

3. Etude du cas p = 2. Résultats généraux

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **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.

3. ETUDE DU CAS $p = 2$. RÉSULTATS GÉNÉRAUX

Ce paragraphe regroupe quelques résultats valables pour tous les corps dyadiques.

3.1. Proposition

Soit u une unité de A , anneau des entiers du corps dyadique K (extension finie de \mathbf{Q}_2).

1. Le plus petit entier impair $2k+1$ tel que $u\pi^{2k+1}$ soit somme de carrés d'entiers est $2d+1$; (d est la partie entière de $e/2$).

2. Pour que u soit somme de carrés d'entiers ($u \in V$), il faut et il suffit qu'on ait $\delta(u) \geq e$. De plus, si on a $\delta(u) \geq e+1$, alors u est somme de deux carrés d'entiers.

Remarquons que -1 est somme de carrés dans A , ce qui permet d'affirmer que A_2 est bien un sous-anneau de A : dans l'anneau \mathbf{Z}_2 des entiers dyadiques, -7 est un carré car 2 est une uniformisante et -7 est congru à 1 modulo 8 . Il en résulte que $-1 = 1+1+4-7$ est somme de quatre carrés dans A . Ceci étant:

1. Pour tout élément a de A on a l'égalité $2a = (a+1)^2 - (a^2+1)$; par conséquent $2a$ est somme de carrés dans A . Plus précisément, si b est une racine carrée de -7 dans \mathbf{Z}_2 , on a l'égalité obtenue à partir de la propriété de multiplicativité de la norme des quaternions:

$$2a = (1+a)^2 + (1+a)^2 + (1-a)^2 + (2+ab)^2 + (2a-b)^2.$$

Par ailleurs, il existe une unité ε de A satisfaisant à $\pi^e = 2\varepsilon$. Dans ces conditions on a bien $u\pi^e \in A_2$ pour toute unité u de A . En particulier, on a $u\pi^{2d+1} \in A_2$ pour toute unité u de A .

Réciproquement, soit u une unité de A , $2k+1$ un entier impair tels qu'on ait $u\pi^{2k+1} \in A_2$; il existe une famille finie $\{a_1, \dots, a_N\}$ d'éléments de A telle que:

$$u\pi^{2k+1} = \sum_{j=1}^N a_j^2 = \left(\sum_{j=1}^N a_j \right)^2 - 2 \sum_{1 \leq i < j \leq N} a_i a_j.$$

Comparons les valuations \mathfrak{B} -adiques de chacun des termes écrits ci-dessus; on a $v_K(u\pi^{2k+1}) \geq \min \left\{ 2v_K \left(\sum_{j=1}^N a_j \right), e + v_K \left(\sum_{1 \leq i < j \leq N} a_i a_j \right) \right\}$. On ne peut

avoir $2v_K \left(\sum_{j=1}^N a_j \right) < e + v_K \left(\sum_{1 \leq i < j \leq N} a_i a_j \right)$ car $v_K(u\pi^{2k+1})$ est impair. On en conclut que $2k+1 \geq e$ et de façon plus précise que k est supérieur ou égal à d .

2. Si $u \in U$ est une somme de carrés dans A , il existe une famille finie d'éléments de A , soit $\{a_1, \dots, a_N\}$, telle que

$$u = \sum_{j=1}^N a_j^2 = \left(\sum_{j=1}^N a_j \right)^2 - 2 \sum_{i < j} a_i a_j;$$

ceci prouve que $\delta(u)$ est supérieur ou égal à e . Réciproquement, si $\delta(u)$ est supérieur ou égal à e , il existe une unité v de A et un entier b tels que $u = v^2 + \pi^e b$; or on vient de voir que $\pi^e b$ est somme de carrés dans A .

3. Si l'unité u satisfait à $\delta(u) \geq e+1$, il existe une unité v de A et un entier b tels qu'on ait:

$$u = v^2 + 2\pi b = \frac{1}{2} v^2 [1 + 1 + 4\pi b v^{-2}].$$

De l'égalité (CAR) obtenue au paragraphe (1.3.2.) on déduit:

$$u = \frac{1}{2} v^2 \left\{ 1 + \left[1 + \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n} \right]^2 \right\},$$

$$u = v^2 \left\{ \left[1 + \frac{1}{2} \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n} \right]^2 + \left[\frac{1}{2} \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n} \right]^2 \right\}.$$

Alors u est somme de deux carrés dans A puisque pour tout $n \geq 1$ $\binom{2n}{n}$ est un nombre pair.

3.2. Théorème

Soit T la sous-extension non ramifiée maximale de K et soit B l'anneau des entiers de T . Alors :

1. Les anneaux B et B_2 coïncident, c'est-à-dire que tout entier de T est somme de carré d'entiers de T .

2. L'anneau A_2 est un anneau local, nœthérien, de dimension 1 ; son idéal maximal est $\mathfrak{P} \cap A_2$. En tant que B -module, A_2 est libre de rang e . En tant que B -algèbre, A_2 est égal à $B[\pi^2, 2\pi]$.

3. Avec les notations 1, on a la double égalité :

$$(A : A_2) = (U : V) = 2^{df}$$

1. Puisque B est non ramifié sur \mathbf{Z}_2 , 2 est une uniformisante de B ; tout élément non nul de B s'écrit donc de façon unique sous la forme $2^n(1+2a)$ avec $n \in \mathbf{N}$ et $a \in B$, et on a dans $B : 1+2a = (a+1)^2 + a^2 + a^2 + 4a^2 + (\sqrt{-7})^2 a^2$.

2. L'anneau A est une extension totalement ramifiée de B ; il en résulte que π , uniformisante de A , est racine d'un polynôme d'Eisenstein à coefficients dans B ; en d'autres termes, il existe une unité b_0 de B et $(e-1)$ éléments b_1, \dots, b_{e-1} de B tels qu'on ait :

$$\pi^e = 2 \sum_{j=0}^{e-1} b_j \pi^j .$$

Par ailleurs, on sait que $A = B[\pi]$ et que la famille $\{1, \pi, \dots, \pi^{e-1}\}$ est une base du B -module A . On va montrer que si e est pair, (resp. impair), la famille $\{1, 2\pi, \pi^2, \dots, \pi^{e-2}, 2\pi^{e-1}\}$ (resp. $\{1, 2\pi, \pi^2, \dots, 2\pi^{e-2}, \pi^{e-1}\}$) constitue une base de A_2 considéré comme B -module. En premier lieu, il est clair que B est un sous-anneau de A^2 et que la famille considérée est libre sur B .

Remarquons qu'on peut choisir comme système R de représentants non nuls de A modulo \mathfrak{P} un ensemble d'unités de B , ces unités étant elles-mêmes des carrés dans B . (On a en effet $\bar{K} = \bar{K}^2$ et toute unité de B est congrue à un carré modulo $2B$.) Tout élément a de A admet donc un développement de Hensel de la forme :

$$a = \sum_{j=0}^{\infty} r_j^2 \pi^j \quad (r_j^2 \in R \cup \{0\} \quad \text{pour tout } j \in \mathbf{N}).$$

En particulier, il résulte de la proposition 3.1.1.) que tout $a \in A_2$ admet un développement de Hensel de la forme :

$$a = \sum_{j=0}^d r_{2j}^2 \pi^{2j} + \pi^{1+2d} \sum_{j=0}^{\infty} r_{j+1+2d}^2 \pi^j .$$

Remarquons alors les détails suivants :

a) L'ensemble A_2 est un fermé de A pour la topologie \mathfrak{P} -adique. Ceci est encore une conséquence de la proposition 3.1.1.).

b) L'ensemble $B[\pi^2, 2\pi]$ est un fermé de A pour la topologie \mathfrak{P} -adique.

Or sur $B[\pi^2, 2\pi]$ cette topologie coïncide avec l'unique prolongement à cet espace de la topologie 2-adique de B . En particulier $B[\pi^2, 2\pi]$ est un fermé de A_2 .

Il reste en définitive à prouver que $B[\pi^2, 2\pi]$ est dense dans A_2 . Pour cela, il suffit de montrer que pour tout $n \in \mathbb{N}$, π^{e+n} est combinaison linéaire à coefficients dans B des éléments de la famille considérée plus haut. Faisons la démonstration dans le cas e pair; (dans le cas e impair, la démonstration est analogue):

Les remarques faites au début de la démonstration montrent que la propriété à démontrer est vraie pour $n = 0$. De plus, on a les égalités:

$$\pi^{e+1} = 2\pi \sum_{j=0}^{e-1} b_j \pi^j = 2 \sum_{j=0}^{d-2} b_{2j+1} \pi^{2(j+1)} + 2b_{e-1} \pi^e + 2\pi \sum_{j=0}^{d-1} b_{2j} \pi^{2j};$$

$$\pi^{e+1} = 2b_0 b_{e-1} + \sum_{j=1}^{d-1} (b_{2j-1} + 2b_{e-1} b_{2j}) \pi^{2j}$$

$$+ 2\pi \sum_{j=0}^{d-1} (b_{2j} + 2b_{e-1} b_{2j+1}) \pi^{2j};$$

$$\pi^{e+2} = 2b_{e-1} \pi^{e+1} + 2b_{e-2} \pi^e + \sum_{j=0}^{e-3} 2b_j \pi^{j+2}.$$

A partir de là on raisonne par récurrence sur m pour évaluer π^{e+2m} et π^{e+1+2m} .

Enfin, puisque B est un anneau de valuation discrète, la B -algèbre de type fini $B[\pi^2, 2\pi]$ est un anneau noëthérien; puisque A est un anneau de valuation discrète entier sur A_2 , l'unique idéal maximal de A_2 est $\mathfrak{P} \cap A_2$.

3. L'égalité $(A : A_2) = 2^{df}$ résulte de ce que $\{1, \pi, \dots, \pi^{e-1}\}$ est une base de A en tant que B -module, tandis qu'une base de A_2 comme B -module est $\{1, 2\pi, \dots, 2\pi^{e-1}\}$ ou $\{1, 2\pi, \dots, \pi^{e-1}\}$ selon que e est pair ou impair. Reste à démontrer la dernière égalité.

Pour tout $n \geq 1$ soit U_n le sous-groupe $1 + \mathfrak{P}^n$ de U . On sait que $(U : U_1) = 2^f - 1$ et que pour tout $n \geq 1$ on a $(U_n : U_{n+1}) = 2^f$. (Pour plus de détails, voir [4] ou [5].) Il résulte de la proposition 3.1, 1), qu'on a:

$$V = U^2 \cdot U_{2d+1}.$$

Montrons qu'on a $U^2 \cap U_{2d+1} = U_{d+1}^2$. L'inclusion $U_{d+1}^2 \subset U^2 \cap U_{2d+1}$ est évidente. Réciproquement, soit $x \in U$ tel que $x^2 = 1 + a\pi^{2d+1}$ avec $a \in A$. Quitte à changer x en $-x$ on peut écrire x sous la forme $1 + b\pi^2$ avec $\varepsilon \geq 1$ et $b \in A$. On obtient alors $b^2 \pi^{2\varepsilon} = a\pi^{2d+1} - 2b\pi^\varepsilon$ ce qui implique $2\varepsilon \geq 2d+1$ et $\varepsilon \geq d+1$.

Ceci montre l'existence d'un isomorphisme entre le groupe V/U_{2d+1} et le groupe U^2/U_{d+1}^2 . La proposition sera alors une conséquence du lemme de Herbrand :

Lemme de Herbrand. Soit $\varphi : G \rightarrow G'$ un homomorphisme de groupes et soit H un sous-groupe de G .

1. Les deux assertions suivantes sont équivalentes :
 - a) le sous-groupe H est d'indice fini dans G ;
 - b) les indices $(\varphi(G) : \varphi(H))$ et $(\text{Ker } \varphi = H \cap \text{Ker } \varphi)$ sont finis.
2. Si les assertions ci-dessus sont vraies, alors :

$$(G:H) = (\varphi(G) : \varphi(H)) \cdot (\text{Ker } \varphi : H \cap \text{Ker } \varphi).$$

Pour une démonstration, voir [4] § 63.

Appliquons ce lemme au groupe U , à son sous-groupe U_{d+1} et à l'homomorphisme $\varphi : U \rightarrow U^2 (x \mapsto x^2)$; puisque -1 appartient à U_{d+1} , on a l'égalité

$$(U : U_{d+1}) = (U^2 : U_{d+1}^2)$$

et les égalités :

$$(U : U_{2d+1}) = (U : U_{d+1}) (U_{d+1} : U_{2d+1}) = (U : V) (V : U_{2d+1}).$$

On en conclut :

$$(U : V) = (U_{d+1} : U_{2d+1}) = 2^{df}.$$

4. RÉSULTATS PROPRES AU CAS $p = 2$ ET e IMPAIR

4.1. Théorème

Supposons e impair et soit $u \in U$. Alors :

1. Si $\delta(u) > e$, u est somme de deux carrés dans A ;
2. Si $\delta(u) = e$, il existe $a, b \in U$ tels que $u = a^2 + 2b$; avec ces notations, les trois assertions suivantes sont équivalentes :
 - a) l'unité u est somme de deux carrés dans $A (u \in V_2)$;
 - b) la trace absolue de (b/a^2) appartient à $2\mathbb{Z}_2$;
 - c) il existe $c \in U$ tel que $b = a^2(c^2 - c)$.

De plus :