

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 18 (1972)  
**Heft:** 1: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** ÉTUDE ARITHMÉTIQUE DES CORPS CYCLIQUES DE DEGRE  $p'$   
SUR LE CORPS DES NOMBRES RATIONNELS  
**Autor:** Oriat, Bernard  
**Kapitel:** Chapitre III BASES D'ENTIERS  
**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:** 17.10.2025

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

## CHAPITRE III

### BASES D'ENTRIERS

#### 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'ENTRIERS 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  $(nd)^{\text{eme}}$  de 1. Soient  $F$  l'ensemble des racines primitives  $(nd)^{\text{eme}}$  de 1 et  $F''$  l'ensemble des  $\xi^b$  tels que:  $0 \leq b < \varphi(nd)$  et  $PGCD(b, n) \neq 1$ .

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

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

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  $d^{\text{ème}}$  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  $(p^2)^{\text{ème}}$  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  $(p^2)^{\text{ème}}$  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'ENTIERIS 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  $(n_r)^{\text{ème}}$  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  $n_r^{\text{eme}}$  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  $p^{\text{eme}}$  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 :

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

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  $Tr_{K/Q}(\theta) = 1$ .

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  $\Phi_{n_r}(X) = \frac{\Phi_{n_r}(X^{p^{u_r-1}})}{p}$ , 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 :

$$\text{Tr}_{K_r/Q}(x) = \text{Tr}_{K_r/Q}(x'') = p \text{Tr}_{K_{r-1}/Q}(x'').$$

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:  $\text{Tr}_{K/Q}(\theta) = 1$ .

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

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

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

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  $n_r^{\text{eme}}$  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  $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ .

$Tr_{\Omega\left(\frac{n_r}{p^{r-l+1}}\right)/K_{l-1}}\left(\xi^{p^{r-l+1}}\right)$  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:

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

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:

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

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: 
$$\text{PGCD}\left(\frac{n_r}{p^u}, \frac{n_r}{v}\right) = \frac{n_r}{p^u v}.$$

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:

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

Comme  $K_r \cap \Omega\left(\frac{n_r}{p^u}\right) \supset K_r \cap \Omega\left(\frac{n_r}{v}\right)$  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

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

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  $G(16.17) \text{ mod. } S_3$  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:

$$X^2 + 16 + \eta(2) + 2\eta(3.8) - \eta(8)$$



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:

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

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

$$\sqrt{-17 + 3\sqrt{17} + \sqrt{17 + \sqrt{17}}} \text{ et } \sqrt{-17 - 3\sqrt{17} + \sqrt{17 - \sqrt{17}}}$$

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  $\alpha'_0 = 6$ :*

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

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

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

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

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

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

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

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