

# 3. DÉMONSTRATION DU THÉORÈME (3)

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.09.2024**

## **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.

Resté à prouver (ii). L'inclusion  $T^{-1}A \subset A_S$  est évidente, puisqu'on a déjà remarqué que  $t$  est une  $S$ -unité, donc que les  $1/t^m$  ( $m \geq 0$ ) sont des  $S$ -entiers. Inversement, soit  $y \in A_S$ , et considérons le produit  $yt^m$  ( $m \geq 0$ ). En tout  $\mathfrak{q} \notin D$ , on a, d'après (i),

$$v_{\mathfrak{q}}(yt^m) = v_{\mathfrak{q}}(y) \geq 0.$$

En  $\mathfrak{p}_j \in D$ , on a, toujours d'après (i),

$$v_j(yt^m) = v_j(y) + mv_j(t) \geq v_j(y) + m.$$

Choisissons pour  $m$  une valeur  $\geq \sup_j |v_j(y)|$  et posons  $x = yt^m$ . Pour toute valuation discrète normalisée  $v$  de  $K$ , on a alors  $v(x) \geq 0$ : donc  $x \in A$ ,  $y = x/t^m \in T^{-1}A$ , et finalement  $A_S \subset T^{-1}A$ , ce qui achève de démontrer (ii), et la proposition.

### 3. DÉMONSTRATION DU THÉORÈME (3)

Nous noterons  $z_1, z_2, \dots, z_s$  les coordonnées dans l'espace  $\mathbf{R}^s = \mathbf{R}^a \times \mathbf{R}^d = \mathbf{R}^{r+1} \times \mathbf{R}^d$ .

La démonstration se décomposera en quatre parties:

(a) *L'homomorphisme  $\Lambda$  a pour noyau  $W$ .*

En effet, si  $x \in U_S$ , l'égalité  $\Lambda(x) = 0$  implique d'abord

$$|x|_{a+1} = \dots = |x|_s = 1,$$

ce qui signifie que  $x$  est non seulement une  $S$ -unité, mais une unité de  $A$ ;  $\Lambda(x) = 0$  implique d'autre part  $|x|_1 = \dots = |x|_a = 1$ , ce qui montre que cette unité  $x$  appartient au noyau de  $L$ , donc à  $W$  (théorème (1)); inversement, il est clair que  $x \in W$  implique  $\Lambda(x) = 0$ . D'où (a).

(b)  *$\Lambda(U_S)$  est un sous-groupe discret de  $\mathbf{R}^s$ .*

Les valeurs absolues  $|\cdot|_{a+1}, \dots, |\cdot|_s$  provenant de valuations discrètes, il est clair qu'on peut trouver dans  $\mathbf{R}^d$  un voisinage  $V'$  de l'origine tel que la condition

$$(\log |x|_{a+1}, \dots, \log |x|_s) \in V'$$

implique  $|x|_{a+1} = \dots = |x|_s = 1$ , ce qui signifie (si  $x \in U_S$ ) que  $x$  est en fait une unité de  $A$ . Soit alors  $V$  un voisinage borné de 0 dans  $\mathbf{R}^a$ : la double condition

$$x \in U_S \text{ et } \Lambda(x) \in V \times V'$$

peut s'écrire

$$x \in U \text{ et } L(x) \in V,$$

et d'après le théorème (1), ceci n'est possible que pour un nombre fini de  $x$ . D'où (b).

(c)  $\Lambda(U_S)$  est contenu dans l'hyperplan  $z_1 + z_2 + \dots + z_s = 0$ .

Supposons en effet  $x \in U_S$  et décomposons l'idéal  $xA$  en facteurs premiers (dans  $A$ ):

$$xA = \prod_{1 \leq j \leq d} \mathfrak{p}_j^{v_j(x)}.$$

Egalons les normes absolues des deux membres:

$$|Nx| = \prod_{1 \leq j \leq d} (N\mathfrak{p}_j)^{v_j(x)}.$$

Si  $\sigma_1, \dots, \sigma_n$  sont les plongements  $K \rightarrow \mathbf{C}$  indexés de telle manière que  $\sigma_1, \dots, \sigma_{r_1}$  soient les plongements réels, et que, pour  $1 \leq k \leq r_2$ ,  $\sigma_{r_1+k}$  et  $\sigma_{r_1+r_2+k}$  soient complexes conjugués, la formule ci-dessus devient

$$\prod_{1 \leq i \leq r_1} |\sigma_i x| \cdot \prod_{r_1+1 \leq i \leq a} |\sigma_i x|^2 \cdot \prod_{1 \leq j \leq d} (N\mathfrak{p}_j)^{-v_j(x)} = 1,$$

soit, compte tenu de la définition des valeurs absolues normalisées:

$$\prod_{1 \leq i \leq s} |x|_i = 1.$$

(c) résulte de là, en prenant les logarithmes. Notons que nous venons en fait de redémontrer la formule du produit.

(d)  $\Lambda(U_S)$  contient un réseau de rang  $s - 1$ .

C'est en principe la partie difficile: en réalité, tout le travail a été fait dans le théorème (1). Soit en effet  $u_1, u_2, \dots, u_r$  (rappel:  $r = a - 1 = r_1 + r_2 - 1$ ) un système fondamental d'unités de  $K$  (nous utilisons le théorème (1)) et considérons le sous-groupe  $G$  de  $U_S$  engendré par  $u_1, \dots, u_r, x_1, \dots, x_d$ .  $\Lambda(G)$  est un sous-groupe de  $\Lambda(U_S)$  (donc un réseau de  $\mathbf{R}^s$ ), et il est engendré par  $\Lambda(u_1), \dots, \Lambda(u_r), \Lambda(x_1), \dots, \Lambda(x_d)$ . La matrice de ces  $r + d = s - 1$  vecteurs dans la base canonique de  $\mathbf{R}^s = \mathbf{R}^a \times \mathbf{R}^d$  s'écrit

$$\left. \begin{array}{l} \mathbf{R}^a \\ \vdots \\ \mathbf{R}^d \end{array} \right\} \left[ \begin{array}{c|ccc} & M & & X \\ \hline & & \lambda_1 & \\ & & & \lambda_2 \\ & 0 & & \cdot \\ & & & \cdot \\ & & & \cdot \\ & & & \lambda_d \end{array} \right]$$

$M$  désignant la matrice de  $L(u_1), \dots, L(u_r)$  dans la base canonique de  $\mathbf{R}^a$ , et les  $\lambda_j$  désignant les quantités  $\log |x_j|_j$ . Par construction des  $x_j$ , on a  $\lambda_1 \neq 0, \dots, \lambda_d \neq 0$ ; 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  $\alpha \mapsto \alpha A_S$  définit un homomorphisme surjectif  $\varphi$  du groupe des idéaux de  $A$  sur le groupe des idéaux de  $A_S$ ; comme  $\varphi$  transforme évidemment tout idéal principal en un idéal principal,  $\varphi$  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  $\alpha_1, \alpha_2, \dots, \alpha_h$  des idéaux entiers de  $A$  représentant les  $h$  classes d'idéaux de  $A$ , et soit  $D = \{p_1, p_2, \dots, p_d\}$  l'ensemble des idéaux premiers de  $A$  qui divisent l'un au moins des  $\alpha_i$ ; 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  $\alpha$  de  $A$  tel que  $\mathfrak{b} = \alpha A_S$  (prop. 1, (v)); d'autre part, il existe  $y \in K^*$  et  $i$  tels que  $\alpha = y\alpha_i$ ; enfin,  $\alpha_i$  se décompose en produit de facteurs premiers appartenant tous à  $D$ :

$$\alpha_i = p_1^{m_1} p_2^{m_2} \dots p_d^{m_d}.$$

D'où immédiatement (prop. 1, (iv))

$$\mathfrak{b} = y A_S;$$

$\mathfrak{b}$ , 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