III.2. Bases d'entiers dans les corps cyclotomiques

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

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.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CHAPITRE III

BASES D'ENTIERS

III.1. RAPPELS

Bases d'entiers normales

Soit K une extension abélienne de Q. On dit qu'un élément θ de K engendre une base normale des entiers de K si l'anneau des entiers de K admet pour base, sur Z, l'ensemble des conjugués de θ.

Si K possède une base d'entiers normale, engendrée par θ, alors:

— Tout sous-corps L de K possède également une base d'entiers normale engendrée par $Tr_{K/L}(\theta)$.

En effet, tout entier x de L, s'écrit:

$$x = \sum_{\sigma \in G(K/Q)} \lambda_\sigma \, \sigma(\theta), \ \lambda_\sigma \text{ appartenant à } Z.$$

Puisque x est invariant par tout L-automorphisme de K, alors $\lambda_\sigma = \lambda_{\sigma'}$, pour tous σ et σ' situés dans la même classe modulo $G({}^{K}/_{L})$.

— La trace de θ sur Q est égale à ± 1.

En effet Z n'a pas d'autre base d'entiers que $\{1\}$ ou $\{-1\}$.

Corps cyclotomiques

ξ étant une racine primitive n^{eme} de 1, on notera $\Phi_n(X)$ le n^{eme} polynome cyclotomique, c'est-à-dire le polynome minimal de ξ sur Q. On rappelle qu'on a la relation: $X^n - 1 = \prod_{k|n} \Phi_k(X)$.

Si $n = p_1^{u_1} \dots p_m^{u_m}$ est la décomposition de n en facteurs premiers, on a:

$$\Phi_n(X) = \Phi_{p_1 \dots p_m}\left(X^{p_1^{u_1-1} \dots p_m^{u_m-1}}\right)$$

([6] chapitre 8).

III.2. BASES D'ENTIERS DANS LES CORPS CYCLOTOMIQUES

LEMME III.1.

Soit d un entier sans facteur carré et ξ une racine primitive d^{eme} de 1. On a alors $Tr_{\Omega(d)/Q}(\xi) = (-1)^m$, m étant le nombre de facteurs premiers de d.

On peut raisonner par récurrence sur m, en utilisant: $\Phi_d = \dfrac{X^d - 1}{\prod\limits_{\substack{k|d \\ k \neq d}} \Phi_k}$.

Pour tout diviseur k de d soit m_k le nombre de facteurs premiers de k. D'après l'hypothèse de récurrence, les Φ_k sont de la forme:

$$X^{\varphi(k)} - (-1)^{m_k} X^{\varphi(k)-1} + \dots$$

et $\prod\limits_{\substack{k|d \\ k \neq d}} \Phi_k$ sera de la forme:

$$X^{\varphi(d)-d} - s X^{\varphi(d)-d-1} + \dots \qquad \text{avec} \qquad s = \sum_{\substack{k|d \\ k \neq d}} (-1)^{m_k}.$$

Comme le nombre de diviseurs k de d, possèdant m_k facteurs premiers est $C_m^{m_k}$, on aura donc:

$$s = \sum_{0 \leq j \leq m-1} (-1)^j C_m^j = -(-1)^m.$$

Φ_d sera donc de la forme:

$$X^{\varphi(d)} - (-1)^m X^{\varphi(d)-1} + \dots$$

LEMME III.2.

> Soient n et d deux entiers tels que d soit sans facteur carré et premier avec n. Soit ξ une racine primitive $(nd)^{\text{eme}}$ de 1. Soient F l'ensemble des racines primitives $(nd)^{\text{eme}}$ de 1 et F'' l'ensemble des ξ^b tels que: $0 \leqq b < \varphi(nd)$ et $PGCD(b, n) \neq 1$.
>
> Alors le module engendré sur Z par $F \cup F''$ est l'anneau des entiers de $\Omega(nd)$.

Comme $\{1, \xi, \xi^2, \dots, \xi^{\varphi(nd)-1}\}$ est une base de l'anneau des entiers de $\Omega(nd)$, il suffit de montrer que si c est premier avec n et non premier avec d, alors ξ^c appartient au module engendré par F.

Soit $v = PGCD(c, d)$. $\xi^{\frac{nd}{v}}$ est une racine primitive veme de 1 et v est sans facteur carré. D'après le lemme III.1, on a la relation:

$$\pm 1 = \sum_{\substack{0<k<v \\ PGCD(k,v)=1}} \xi^{\frac{ndk}{v}} \quad \text{d'où: } \xi^c = \pm \sum_{\substack{0<k<v \\ PGCD(k,v)=1}} \xi^{\frac{ndk}{v}+c}$$

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 ξ, racine primitive d^{eme} 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 ξ une racine primitive $(p^2)^{\text{eme}}$ de 1. Comme $\Phi_{p2}(X) = \Phi_p(X^p)$, on a $Tr_{\Omega(p2)/Q}(\xi) = 0$. D'autre part:

$$Tr_{\Omega(p^2)/Q}(\xi^p) = p\, Tr_{\Omega(p)/Q}(\xi^p) = -p$$

et la trace de toute racine $(p^2)^{\text{eme}}$ 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 surcorps 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'ENTIERS NORMALE

> *Notation :* Si K est une extension cyclique sur Q, θ un élément de K, σ un automorphisme de K, t un entier positif, $B(\theta, \sigma, t)$ désignera l'ensemble des t premiers conjugués successifs de θ par σ, c'est-à-dire:
>
> $$B(\theta, \sigma, t) = \{\sigma^k(\theta), 0 \leqq k < t\}$$

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 ξ est une racine primitive $(n_r)^{\text{eme}}$ 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 σ un générateur de $G(K_r/Q)$.