4. DÉMONSTRATION DU THÉORÈME 4

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **16 (1970)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.05.2024**

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

M désignant la matrice de $L(u_1), \ldots, L(u_r)$ dans la base canonique de $\mathbf{R}^a$, et les λ_j désignant les quantités $\log |x_j|_j$. Par construction des x_j, on a $\lambda_1 \neq 0, \ldots \lambda_d \neq 0$; d'après le théorème (1), M est de rang $r = a - 1$: la matrice ci-dessus est donc de rang $r + d = s - 1$, et aussi le groupe $\Lambda(G)$, ce qui prouve (d).

(b), (c) et (d) montrent que $\Lambda(U_S)$ est un réseau de rang exactement $s - 1$, et le théorème (3) est démontré.

4. Démonstration du théorème 4

La partie (v) de la proposition 1 du §2 montre que l'application $\mathfrak{a} \mapsto \mathfrak{a}A_S$ définit un homomorphisme surjectif φ du groupe des idéaux de A sur le groupe des idéaux de A_S; comme φ transforme évidemment tout idéal principal en un idéal principal, φ donne lieu par passage au quotient à un homomorphisme surjectif du groupe des classes d'idéaux de A sur le groupe des classes d'idéaux de A_S; comme le premier groupe est fini, d'ordre h (théorème (2)), le second est lui aussi fini, d'ordre h_S diviseur de h, d'où la première assertion du théorème (4).

Le même raisonnement prouve d'ailleurs plus généralement que si $S \subset S'$, alors $h_{S'}$ divise h_S: pour achever de démontrer le théorème (4), il suffit donc de prouver ceci: *il existe un ensemble S tel que $h_S = 1$.*

Or, soient $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ des idéaux entiers de A représentant les h classes d'idéaux de A, et soit $D = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d\}$ l'ensemble des idéaux premiers de A qui divisent l'un au moins des $\mathfrak{a}_i$; enfin, soit S l'ensemble formé des places archimédiennes de K et des places discrètes appartenant à D; alors, $h_S = 1$: en effet, soit $\mathfrak{b}$ un idéal entier de A_S; il existe un idéal entier $\mathfrak{a}$ de A tel que $\mathfrak{b} = \mathfrak{a}A_S$ (prop. 1, (v)); d'autre part, il existe $y \in K^*$ et i tels que $\mathfrak{a} = y\mathfrak{a}_i$; enfin, $\mathfrak{a}_i$ se décompose en produit de facteurs premiers appartenant tous à D:

$$\mathfrak{a}_i = \mathfrak{p}_1^{m_1} \mathfrak{p}_2^{m_2} \ldots \mathfrak{p}_d^{m_d}.$$

D'où immédiatement (prop. 1, (iv))

$$\mathfrak{b} = yA_S;$$

$\mathfrak{b}$, idéal entier quelconque de A_S, est principal, et $h_S = 1$. Le théorème (4) est entièrement démontré.

Notons qu'il suffit, dans la démonstration ci-dessus, de prendre pour D une famille finie d'idéaux premiers dont les classes forment un système générateur du groupe des classes de A. Dans la pratique, il est facile de

déterminer explicitement une telle famille: on sait en effet (voir par exemple [10], p. 70) que toute classe d'idéaux de A contient un idéal entier $\mathfrak{a}$ tel que

$$N\mathfrak{a} \leqq M_K = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|},$$

Δ désignant le discriminant de K. On voit donc qu'on peut prendre pour D l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que $N\mathfrak{p} \leq M_K$. Bien entendu, l'ensemble D ainsi construit est en général « beaucoup trop grand »: mais il est clair que la détermination d'un D « minimal » équivaut pratiquement à la détermination de la structure du groupe des classes de A, ce qui est une autre affaire.

5. Un exemple explicite

Montrons pour terminer, sur un exemple numérique simple, que les méthodes précédentes mènent à des résultats tout à fait explicites. Nous considérons le corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-23})$, pour lequel $n = 2$, $r_1 = 0$, $r_2 = 1$, $a = 1$, $r = 0$, $W = \{1, -1\}$. Posons:

$$\alpha = \frac{-1+\sqrt{-23}}{2};$$

le polynôme minimal de α sur $\mathbf{Q}$ est $X^2 + X + 6$, et on a $A = \mathbf{Z}[\alpha]$, Δ (le discriminant) $= -23$. De là

$$\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|} = \frac{2\sqrt{23}}{\pi} \leq 4,$$

et le groupe des classes de A est engendré par les classes des facteurs premiers de 2 et de 3 dans A. Mais (pour $p = 2,3$) on a

$$A/pA = \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/(p, X^2+X+6)$$

d'où, puisque $6 \equiv 0 \pmod{p}$,

$$A/pA \simeq \mathbf{Z}[X]/(p, X^2+X) \simeq \mathbf{F}_p[X]/(X(X+1))$$

et finalement $A/pA \simeq \mathbf{F}_p \times \mathbf{F}_p$. Ainsi, 2 et 3 sont décomposés dans A, et le calcul ci-dessus montre plus précisément qu'on peut écrire

$$(2) = \mathfrak{p}\bar{\mathfrak{p}}, \quad (3) = \mathfrak{q}\bar{\mathfrak{q}},$$

avec