

## I.4. Système de générateurs de $S_r$ . Cas où est impair

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.04.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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  $p^{r-l} e_0 \notin H_r$ .