**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:** I.6. Système de générateurs de \$S\_r\$. Cas où p=2

**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:** 10.12.2025

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

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

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  $1 \le j \le m_r$ . Le noyau de  $\mu$  qui a pour base:  $\{(p-1)$   $p^{r-l+1}e_0, (p_1-1)$   $e_1, ... (p_{m_r}-1)$   $e_{m_r}\}$  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

$$\operatorname{Card}\left(\frac{G\left(n_{r}\right)}{S_{r}}\right) = \operatorname{Card}\left(\frac{Z^{m_{r}+1}}{H_{r}}\right) = p^{r}.$$

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  $\{p^ie_1, f_0, f_2, ... f_{m_r}\}$ , 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  $b_0^{(p-1)p^{r-l}} \notin S_r$ ,  $T\left(n_r, \frac{n_r}{p}\right) \nsubseteq S_r$  d'où  $K_r \nsubseteq \Omega\left(\frac{n_r}{p}\right)$ .

De même si  $m_{i-1} < j \le m_i$ , 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:

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

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

Si  $u_r = 2$ ,  $a_0$  engendre  $T\left(n_r, \frac{n_r}{4}\right)$  et  $G\left(n_r\right)$  est produit direct de  $T\left(n_r, \frac{n_r}{4}\right)$  et des sous-groupes  $T\left(n_r, \frac{n_r}{p_i}\right)$ , j de 1 à  $m_r$ .

Si  $u_r \ge 3$ ,  $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$  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  $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$ .  $G\left(n_r\right)$  est alors produit direct des sous-groupes cycliques:

$$\{a_0, 1\}$$
,  $T\left(n_r, \frac{n_r}{2^{u_r-2}}\right)$ , et  $T\left(n_r, \frac{n_r}{p_j}\right)$ ,

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  $3 \le u_r \le r + 1$ , il existe des nombres  $\alpha_0, \alpha'_0, \alpha_j$ , pour  $2 \le j \le m_r$ , 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:  $\alpha_0 \equiv 0 \ (2^{r-1})$ .

 $\alpha'_0$  vérifie la condition:

I.3.A bis: 
$$\alpha'_0 \equiv 0 \ (2^{l-1})$$
 et  $\alpha'_0 \equiv 0 \ (2^{l})$ .

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

I.3.B bis: Si 
$$m_{i-1} < j \le m_i$$
, alors  $\alpha_j = 0$   $(2^{i-1})$  et  $\alpha_i \neq 0$   $(2^i)$ .

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

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

Les  $\alpha_i$ , pour  $1 \le j \le m_r$ , vérifient la condition I.3.B bis.

- Dans le cas où  $u_r = 2$ , il existe des nombres  $\alpha_j$ , pour  $2 \le j \le m_r$ , vérifiant la condition I.3.B bis et tels que  $S_r$  soit engendré par:  $\{c_1^{2^{r-1}}a_0, c_1^{\alpha}ic_j; 2 \le j \le m_r\}$ .
- Dans le cas où  $u_r = 0$ , il existe des nombres  $\alpha_j$ , pour  $2 \le j \le m_r$ , vérifiant la condition I.3.B bis et tels que  $S_r$  soit engendré par:  $\{c_1^{2r}, c_1^{\alpha} i c_j; 2 \le j \le m_r\}$ .

On démontre tout d'abord le lemme suivant:

## LEMME I.2 bis

- Dans le cas où  $u_r \ge 3$ ,  $a_0'^{2^{r-l+1}} = 1$  et  $a_0'^{2^{r-l}} \notin S_r$ .
- Dans le cas où  $u_r = 2$ ,  $a_0 \notin S_r$ .
- Si  $m_{i-1} < j \le m_i$  alors  $c_j^{2^{r-i+1}} \in S_r$  et  $c_j^{2^{r-i}} \notin S_r$ .

En effet si  $u_r \ge 3$ , 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  $a_0^{r-l+1} \in S_r$ , alors:

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

D'où  $K_r \subseteq \Omega\left(\frac{n_r}{2}\right)$  et  $\Omega\left(n_r\right)$  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 $2^{\rm r}$ sur Q Proposition I.4 bis

Réciproquement, soit r un entier positif et  $(\Omega(n_i))_{1 \le i \le r}$  une suite de corps cyclotomiques vérifiant les conditions I.2.A bis et I.2.B bis.

— Si  $3 \le u_r \le r + 1$ , soient des nombres:  $\alpha_0 \equiv 0 \ (2^{r-1}), \ \alpha'_0$ , vérifiant I.3.A bis,  $\alpha_j$ , pour  $2 \le j \le m_r$ , vérifiant I.3.B bis. Soit  $S_r$