

# III.3. Conditions pour qu'une extension abélienne de $\mathbb{Q}$ POSSÈDE UNE BASE D'ENTRIERS NORMALE

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

## **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.

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  $G(K_r/Q)$ .

Alors:

$B_{r-1} \cup B(\theta, \sigma, \varphi(p^r))$  est une base de l'anneau des entiers de  $K_r$ .

Soit  $g$  un automorphisme de  $\Omega(n_r)$  prolongeant  $\sigma$ . Les classes de  $G(n_r)$  modulo  $S_r$  sont  $g^k S_r$ ,  $0 \leq k < p^r$ .

Introduisons les ensembles suivants:

$F$  est l'ensemble des racines primitives  $n_r^{\text{eme}}$  de 1 c'est-à-dire:

$$F = \{ \xi^a; a \in G(n_r) \},$$

$$F' = \{ \xi^a; a \in \bigcup_{0 \leq k \leq \varphi(p^r)} g^k S_r \}$$

et

$$F'' = \{ \xi^b; 0 \leq b < \varphi(n_r) \text{ et } p \mid b \}.$$

Puisque  $p^{ur}$  est le plus grand facteur carré divisant  $n_r$ , le lemme III.2 permet d'affirmer que le module engendré sur  $Z$  par  $F \cup F''$  est l'anneau des entiers de  $\Omega(n_r)$ . Montrons que  $F' \cup F''$  est une base de cet anneau. Pour cela il suffit de constater que:

—  $\text{Card } F' \cup F'' = \varphi(n_r)$ .

— Tout élément de  $F - F'$  appartient au module engendré par  $F'$ .

La première assertion résulte d'un dénombrement immédiat des éléments de  $F' \cup F''$ . Pour démontrer la deuxième, on écrit tout d'abord que:

$$\sum_{0 \leq k \leq p-1} \xi^{\frac{n_r}{p} k} = 0$$

( $\xi^{\frac{n_r}{p}}$  est une racine primitive  $p^{\text{eme}}$  de 1).

Soit en multipliant cette égalité par  $\xi$ , on obtient:

$$(1) \quad \sum_{a \in T\left(n_r, \frac{n_r}{p}\right)} \xi^a = 0$$

Examinons comment sont répartis les éléments de  $T\left(n_r, \frac{n_r}{p}\right)$  dans les classes de  $G(n_r)$  modulo  $S_r$ .

Puisque  $K_r \not\subseteq \Omega\left(\frac{n_r}{p}\right)$  on a  $\Omega(n_r) = K_r \cdot \Omega\left(\frac{n_r}{p}\right)$  et puisque  $K_{r-1} \subseteq \Omega\left(\frac{n_r}{p}\right)$  (condition I.2.A sur la suite  $(u_i)_{1 \leq i \leq r}$ ), on a:

$$K_{r-1} = K_r \cap \Omega\left(\frac{n_r}{p}\right).$$

Les sous-groupes correspondants de  $G(n_r)$  vont donc vérifier les égalités:

$$T\left(n_r, \frac{n_r}{p}\right) \cdot S_r = S_{r-1} \quad \text{et} \quad T\left(n_r, \frac{n_r}{p}\right) \cap S_r = \{1\},$$

qui montrent que  $S_{r-1}$ , groupe des  $K_{r-1}$ -automorphismes de  $\Omega(n_r)$ , est produit direct de  $S_r$  et de  $T\left(n_r, \frac{n_r}{p}\right)$ . Dans toute classe de  $S_{r-1}$  modulo  $S_r$ ,

il existe donc un seul élément de  $T\left(n_r, \frac{n_r}{p}\right)$ . Ces classes sont  $g^{kp^{r-1}} S_r$ ,  $0 \leq k \leq p-1$ .

Si  $sg^{p^{r-1}}$  est l'unique élément de  $g^{p^{r-1}} S_r \cap T\left(n_r, \frac{n_r}{p}\right)$ , alors

pour tout  $k$  entre 0 et  $p-1$ ,  $s^k g^{kp^{r-1}}$  est l'unique élément de  $g^{kp^{r-1}} S_r \cap$

$T\left(n_r, \frac{n_r}{p}\right)$  et les éléments de  $T\left(n_r, \frac{n_r}{p}\right)$  sont donc  $s^k g^{kp^{r-1}}$ ,  $0 \leq k \leq p-1$ .

L'égalité (1) va donc s'écrire:

$$(2) \quad \sum_{0 \leq k \leq p-1} \xi s^k g^{kp^{r-1}} = 0,$$

$s$  appartenant à  $S_r$ .

Tout élément de  $F - F''$  peut s'écrire sous la forme:

$$\xi s' s^{p-1} g^{t+(p-1)p^{r-1}} \quad \text{avec} \quad s' \in S_r \quad \text{et} \quad 0 \leq t < p^{r-1}.$$

Transformant alors l'égalité (2) par l'automorphisme  $s'g^t$ , on obtiendra:

$$\xi s' s^{p-1} g^{t+(p-1)p^{r-1}} = - \sum_{0 \leq k \leq p-2} \xi s' s^k g^{t+kp^{r-1}}.$$

Les racines primitives de 1, intervenant sous le signe  $\sum$  sont dans  $F'$ .  $F' \cup F''$  est donc une base des entiers de  $\Omega(n_r)$ .

Soit  $x$  un entier de  $K_r$ . On a  $x = x' + x''$  avec  $x'$  (respectivement  $x''$ ) appartenant au module engendré sur  $Z$ , par  $F'$  (respectivement  $F''$ ). Soit  $s$  un  $K_r$ -automorphisme. Comme  $F''$  est une base de l'anneau des entiers de

$\Omega\left(\frac{n_r}{p}\right)$ ,  $s(x'')$  appartient encore à  $\Omega\left(\frac{n_r}{p}\right)$ , donc au module engendré par  $F''$ .

De même  $s(x')$  appartient encore au module engendré par  $F'$ , car  $s$  permute entre eux les éléments de  $F'$ . Comme enfin  $s(x) = x$ , on aura donc  $s(x') = x'$  et  $s(x'') = x''$ .

$x''$  étant invariant par tout  $K_r$ -automorphisme, appartient à  $\Omega\left(\frac{n_r}{p}\right) \cap K_r$

c'est-à-dire à  $K_{r-1}$ .

Quant à  $x'$ , il s'écrit :

$$\sum_{\substack{a \in \\ 0 \leq k < \varphi(p^r)}} \lambda_a \xi^a, \lambda_a \in Z$$

De  $x' = s(x')$  on déduit que  $\lambda_a = \lambda_{a'}$  si  $a$  et  $a'$  sont congrus modulo  $S_r$ .

Posant alors  $\mu_k = \lambda_{g^k}$ , on obtient :

$$x' = \sum_{0 \leq k < \varphi(p^r)} \mu_k \left( \sum_{a \in S_r} \xi^{ag^k} \right) = \sum_{0 \leq k < \varphi(p^r)} \mu_k \sigma^k(\theta)$$

*Remarque III.1.*

On n'utilise pas complètement le fait que  $\Omega(n_r)$  est le plus petit corps cyclotomique contenant  $K_r$ , mais seulement que  $n_r$  est de la forme  $p^{u_r} n'$ , avec  $n'$  premier avec  $p$ , sans facteur carré,  $K_r \subseteq \Omega(n_r)$  et  $K_r \not\subseteq \Omega\left(\frac{n_r}{p}\right)$ .

PROPOSITION III.2.

Soit  $K$  une extension abélienne de  $Q$ . Les conditions suivantes sont équivalentes :

III.2.A:  $K$  possède une base d'entiers normale.

III.2.B: Il existe un entier  $\theta$  de  $K$  tel que  $Tr_{K/Q}(\theta) = 1$ .

III.2.C: Le plus petit corps cyclotomique contenant  $K$  possède une base d'entiers normale.

III.2.D:  $K$  est modérément ramifiée.

$C \Rightarrow A$  et  $A \Rightarrow B$  résultent des rappels effectués au paragraphe III.1.

$B \Rightarrow C$  résulte pour les extensions cycliques de degré  $p^r$  sur  $Q$  de la proposition III.1. Reprenant les mêmes notations, si  $\Omega(n_r)$  ne possède pas de base d'entiers normale, alors, d'après le lemme III.3,  $n_r$  possède un facteur carré, donc  $u_r \geq 2$ .

Comme  $\Phi_{n_r}(X) = \frac{\Phi_{n_r}(X^{p^{u_r-1}})}{p}$ , la trace de  $\xi$  sur  $Q$  est nulle, donc celle

de  $\theta$  également. Si  $x$  est un entier de  $K_r$ ,  $x$  se décompose comme précédemment en  $x = x' + x''$  et l'on a :

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

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  $K_r$ .