

**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:** III.2. Bases d'entiers dans les corps cyclotomiques  
**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:** 01.07.2025

**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'ENTRIERS 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  $G(K_r/Q)$ .