

**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 DEGRÉ  $p^r$   
SUR LE CORPS DES NOMBRES RATIONNELS  
**Autor:** Oriat, Bernard  
**Kapitel:** I.5. Construction d'extensions cycliques  $K_r$  de degré  $p^r$  sur  $Q$   
DANS LE CAS OÙ  $p$  EST IMPAIR  
**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>**

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  $G(n_r)$ .