; a \in G(n_r) \},$$

$$F' = \{ \xi^a; a \in \bigcup_{0 \leq k \leq \varphi(p^r)} g^k S_r \}$$

et

$$F'' = \{ \xi^b; 0 \leq b < \varphi(n_r) \text{ et } p \mid b \}.$$

Puisque  $p^{ur}$  est le plus grand facteur carré divisant  $n_r$ , le lemme III.2 permet d'affirmer que le module engendré sur  $Z$  par  $F \cup F''$  est l'anneau des entiers de  $\Omega(n_r)$ . Montrons que  $F' \cup F''$  est une base de cet anneau. Pour cela il suffit de constater que:

—  $\text{Card } F' \cup F'' = \varphi(n_r)$ .

— Tout élément de  $F - F'$  appartient au module engendré par  $F'$ .

La première assertion résulte d'un dénombrement immédiat des éléments de  $F' \cup F''$ . Pour démontrer la deuxième, on écrit tout d'abord que:

$$\sum_{0 \leq k \leq p-1} \xi^{\frac{n_r}{p} k} = 0$$

( $\xi^{\frac{n_r}{p}}$  est une racine primitive  $p^{eme}$  de 1).

Soit en multipliant cette égalité par  $\xi$ , on obtient:

$$(1) \quad \sum_{a \in T\left(n_r, \frac{n_r}{p}\right)} \xi^a = 0$$

Examinons comment sont répartis les éléments de  $T\left(n_r, \frac{n_r}{p}\right)$  dans les classes de  $G(n_r)$  modulo  $S_r$ .

Puisque  $K_r \not\subseteq \Omega\left(\frac{n_r}{p}\right)$  on a  $\Omega(n_r) = K_r \cdot \Omega\left(\frac{n_r}{p}\right)$  et puisque  $K_{r-1} \subseteq \Omega\left(\frac{n_r}{p}\right)$  (condition I.2.A sur la suite  $(u_i)_{1 \leq i \leq r}$ ), on a:

$$K_{r-1} = K_r \cap \Omega\left(\frac{n_r}{p}\right).$$

Les sous-groupes correspondants de  $G(n_r)$  vont donc vérifier les égalités:

$$T\left(n_r, \frac{n_r}{p}\right) \cdot S_r = S_{r-1} \quad \text{et} \quad T\left(n_r, \frac{n_r}{p}\right) \cap S_r = \{1\},$$

qui montrent que  $S_{r-1}$ , groupe des  $K_{r-1}$ -automorphismes de  $\Omega(n_r)$ , est produit direct de  $S_r$  et de  $T\left(n_r, \frac{n_r}{p}\right)$ . Dans toute classe de  $S_{r-1}$  modulo  $S_r$  il existe donc un seul élément de  $T\left(n_r, \frac{n_r}{p}\right)$ . Ces classes sont  $g^{kp^{r-1}} S_r$ ,  $0 \leq k \leq p-1$ . Si  $sg^{p^{r-1}}$  est l'unique élément de  $g^{p^{r-1}} S_r \cap T\left(n_r, \frac{n_r}{p}\right)$ , alors pour tout  $k$  entre 0 et  $p-1$ ,  $s^k g^{kp^{r-1}}$  est l'unique élément de  $g^{kp^{r-1}} S_r \cap T\left(n_r, \frac{n_r}{p}\right)$  et les éléments de  $T\left(n_r, \frac{n_r}{p}\right)$  sont donc  $s^k g^{kp^{r-1}}$ ,  $0 \leq k \leq p-1$ . L'égalité (1) va donc s'écrire:

$$(2) \quad \sum_{0 \leq k \leq p-1} \xi s^k g^{kp^{r-1}} = 0,$$

$s$  appartenant à  $S_r$ .

Tout élément de  $F - F''$  peut s'écrire sous la forme:

$$\xi s' s^{p-1} g^{t+(p-1)p^{r-1}} \quad \text{avec} \quad s' \in S_r \quad \text{et} \quad 0 \leq t < p^{r-1}.$$

Transformant alors l'égalité (2) par l'automorphisme  $s'g^t$ , on obtiendra:

$$\xi s' s^{p-1} g^{t+(p-1)p^{r-1}} = - \sum_{0 \leq k \leq p-2} \xi s' s^k g^{t+kp^{r-1}}.$$

Les racines primitives de 1, intervenant sous le signe  $\sum$  sont dans  $F'$ .  $F' \cup F''$  est donc une base des entiers de  $\Omega(n_r)$ .

Soit  $x$  un entier de  $K_r$ . On a  $x = x' + x''$  avec  $x'$  (respectivement  $x''$ ) appartenant au module engendré sur  $Z$ , par  $F'$  (respectivement  $F''$ ). Soit  $s$  un  $K_r$ -automorphisme. Comme  $F''$  est une base de l'anneau des entiers de  $\Omega\left(\frac{n_r}{p}\right)$ ,  $s(x'')$  appartient encore à  $\Omega\left(\frac{n_r}{p}\right)$ , donc au module engendré par  $F''$ . De même  $s(x')$  appartient encore au module engendré par  $F'$ , car  $s$  permute entre eux les éléments de  $F'$ . Comme enfin  $s(x) = x$ , on aura donc  $s(x') = x'$  et  $s(x'') = x''$ .

$x''$  étant invariant par tout  $K_r$ -automorphisme, appartient à  $\Omega\left(\frac{n_r}{p}\right) \cap K_r$

c'est-à-dire à  $K_{r-1}$ .

Quant à  $x'$ , il s'écrit :

$$\sum_{a \in \bigcup_{0 \leq k < \varphi(p^r)} g^k S_r} \lambda_a \xi^a, \lambda_a \in \mathbb{Z}$$

De  $x' = s(x')$  on déduit que  $\lambda_a = \lambda_{a'}$  si  $a$  et  $a'$  sont congrus modulo  $S_r$ . Posant alors  $\mu_k = \lambda_{g^k}$ , on obtient :

$$x' = \sum_{0 \leq k < \varphi(p^r)} \mu_k \left( \sum_{a \in S_r} \xi^{ag^k} \right) = \sum_{0 \leq k < \varphi(p^r)} \mu_k \sigma^k(\theta)$$

### Remarque III.1.

On n'utilise pas complètement le fait que  $\Omega(n_r)$  est le plus petit corps cyclotomique contenant  $K_r$ , mais seulement que  $n_r$  est de la forme  $p^{u_r} n'$ , avec  $n'$  premier avec  $p$ , sans facteur carré,  $K_r \subseteq \Omega(n_r)$  et  $K_r \not\subseteq \Omega\left(\frac{n_r}{p}\right)$ .

### PROPOSITION III.2.

Soit  $K$  une extension abélienne de  $Q$ . Les conditions suivantes sont équivalentes :

III.2.A:  $K$  possède une base d'entiers normale.

III.2.B: Il existe un entier  $\theta$  de  $K$  tel que  $\text{Tr}_{K/Q}(\theta) = 1$ .

III.2.C: Le plus petit corps cyclotomique contenant  $K$  possède une base d'entiers normale.

III.2.D:  $K$  est modérément ramifiée.

$C \Rightarrow A$  et  $A \Rightarrow B$  résultent des rappels effectués au paragraphe III.1.

$B \Rightarrow C$  résulte pour les extensions cycliques de degré  $p^r$  sur  $Q$  de la proposition III.1. Reprenant les mêmes notations, si  $\Omega(n_r)$  ne possède pas de base d'entiers normale, alors, d'après le lemme III.3,  $n_r$  possède un facteur carré, donc  $u_r \geq 2$ .

Comme  $\Phi_{n_r}(X) = \prod_{\substack{a=1 \\ p \nmid a}}^{n_r-1} (X^{p^{u_r} a} - 1)$ , la trace de  $\xi$  sur  $Q$  est nulle, donc celle

de  $\theta$  également. Si  $x$  est un entier de  $K_r$ ,  $x$  se décompose comme précédemment en  $x = x' + x''$  et l'on a :

$$Tr_{K_r/Q}(x) = Tr_{K_r/Q}(x'') = p Tr_{K_{r-1}/Q}(x'').$$

La trace d'un entier de  $K_r$  ne peut donc être égale à 1.

Soit maintenant  $K$  une extension abélienne de  $Q$  et  $\Omega(n)$  le plus petit corps cyclotomique contenant  $K$ . Supposons qu'il existe un entier  $\theta$  de  $K$  tel que:  $Tr_{K/Q}(\theta) = 1$ .

Le groupe de Galois de  $K$  sur  $Q$  est produit direct de  $m$  groupes cycliques d'ordre  $p_i^{r_i}$ .

Soit  $K_i$  le corps fixe de  $G_1 \times \dots \times G_{i-1} \times \{1\} \times G_{i+1} \times \dots \times G_m$ .  $K_i$  est cyclique de degré  $p_i^{r_i}$  sur  $Q$  et  $K = K_1 K_2 \dots K_m$ .

Soit  $\theta_i = Tr_{K/K_i}(\theta)$ .  $\theta_i$  est un entier de  $K_i$  tel que  $Tr_{K_i/Q}(\theta_i) = 1$ .

Si  $\Omega(n_i)$  est le plus petit corps cyclotomique contenant  $K_i$  alors  $n_i$  est sans facteur carré d'après la démonstration précédente.

$n$  est le PPCM des  $n_i$ , donc il est sans facteur carré.

Soit  $p$  un nombre premier se ramifiant dans  $K$ , c'est-à-dire divisant  $n$ . Si  $n$  est sans facteur carré, alors l'indice de ramification de  $p$  dans  $\Omega(n)$  est  $p-1$  et l'indice de ramification de  $p$  dans  $K$ , divise  $p-1$ , donc est premier à  $p$ .

Réciproquement, si  $n$  possède un facteur carré, alors  $n$  est de la forme  $n = p^s n'$ , avec  $p$  premier, ne divisant pas  $n'$  et  $s \geq 2$ . Soit  $\pi$  l'application de  $G(n)$  sur  $G(K/Q)$  qui à tout automorphisme de  $\Omega(n)$  fait correspondre sa restriction à  $K$ . Puisque  $K \not\subseteq \Omega\left(\frac{n}{p}\right)$ , alors

$$Ker \pi = G(\Omega(n)/K) \not\subseteq T\left(n, \frac{n}{p}\right).$$

Donc  $\pi\left(T\left(n, \frac{n}{p}\right)\right)$  a pour ordre  $p$  et il est inclus dans  $\pi(T(n, n'))$  qui est le groupe d'inertie de  $p$  dans  $K$ . L'indice de ramification de  $p$  dans  $K$  est donc multiple de  $p$ .

#### III.4. BASES D'ENTRIERS DANS LES EXTENSIONS $K_r$

##### PROPOSITION III.3.

|| Soit  $K_r$  une extension cyclique de degré  $p^r$  sur  $Q$ ,  $\Omega(n_r)$  le plus petit corps cyclotomique contenant  $K_r$ .

On suppose que  $u_r \geq 2$ ; c'est-à-dire que  $K_r$  ne possède pas de base d'entiers normale.  $\xi$  désignant une racine primitive  $n_r^{eme}$  de 1, on pose  $\theta_i = \sum_{s \in S_r} \xi^{sp^{r-i}}$  pour tout  $i$  de  $l$  à  $r$ .

Si  $p$  est impair ou si  $p = 2$  et  $u_r = 2$ , on pose:

$$\theta_{l-1} = \sum_{s \in S_r} \xi^{sp^{r-l+1}}$$

Si  $p = 2$  et  $u_r \geq 3$ , on pose:

$$\theta_{l-1} = \frac{1}{2} \sum_{s \in S_r} \xi^{s2^{r-l+2}}$$

$\sigma$  est un générateur du groupe de Galois de  $K_r$  sur  $Q$ .

Alors:

$$B(\theta_{l-1}, \sigma, p^{l-1}) \cup \left( \bigcup_{l \leq i \leq r} B(\theta_i, \sigma, \varphi(p^i)) \right)$$

est une base de l'anneau des entiers de  $K_r$ .

On montre tout d'abord que  $B(\theta_{l-1}, \sigma, p^{l-1})$  est une base de l'anneau des entiers de  $K_{l-1}$ .

Dans le cas où  $p$  est impair ou  $p = 2$  et  $u_r = 2$ , on a:  $u_r = r - l + 2$ ,  $K_{l-1} \subseteq \Omega\left(\frac{n_r}{p^{r-l+1}}\right) \cdot \frac{n_r}{p^{r-l+1}}$  est sans facteur carré, donc  $\xi^{p^{r-l+1}}$  engendre une base normale des entiers de  $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ .

$Tr_{\Omega\left(\frac{n_r}{p^{r-l+1}}\right)/K_{l-1}}(\xi^{p^{r-l+1}})$  engendre donc une base normale des entiers de  $K_{l-1}$ . Il reste donc à montrer que cette quantité est égale à  $\theta_{l-1}$ . Pour cela introduisons l'application  $\pi_{l-1}$  de  $G(n_r)$  dans  $G\left(\frac{n_r}{p^{r-l+1}}\right)$  qui à toute classe modulo  $n_r$  fait correspondre la classe modulo  $\frac{n_r}{p^{r-l+1}}$  qui la contient.

$S_r$  étant le groupe des  $K_r$ -automorphismes de  $\Omega(n_r)$ ,  $\pi_{l-1}(S_r)$  sera le groupe des  $K_r \cap \Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ -automorphismes de  $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ .

Comme  $K_l \not\subseteq \Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ , (condition I.2.A;  $u_l = 2$ ) on a donc

$$K_{l-1} = K_r \cap \Omega\left(\frac{n_r}{p^{r-l+1}}\right)$$

$\pi_{l-1}(S_r)$  est donc le groupe des  $K_{l-1}$ -automorphismes de  $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ .

On aura donc l'égalité:

$$Tr_{\Omega\left(\frac{n_r}{p^{r-l+1}}\right)/K_{l-1}}(\xi^{p^{r-l+1}}) = \sum_{s' \in \pi_{l-1}(S_r)} \xi^{s' p^{r-l+1}}$$

D'autre part, on déduit des égalités:

$$\left[ K_r \cdot \Omega\left(\frac{n_r}{p^{r-l+1}}\right) : \Omega\left(\frac{n_r}{p^{r-l+1}}\right) \right] = \left[ K_r : K_r \cap \Omega\left(\frac{n_r}{p^{r-l+1}}\right) \right] = p^{r-l+1}$$

et

$$\left[ \Omega(n_r) : \Omega\left(\frac{n_r}{p^{r-l+1}}\right) \right] = p^{r-l+1},$$

que

$$\Omega(n_r) = K_r \cdot \Omega\left(\frac{n_r}{p^{r-l+1}}\right).$$

Les sous-groupes de  $G(n_r)$  correspondants vont donc vérifier:

$$T\left(n_r, \frac{n_r}{p^{r-l+1}}\right) \cap S_r = 1$$

La restriction de  $\pi_{l-1}$  à  $S_r$  est donc bijective. On en déduit:

$$\sum_{s' \in \pi_{l-1}(S_r)} \xi^{s' p^{r-l+1}} = \sum_{s \in S_r} \xi^{\pi_{l-1}(s) p^{r-l+1}}.$$

Cette dernière quantité est égale à  $\theta_{l-1}$  puisque, par définition de  $\pi_{l-1}$ :

on a

$$s \equiv \pi_{l-1}(s) \left( \frac{n_r}{p^{r-l+1}} \right)$$

d'où

$$s p^{r-l+1} \equiv \pi_{l-1}(s) p^{r-l+1} (n_r)$$

Dans le cas où  $p = 2$  et  $u_r \geq 3$ , on a alors:  $u_r = r - l + 3$  et l'on utilise alors l'application  $\pi_{l-2}$  de  $G(n_r)$  sur  $G\left(\frac{n_r}{2^{r-l+2}}\right)$ . La démonstration est identique à la précédente, à ceci près que:

$$\left[ \Omega(n_r) : K_r \cdot \Omega\left(\frac{n_r}{2^{r-l+2}}\right) \right] = 2$$

c'est-à-dire que  $T\left(n_r, \frac{n_r}{2^{r-l+2}}\right) \cap S_r$  possède deux éléments. On aura cette fois:

$$\sum_{s' \in \pi_{l-2}(S_r)} \xi^{s' 2^{r-l+2}} = \frac{1}{2} \sum_{s \in S_r} \xi^{\pi_{l-2}(s) 2^{r-l+2}}$$

On montre ensuite par récurrence sur  $t$  que:

$$B_t = B(\theta_{l-1}, \sigma, p^{l-1}) \cup \left( \bigcup_{l \leq i \leq t} B(\theta_i, \sigma, \varphi(p^i)) \right)$$

est une base de  $K_t$ . Supposons donc que  $B_{t-1}$  soit une base de l'anneau des entiers de  $K_{t-1}$ . Soit  $\pi_t$  l'application canonique de  $G(n_r)$  sur  $G\left(\frac{n_r}{p^{r-t}}\right)$ .

Comme  $K_t \subseteq \Omega\left(\frac{n_r}{p^{r-t}}\right)$  et  $K_{t+1} \not\subseteq \Omega\left(\frac{n_r}{p^{r-t}}\right)$  (proposition I.2; condition I.2.A;  $u_{i+1} = u_i + 1$ ), on a

$$K_t = \Omega\left(\frac{n_r}{p^{r-t}}\right) \cap K_r$$

et  $\pi_t(S_r)$  est le groupe des  $K_t$ -automorphismes de  $\Omega\left(\frac{n_r}{p^{r-t}}\right)$ .

Si  $\theta'_t = \sum_{s' \in \pi_t(S_r)} \xi^{s' p^{r-t}}$ , la proposition III.1 et la remarque III.1, appliquées à  $\Omega\left(\frac{n_r}{p^{r-t}}\right)$  et  $K_t$  permettent de conclure que:  $B_{t-1} \cup B(\theta'_t, \sigma, \varphi(p^t))$  est une base de l'anneau des entiers de  $K_t$ . Il reste alors à montrer que  $\theta'_t = \theta_t$ . Ceci se déduit comme précédemment de l'égalité  $T\left(n_r, \frac{n_r}{p^{r-t}}\right) \cap S_r = 1$ , toujours vraie si  $l \leq t \leq r$ .

On utilisera dans le paragraphe suivant les remarques:

### Remarque III.3.A

Pour tout  $i \geq l$   $Tr_{K_i/K_{i-1}}(\theta_i) = 0$ .

En effet:

$$\begin{aligned} Tr_{K_i/K_{i-1}}(\theta_i) &= Tr_{\Omega\left(\frac{n_r}{p^{r-i}}\right)/K_{i-1}}\left(\xi^{p^{r-i}}\right) \\ &= Tr_{\Omega\left(\frac{n_r}{p^{r-i+1}}\right)/K_{i-1}}\left(Tr_{\Omega\left(\frac{n_r}{p^{r-i}}\right)/\Omega\left(\frac{n_r}{p^{r-i+1}}\right)}\left(\xi^{p^{r-i}}\right)\right) \end{aligned}$$



Cette quantité est nulle car  $X^p - \xi^{p^{r-i+1}}$  est le polynome minimal de  $\xi^{p^{r-i}}$  sur  $\Omega\left(\frac{n_r}{p^{r-i+1}}\right)$ .

### Remarque III.3.B

$$\text{Tr}_{K_{l-1}/\mathbb{Q}}(\theta_{l-1}) = (-1)^{m_{r+1}}$$

Il suffit d'appliquer le lemme III.1 à  $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$  ou  $\Omega\left(\frac{n_r}{2^{r-l+2}}\right)$ , suivant les cas.

### Remarque III.3.C

Dans le cas où  $p = 2$  et  $u_r \geq 3$ , on a :

$$\sum_{s \in S_r} \xi^{s2^{r-l+1}} = 0$$

En effet :

$$\sum_{s \in S_r} \xi^{s2^{r-l+1}} = \text{Tr}_{\Omega\left(\frac{n_r}{2^{r-l+1}}\right)/K_{l-1}}\left(\xi^{2^{r-l+1}}\right)$$

et d'autre part

$$K_{l-1} \subseteq \Omega\left(\frac{n_r}{2^{r-l+3}}\right)$$

et

$$\text{Tr}_{\Omega\left(\frac{n_r}{2^{r-l+1}}\right)/\Omega\left(\frac{n_r}{2^{r-l+3}}\right)}\left(\xi^{2^{r-l+1}}\right) = 0$$

car  $X^2 - \xi^{2^{r-l+2}}$  est le polynome minimal de  $\xi^{2^{r-l+1}}$  sur  $\Omega\left(\frac{n_r}{2^{r-l+3}}\right)$ .

## III.5. EXEMPLE

Soit  $B$  la base introduite à la proposition III.3. On se propose de chercher les polynomes caractéristiques des  $\theta_i$ . Pour cela, il faut pouvoir calculer les coordonnées, par rapport à  $B$ , des produits mutuels d'éléments de  $B$ .

Les  $\theta_i$  sont des périodes de Gauss ([7] chapitre 7). On pose pour tout entier  $a$  :  $\eta(a) = \sum_{s \in S_r} \xi^{as}$ .

On a en particulier:

$$\theta_i = \eta(p^{r-i}) \quad \text{pour } l \leq i \leq r$$

et suivant les cas:

$$\theta_{l-1} = \eta(p^{r-l+1}) \quad \text{ou} \quad \frac{1}{2}\eta(2^{r-l+2}).$$

Pour tout  $b$  appartenant à  $G(n_r)$ , le transformé de  $\eta(a)$  par  $b$  est  $\eta(ab)$ . En particulier les conjugués de  $\theta_i$ , pour  $l \leq i \leq r$ , seront:

$$\sigma^k(\theta_i) = \eta(g^k p^{r-i}).$$

Le produit de deux périodes  $\eta(a)$  et  $\eta(a')$  est donné par:  $\eta(a)\eta(a') = \sum_{s \in S_r} \eta(a+a's)$ . Appliquant cette formule à deux éléments de  $B$ , on est alors ramené au problème suivant: donner les coordonnées de  $\eta(a)$ ,  $a$  entier quelconque, dans la base  $B$ .

$c$  et  $c'$  désignent dans ce qui suit, des nombres premiers avec  $p$ .

1. Dans le cas  $p$  impair ou  $p = 2$  et  $u_r = 2$ ,  $\eta(p^u c)$ , avec  $u \geq r - l + 2$ , peut s'exprimer comme somme de périodes de la forme  $\eta(p^{r-l+1} c')$ . Il suffit d'écrire l'égalité:

$$\sum_{0 < k < p} \xi^{\frac{n_r}{p} k} = -1;$$

multipliant alors cette égalité par  $\xi^{p^u c}$  on obtient:

$$\sum_{0 < k < p} \eta\left(\frac{n_r}{p} k + p^u c\right) = -\eta(p^u c).$$

Les quantités  $\frac{n_r}{p} k + p^u c$  sont de la forme  $p^{r-l+1} c'$ .

Dans le cas où  $p = 2$  et  $u_r \geq 3$ ,  $\eta(2^u c)$ , avec  $u \geq r - l + 3$ , est l'opposé d'une période  $\eta(2^{r-l+2} c')$ .

2.  $\eta(p^u c)$ , avec  $u \leq r - l + 1$  (ou  $u \leq r - l + 2$ , suivant les cas) peut s'exprimer comme somme de périodes de la forme  $\eta(p^u c')$ ,  $c'$  appartenant à  $G(n_r)$ , en procédant de la même façon qu'au lemme III.2. C'est-à-dire: si  $v$  désigne le PGCD de  $c$  et de  $n_r$ , et  $m_v$  le nombre de diviseurs premiers de  $v$ , on a:

$$\sum_{\substack{0 < k < v \\ \text{PGCD}(k, v) = 1}} \xi^{\frac{n_r}{v} k} = (-1)^{m_v}$$

d'où:

$$(-1)^{mv} \eta(p^u c) = \sum_{\substack{0 \leq k \leq v \\ PGCD(k, v) = 1}} \eta\left(\frac{n_r}{v} k + p^u c\right)$$

Les quantités  $\frac{n_r}{v} k + p^u c$  sont de la forme  $p^u c'$ , avec  $c'$  premier avec  $n_r$ .

*Cas particulier :*

Si  $K_r \cap \Omega\left(\frac{n_r}{v}\right) \subset K_r \cap \Omega\left(\frac{n_r}{p^u}\right)$  et  $u \leq r - l$ , alors  $\eta(p^u c) = 0$ .

En effet on a :  $PGCD\left(\frac{n_r}{p^u}, \frac{n_r}{v}\right) = \frac{n_r}{p^u v}$ .

D'où  $K_r \cap \Omega\left(\frac{n_r}{v}\right) \subset \Omega\left(\frac{n_r}{p^u v}\right)$ . En employant la même méthode que dans la démonstration de la proposition III.3,  $\eta(p^u c)$  est égal, à un coefficient près, à :

$$Tr_{\Omega\left(\frac{n_r}{p^u v}\right)/K_r \cap \Omega\left(\frac{n_r}{v}\right)}(\xi^{p^u c})$$

Comme  $K_r \cap \Omega\left(\frac{n_r}{v}\right) \supset K_r \cap \Omega\left(\frac{n_r}{p^u}\right)$  et comme  $u \leq r - l$ , on aura donc :

$$K_r \cap \Omega\left(\frac{n_r}{p^{u+1}}\right) \supseteq K_r \cap \Omega\left(\frac{n_r}{v}\right).$$

$\Omega\left(\frac{n_r}{p^{u+1} v}\right)$  sera donc compris entre  $K_r \cap \Omega\left(\frac{n_r}{v}\right)$  et  $\Omega\left(\frac{n_r}{p^u v}\right)$  et l'on a

$$Tr_{\Omega\left(\frac{n_r}{p^u v}\right)/\Omega\left(\frac{n_r}{p^{u+1} v}\right)}(\xi^{p^u c}) = 0$$

3.  $\eta(p^u c)$ , avec  $u \leq r - l + 1$  (ou  $u \leq r - l + 2$  suivant le cas) et  $c$  premier avec  $n_r$ , est un conjugué de  $\eta(p^u) = \theta_{r-u}$  (à moins qu'il ne soit nul; remarque III.3.C).

S'il n'est pas dans  $B$ , alors ses conjugués sur  $K_{r-u-1}$ , seront dans  $B$  et il suffit alors d'utiliser la remarque III.3.A.

Considérons par exemple, la suite de corps cyclotomiques vérifiant les conditions I.2.A *bis* et I.2.B *bis*:  $\Omega(17)$ ,  $\Omega(8.17)$ ,  $\Omega(16.17)$ .

On a donc  $r = 3$ ;  $l = 2$ ;  $m_1 = m_2 = m_3 = 1$ ;  $p_1 = 17$ .

Il y a quatre extensions  $K_3$ , cycliques de degré 8 sur  $Q$  associées à cette suite (proposition I.5 *bis*).

Elles ont pour discriminant sur  $Q$ :  $2^{22} 17^7$  (proposition II.3).

$T(16.17, 17)$  a pour éléments 1, 35, 69, 103, 137, 171, 205, 239.

$a_0 = 239$  et l'on peut choisir comme générateur de  $T(16.17, 4.17)$ :

$$a'_0 = 69.$$

On cherche de même les éléments de  $T(16.17, 16)$  et un générateur  $c_1$  de ce sous-groupe. On peut prendre par exemple  $c_1 = 65$ . Les puissances successives de  $c_1$  sont données par le tableau suivant:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
65	145	177	81	97	49	193	33	241	161	129	225	209	257	113

$S_3$  est engendré par  $\{c_1^8, c_1^{\alpha_0} a_0, c_1^{\alpha'_0} a'_0\}$ ,  $\alpha_0$  et  $\alpha'_0$  vérifiant les conditions  $\alpha_0 \equiv 0(4)$ ;  $\alpha'_0 \equiv 0(2)$  et  $\alpha'_0 \not\equiv 0(4)$  (proposition I.4 *bis*). Les éléments de  $S_3$  sont de la forme:

$$s = c_1^{8\beta_1 + \alpha_0\beta_0 + \alpha'_0\beta'_0} \begin{matrix} \beta_0 & \beta'_0 \\ a_0 & a'_0 \end{matrix}$$

avec  $\beta_0 = 0$  ou 1;  $\beta'_0 = 0, 1, 2$  ou 3;  $\beta_1 = 0$  ou 1.

Prenons par exemple:  $\alpha_0 = 4$  et  $\alpha'_0 = 2$ .

Le tableau suivant donne les valeurs de  $s$ , en fonction de  $\beta_0, \beta'_0, \beta_1$ . On trouve donc à la dernière ligne les éléments de  $S_3$ :

$\beta_0$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$\beta'_0$	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
$\beta_1$	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
$s$	1	213	217	253	33	229	89	189	47	219	135	195	191	155	103	179

On remarque que  $3^4 = 81$  n'appartient pas à  $S_3$ , c'est-à-dire que la classe de 3 modulo  $S_3$  est un générateur de  $\frac{G(16.17)}{S_3}$ .

On prendra donc  $g = 3$ . Les classes de  $G(16.17) \bmod. S_3$  sont données dans le tableau suivant:

$S_3$	1	213	217	253	33	229	89	189	47	219	135	195	191	155	103	179
$3S_3$	3	95	107	215	99	143	267	23	141	113	133	41	29	193	37	265
$3^2S_3$	9	13	49	101	25	157	257	69	151	67	127	123	87	35	111	251
$3^3S_3$	27	39	147	31	75	199	227	207	181	201	109	97	261	105	61	209
$3^4S_5$	81	117	169	93	225	53	137	77	271	59	55	19	239	43	183	83
$3^5S_3$	243	79	235	7	131	159	139	231	269	177	165	57	173	129	5	249
$3^6S_3$	185	237	161	21	121	205	145	149	263	259	223	171	247	115	15	203
$3^7S_3$	11	167	211	63	91	71	163	175	245	233	125	241	197	73	45	65

$B = \{ \eta(1), \eta(3), \eta(3^2), \eta(3^3), \eta(2), \eta(2.3), \frac{1}{2} \eta(8), \frac{1}{2} \eta(8.3) \}$  est une base de l'anneau des entiers de  $K_3$ . On cherche le polynome minimal de  $\eta(1)$  sur  $K_2$ . Le conjugué de  $\eta(1)$  sur  $K_2$  est  $\eta(3^4)$  et d'après la remarque III.3.A,  $\eta(1) + \eta(3^4) = 0$ .

D'autre part:  $\eta(1)^2 = \sum_{s \in S_3} \eta(1+s)$ .

Il reste à exprimer chacun des  $\eta(1+s)$  en fonction de:  $\eta(2), \eta(2.3), \eta(8)$ , et  $\eta(8.3)$ .

Par exemple: pour  $s = 213$ :  $\eta(1+213) = \eta(2.107) = \eta(2.3)$  car  $107 \in 3S_3$ .

Pour  $s = 33$ :  $\eta(1+33) = \eta(2.17) = 0$  car  $\Omega(16) \cap K_3 = Q \subset K_2 = \Omega(8.17) \cap K_3$ .

Pour  $s = 47$ , on écrit  $\xi^{8.17} = -1$  d'où  $\xi^{8.17+48} = -\xi^{48}$  c'est-à-dire:  $\eta(1+47) = -\eta(8.23) = -\eta(8.3)$ .

Pour  $s = 195$ :  $\eta(1+195) = \eta(4.49) = 0$  compte tenu de la remarque III.3.C.

Finalement on obtient:  $\eta(1)^2 = -16 - \eta(2) - 2\eta(8.3) + \eta(8)$ . Le polynome minimal de  $\eta(1)$  sur  $K_2$  est donc:

$$X^2 + 16 + \eta(2) + 2\eta(8.3) - \eta(8)$$

On calcule de la même façon le polynome minimal de  $\eta(2)$  sur  $K_1$ :  $X^2 - \eta(8) - 16$  et celui de  $\eta(8)$  sur  $Q$ :  $X^2 - 2X - 16$ .

Les 8 nombres:

$$\begin{aligned} & \frac{1 + \sqrt{17}}{2}, \frac{1 - \sqrt{17}}{2}, \sqrt{17 + \sqrt{17}}, \sqrt{17 - \sqrt{17}}, \\ & \sqrt{-17 + 3\sqrt{17} - \sqrt{17 + \sqrt{17}}}, \sqrt{-17 - 3\sqrt{17} - \sqrt{17 - \sqrt{17}}}, \\ & \sqrt{-17 + 3\sqrt{17} + \sqrt{17 + \sqrt{17}}} \text{ et } \sqrt{-17 - 3\sqrt{17} + \sqrt{17 - \sqrt{17}}} \end{aligned}$$

forment une base de l'anneau des entiers de  $K_3$ .

Pour les autres valeurs de  $\alpha_0$  et  $\alpha'_0$  le résultat est le suivant: les polynomes minimaux de  $\eta(8)$  et  $\eta(2)$  restent les mêmes que précédemment. Pour obtenir une base des entiers des autres extensions  $K_3$  admettant la même suite de corps cyclotomiques associée:  $\Omega(17)$ ,  $\Omega(8.17)$ ,  $\Omega(16.17)$ , il suffit d'ajouter aux quatre nombres:

$$\frac{1 + \sqrt{17}}{2}, \frac{1 - \sqrt{17}}{2}, \sqrt{17 + \sqrt{17}}, \sqrt{17 - \sqrt{17}},$$

les quatre autres quantités:

*Pour le corps  $K_3$  correspondant à  $\alpha_0 = 4$  et  $\alpha'_0 = 6$ :*

$$\begin{aligned} & \sqrt{-17 + 3\sqrt{17} + 3\sqrt{17 + \sqrt{17}} - 4\sqrt{17 - \sqrt{17}}}, \\ & \sqrt{-17 - 3\sqrt{17} + 3\sqrt{17 - \sqrt{17}} + 4\sqrt{17 + \sqrt{17}}}, \\ & \sqrt{-17 + 3\sqrt{17} - 3\sqrt{17 + \sqrt{17}} + 4\sqrt{17 - \sqrt{17}}}, \\ & \sqrt{-17 - 3\sqrt{17} - 3\sqrt{17 - \sqrt{17}} - 4\sqrt{17 + \sqrt{17}}}, \end{aligned}$$

*Pour le corps  $K_3$  correspondant à  $\alpha_0 = 8$  et  $\alpha'_0 = 2$ :*

$$\begin{aligned} & \sqrt{17 + 3\sqrt{17} + \sqrt{17 - \sqrt{17}}}, \sqrt{17 - 3\sqrt{17} - \sqrt{17 + \sqrt{17}}}, \\ & \sqrt{17 + 3\sqrt{17} - \sqrt{17 - \sqrt{17}}}, \sqrt{17 - 3\sqrt{17} + \sqrt{17 + \sqrt{17}}} \end{aligned}$$

Pour le corps  $K_3$  correspondant à  $\alpha_0 = 8$  et  $\alpha'_0 = 6$ :

$$\sqrt{17 - 3\sqrt{17} + 3\sqrt{17 + \sqrt{17}} - 4\sqrt{17 - \sqrt{17}}},$$

$$\sqrt{17 + 3\sqrt{17} + 3\sqrt{17 - \sqrt{17}} + 4\sqrt{17 + \sqrt{17}}},$$

$$\sqrt{17 - 3\sqrt{17} - 3\sqrt{17 + \sqrt{17}} + 4\sqrt{17 - \sqrt{17}}},$$

$$\sqrt{17 + 3\sqrt{17} - 3\sqrt{17 - \sqrt{17}} - 4\sqrt{17 + \sqrt{17}}}.$$

## BIBLIOGRAPHIE

- [1] SAMUEL, P. Théorie algébrique des nombres (Hermann).
- [2] Mac CARTHY, P. J. Algebraic extensions of fields (Blaisdell Publishing Company).
- [3] HERBRAND, J. Développement moderne de la théorie des corps algébriques. *Mémorial des Sciences Mathématiques* (fasc. LXXV, 1936).
- [4] CHEVALLEY, C. Théorie du corps de classes dans les corps finis et les corps locaux. *Journ. of the Faculty of Sciences*, Tokyo 1933, 365.
- [5] LANG, S. Algebraic Numbers (Addison-Wesley Publishing Company).
- [6] ——— Algebra (Addison-Wesley Publishing Company).
- [7] VAN DER WAERDEN, B. L. Modern Algebra, vol. I (F. Ungar Publishing Company).

(Reçu le 26 octobre 1971)

Bernard Oriat  
 Faculté des sciences  
 Route de Gray  
 F-25 — Besançon