

## III.4. Bases d'entiers dans les extensions $\mathbb{K}_r$

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

### **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.

$$Tr_{K_r/Q}(x) = Tr_{K_r/Q}(x'') = p Tr_{K_{r-1}/Q}(x'').$$

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

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

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

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

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'ENTIERS 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:

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

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  $a$  :  $\eta(a) = \sum_{s \in S_r} \xi^{as}$ .