LE MATHÉMATICIEN

SECTION DIRIGÉE PAR JEAN-PIERRE KAHANE

14

COLLECTION SUP

Les nombres p-adiques

YVETTE AMICE

Professeur à l'Université, Paris VII

Préface de Ch. Pisot

PRESSES UNIVERSITAIRES DE FRANCE

Dépôt légal. — 1re édition : 4e trimestre 1975

SOMMAIRE

Préface

La théorie des nombres, c'est-à-dire l'étude des propriétés des nombres entiers, a suscité l'intérêt des mathématiciens depuis la plus haute Antiquité. Les énoncés des théorèmes sont souvent d'une grande simplicité, en revanche les démonstrations s'avèrent généralement extrêmement difficiles. Cependant les résultats obtenus sont pour la plupart dénués de toute application pratique. On peut donc se demander pourquoi cette discipline continue à occuper une place aussi importante dans les mathématiques, à tel point que beaucoup des plus grands mathématiciens y ont consacré des efforts considérables. La raison doit précisément être cherchée dans les difficultés de la théorie. Les chercheurs ont été conduits à imaginer des méthodes nouvelles et ces méthodes se sont ensuite appliquées à de nombreuses autres branches des mathématiques auxquelles elles ont apporté des outils efficaces. Il s'ensuit qu'à côté des problèmes posés par les sciences expérimentales la théorie des nombres a été l'une des sources importantes de progrès pour l'ensemble des mathématiques. Pour illustrer cette assertion, je citerai trois exemples : l'algèbre, dont l'élaboration provient des efforts faits pour résoudre des équations en nombres entiers ; les espaces vectoriels, dont les propriétés fondamentales sont apparues dans l'étude des corps de nombres algébriques ; les fonctions d'une variable complexe, dont les connaissances ont fortement progressé par toutes les tentatives entreprises pour élucider l'hypothèse de Riemann sur la fonction ζ. C'est ainsi que depuis quelques années, essentiellement depuis le travail de B. Dwork en 1960 sur les fonctions ζ de variétés, une nouvelle méthode est en train de s'élaborer pour attaquer les problèmes, c'est l'analyse p - adique. On sait depuis deux siècles que l'utilisation des fonctions d'une variable complexe apporte une aide puissante en théorie des nombres. Or le corps des nombres

complexes est le corps complet et algébriquement clos pour la valeur absolue ordinaire sur le corps **Q** *des nombres rationnels. Mais on sait depuis 1917 par A. Ostrowski qu'il existe d'autres valeurs absolues sur* **Q** *et qu'à chaque nombre premier* p *est attachée une telle valeur absolue. Les premières recherches ont alors concerné les notions algébriques liées aux corps complétés de* **Q** *relativement à cette valeur absolue et elles ont fait l'objet de plusieurs traités maintenant classiques. Cependant un corps complet algébriquement clos contenant* **Q** *est l'analogue du corps des nombres complexes ordinaire et on est en droit d'espérer que c'est l'analyse dans de tels corps p - adiques qui sera un outil important pour certains problèmes de la théorie des nombres. Le résultat de B. Dwork a renforcé cet espoir et depuis nous assistons à l'élaboration de la théorie des fonctions analytiques p - adiques. Après avoir cherché à calquer le modèle complexe, la construction de cette théorie s'avère nécessiter des idées différentes et nouvelles ; elle propose un champ très vaste et encore peu exploré aux chercheurs doués d'imagination créatrice. L'expérience du passé permet de prédire que des progrès dans le p - adique auront des répercussions sur l'ensemble des mathématiques.*

L'ouvrage que je vous présente a été écrit par Mme Amice, à laquelle on doit en particulier de savoir que les séries d'interpolation sont un instrument de choix dans l'étude des fonctions analytiques ; il est destiné à faciliter aux chercheurs l'accès à l'analyse p - adique. Il n'y est fait appel qu'aux connaissances normales d'un étudiant de deuxième cycle universitaire ; le lecteur y est conduit progressivement depuis la construction des corps de nombres p - adiques jusqu'à l'étude des propriétés des fonctions analytiques. Cette étude est illustrée par une application aux fractions rationnelles ; ces dernières ont joué un rôle important dans le travail de B. Dwork. On sait aussi que Hadamard, auquel on doit le théorème des nombres premiers, avait débuté ses recherches sur les fonctions analytiques classiques par l'étude des fractions rationnelles.

Ajoutons encore que de nombreux exercices apportent des compléments intéressants au texte et permettent au lecteur d'acquérir l'expérience du domaine nouveau et souvent déconcertant qui se présente à lui.

La parution d'un tel ouvrage est devenue de plus en plus nécessaire. De nombreux chercheurs sont attirés par le p - adique dont les propriétés connues se trouvent dispersées dans des articles parus dans des revues diverses. Mme Amice a fait une synthèse, très souvent améliorée par des apports personnels, qui simplifie et rend plus élégants de nombreux résultats. Ce livre vient à point et sera accueilli avec joie par tous les mathématiciens qui veulent s'intéresser à l'analyse p - adique.

Ch. PISOT.

NOTATIONS

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$: les nombres entiers naturels, entiers relatifs, rationnels, réels, complexes.

$\mathbf{R}' : \mathbf{R} \cup \{+\infty\}$, $\mathbf{R}'' : \mathbf{R}' \cup \{-\infty\}$

$\mathbf{Z}_p$: anneau des entiers p-adiques 1.2

$\mathbf{Q}_p$: corps des nombres p-adiques 1.5

$\mathrm{dg}\, P$: le degré du polynôme P 1.7

$v_{\mathfrak{P}}(x)$, $|x|_{\mathfrak{P}}$: la valuation et la valeur absolue $\mathfrak{P}$-adiques ($\mathfrak{P}$ idéal de K) 1.8

$v(K^*)$: groupe de valuation du corps K 2.1

$B(a, r)$, $B'(a, r)$: les boules ouverte et fermée de centre a et de rayon r 2.2

$\tilde{K}$: la clôture algébrique de K 2.6

$\mathbf{C}_p$: le complété de la clôture algébrique de $\mathbf{Q}_p$ 2.7

$C(X, K)$, $B(X, K)$ et $C_0(X, K)$: des espaces de fonctions continues, bornées... sur X 3.1

$b_K(I)$, $c_K(I)$: espaces des familles indexées dans I, à valeurs dans K, bornées ou tendant vers zéro à l'infini..... 3.1

E_0, E'_0, $\overline{E}$: boule unité fermée, ouverte, quotient E_0/E'_0, relatifs à E 3.1

$\binom{X}{n} = X(X-1)\ldots(X-n+1)/n!$: le n-ième polynôme binomial 3.2

$\hat{\bigoplus} E_i$: la somme directe complétée des espaces de Banach E_i 3.2

$E \hat{\otimes} F$: le produit tensoriel complété de E et F..... 3.3

B_m : une algèbre de séries de Laurent 3.5

$D(a, r)$, $D'(a, r)$: les disques ouvert et fermé de centre a, de rayon r 4.1

$A(B)$: l'algèbre des fonctions strictement analytiques sur la boule B 4.1

$R(D)$: l'anneau des fractions rationnelles sans pôle dans D 4.1

$H(D)$, $H_0(D)$: l'espace des éléments analytiques sur D, le sous-espace de ceux qui tendent vers zéro à l'infini.... 4.1

$|\cdot|_D$: la norme de la convergence uniforme sur D..... 4.1

Conv (f) : l'intervalle de convergence de la série de Laurent f 4.2

$L_K(I)$: l'anneau des séries de Laurent f telles que Conv $(f) \supseteq I$ 4.2

Introduction

Les nombres p - adiques ont été introduits par K. Hensel [5][1], à propos de problèmes de théorie des nombres. La théorie des corps p - adiques et l'analyse p - adique fournissent à l'arithmétique un instrument très utile. Nous avons souhaité montrer ce que sont les nombres p - adiques, et comment ils permettent d'obtenir des résultats « rationnels ».

Nous avons choisi, comme exemple d'application de l'analyse p - adique, le critère de rationalité de Borel-Dwork et celui de Polya-F. Bertrandias (qui en est une généralisation). Ces résultats utilisent la théorie des fonctions analytiques p - adiques. Or les fonctions analytiques p - adiques jouissent de bonnes propriétés si le corps de base est assez gros : essentiellement s'il est complet et algébriquement clos.

Le lecteur n'a besoin d'aucune connaissance « p - adique » préalable : les notions de topologie et d'algèbre contenues dans les cours de premier cycle des universités et un peu de topologie générale du niveau du second cycle couvrent les connaissances supposées acquises. Quelques propriétés arithmétiques des corps de nombres sont rappelées sans démonstration à la fin du chapitre 1 : on en trouvera un exposé détaillé par exemple dans le livre de P. Samuel [7]. Une certaine familiarité avec la théorie élémentaire des fonctions d'une variable complexe peut faciliter la compréhension de l'étude des fonctions analytiques.

1. Les chiffres entre crochets renvoient à la Bibliographie, *infra*, p. 187 et suiv.

On construit au premier chapitre le corps $\mathbf{Q}_p$ des nombres p - adiques. Le chapitre 2, consacré aux complétions et extensions algébriques des corps valués, est essentiellement destiné à la construction du corps $\mathbf{C}_p$, complété de la clôture algébrique de $\mathbf{Q}_p$, qui joue en analyse p - adique le rôle que $\mathbf{C}$ joue en analyse classique.

Les espaces de fonctions analytiques ayant le plus souvent une structure naturelle d'espace de Banach, le chapitre 3 contient les propriétés élémentaires de ces espaces et quelques notions sur les algèbres de Banach. Le chapitre 4, outre les propriétés classiques des fonctions analytiques sur les disques et couronnes, présente une ébauche de théorie du prolongement analytique, volontairement limitée à ce qui est nécessaire pour atteindre les critères de rationalité visés. Enfin le chapitre 5, consacré aux deux critères de rationalité annoncés, comporte de brefs exposés sur les déterminants de Hankel et Kronecker d'une part, et sur le diamètre transfini d'autre part, ainsi que sur les lemniscates du plan complexe, ces notions étant nécessaires à la compréhension ou la preuve des théorèmes de rationalité.

Plusieurs collègues ont pris la peine de me signaler des erreurs relevées à la lecture du manuscrit, je les en remercie.

CHAPITRE 1

Construction des nombres p-adiques

1.1. SUITES DE CONGRUENCES

Soient p un nombre premier et a un entier, cherchons à résoudre la suite de congruences (C_n) :

$$x^2 \equiv a \bmod. p^n, \quad \text{pour} \quad n \geqslant 1.$$

Examinons par exemple le cas particulier $a = -1$, $p = 5$. La première congruence, $x^2 \equiv -1 \bmod. 5$, a pour solutions $x \equiv 2$ et $x \equiv -2 \bmod. 5$.

Il est clair que l'ensemble des solutions de (C_n) est réunion d'une famille de classes modulo p^n, et aussi que toute solution de (C_n) est encore solution des (C_k) pour $k \leqslant n$. Ainsi dans l'exemple précédent les solutions de (C_2) constituent des classes modulo 5^2, contenues dans la réunion des classes de 2 et -2 modulo 5. Cherchons par exemple les solutions de (C_2) contenues dans $2 + 5\mathbf{Z}$: en posant $x = 2 + 5x_1$, (C_2) devient :

$$1 + 4x_1 \equiv 0 \bmod. 5, \quad \text{soit} \quad x_1 \equiv 1 \bmod. 5.$$

Plus généralement, supposons que nous ayons construit deux suites de classes $\alpha_1, \alpha_2, \ldots, \alpha_n$ et $\beta_1, \beta_2, \ldots, \beta_n$ telles que α_i et β_i soient des classes modulo 5^i dont la réunion est l'ensemble des solutions de (C_i), pour $i = 1, \ldots, n$,

$\alpha_{i+1} \subset \alpha_i$ et $\beta_{i+1} \subset \beta_i$ pour $i = 1, \ldots, n-1$. Alors les solutions de (C_{n+1}) appartiennent à $\alpha_n \cup \beta_n$. Soit $x_n \in \alpha_n$ (resp. $y_n \in \beta_n$), toute solution de (C_{n+1}) est de la forme $x_{n+1} = x_n + Xp^n$ ou $y_{n+1} = y_n + Yp^n$. Pour que, par exemple, x_{n+1} soit solution de (C_{n+1}) il faut et il suffit que X satisfasse :

$$x_n^2 + 2x_n X 5^n + X^2 5^{2n} \equiv -1 \text{ mod. } 5^{n+1}.$$

Or, par hypothèse, x_n est solution de (C_n), donc $x_n^2 = -1 + 5^n X'$ où $X' \in \mathbf{Z}$; la congruence en X s'écrit donc :

$$2x_n X + X' \equiv 0 \text{ mod. } 5.$$

Nous savons que $x_n \in \alpha_n \subset \alpha_1$, donc $2x_n \equiv \pm 4$ mod. 5, et la congruence ci-dessus a une unique solution X. Nous avons donc montré qu'il existe une unique classe α_{n+1} modulo 5^{n+1} qui soit contenue dans α_n et dont les éléments soient solution de (C_{n+1}).

On voit ainsi qu'il existe deux suites α_n et β_n telles que :

— α_n et β_n sont des classes modulo 5^n;
— $\alpha_{n+1} \subset \alpha_n$ et $\beta_{n+1} \subset \beta_n$;
— $\alpha_n \cup \beta_n$ est l'ensemble des solutions de (C_n).

Si l'on convient de représenter α_n (resp. β_n) par le plus petit entier positif a_n (resp. b_n) lui appartenant, on voit que les suites d'entiers ainsi obtenues sont telles que $5^n \mid a_{n+1} - a_n$ (resp. $5^n \mid b_{n+1} - b_n$), donc

$$a_{n+1} = a_n + x_n 5^n, \qquad b_{n+1} = b_n + y_n 5^n,$$

où x_n et y_n sont des entiers positifs strictement inférieurs à 5, c'est-à-dire des chiffres en numération à base 5. Il existe donc deux suites de chiffres $x_0, x_1, \ldots, x_n, \ldots$; $y_0, y_1, \ldots, y_n, \ldots$, tels que :

$$a_n = x_0 + 5x_1 + \ldots + 5^{n-1}x_{n-1}$$

et :

$$b_n = y_0 + 5y_1 + \ldots + 5^{n-1}y_{n-1}$$

représentent les solutions des congruences (C_n) en ce sens que x est solution de (C_n) si et seulement si x appartient à l'une des deux classes modulo 5^n définies par a_n et b_n. On peut alors convenir de représenter formellement les deux familles de solutions de la suite des congruences (C_n) par les deux séries (formelles) $\sum_{n \geqslant 0} x_n 5^n$ et $\sum_{n \geqslant 0} y_n 5^n$. Les sommes partielles de ces séries fournissent les suites de solutions des (C_n).

L'introduction des nombres p - adiques permet de rendre systématique l'utilisation de suites de classes emboîtées analogues aux α_n ci-dessus, de façon que la série formellement introduite pour les représenter, qui est divergente au sens habituel, devienne convergente et ait pour somme un nouvel objet, qui est un nombre 5 - adique. Ce nombre est alors solution de *l'équation* $x^2 + 1 = 0$, et non plus d'une suite de congruences.

Exercice 1.1. — Soient p un nombre premier et P(X) un polynôme à coefficients entiers. On suppose qu'il existe un entier x_0 tel que :

$$P(x_0) \equiv 0 \text{ mod. } p \quad \text{et} \quad P'(x_0) \not\equiv 0 \text{ mod. } p.$$

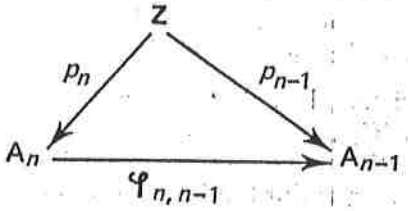
Montrer qu'il existe une suite α_n de classes modulo p^n telle que $x_0 \in \alpha_1$, $\alpha_{n+1} \subset \alpha_n$ et que l'ensemble des solutions de la congruence $P(x) \equiv 0$ mod. p^n appartenant à $x_0 + p\mathbf{Z}$ soit la classe α_n. En déduire quels sont les couples (a, p) pour lesquels la suite des congruences $x^2 \equiv a$ mod. p^n admet deux suites de solutions distinctes modulo p.

1.2. Les entiers p - adiques

Soit p un nombre premier fixé. Pour $n \geqslant 1$, nous noterons $A_n = \mathbf{Z}/p^n\mathbf{Z}$ et p_n la projection canonique de Z sur A_n. On sait que A_n a une structure naturelle d'anneau pour laquelle p_n est un homomorphisme d'anneaux. Nous noterons $\varphi_{n,n-1}$ l'homomorphisme naturel de A_n dans A_{n-1} : si l'on considère les éléments de A_n comme des parties de Z, $\varphi_{n,n-1}$ est aussi définie par l'inclusion en ce sens

que $\varphi_{n,n-1}(\alpha_n)$ est la classe modulo p^{n-1} contenant α_n. Alors le diagramme ci-dessous est commutatif : pour $x \in \mathbf{Z}$:

$$\varphi_{n,n-1}(p_n(x)) = p_{n-1}(x).$$



Soit maintenant $\mathscr{A} = \prod_{n \geqslant 1} A_n$, muni de sa structure d'anneau produit, et soit π_n la projection canonique de $\mathscr{A}$ sur A_n. Chacun des A_n, muni de la topologie discrète, est un anneau topologique compact : on munit $\mathscr{A}$ de la topologie produit, ce qui en fait un anneau topologique compact.

Soit i l'application de $\mathbf{Z}$ dans $\mathscr{A}$ définie par :

$$i(z) = (p_n(z))_{n \geqslant 1}$$

c'est visiblement un morphisme d'anneaux. C'est de plus une injection car :

$$i(z) = 0 \Leftrightarrow p_n(z) = 0 \quad \text{pour} \quad n \geqslant 1$$
$$\Leftrightarrow z \in p^n\mathbf{Z} \quad \text{pour} \quad n \geqslant 1 \Leftrightarrow z = 0.$$

Donc l'image $i(\mathbf{Z})$ est un sous-anneau de $\mathscr{A}$ isomorphe à $\mathbf{Z}$. De plus, pour $n \geqslant 2$ et $a \in i(\mathbf{Z})$:

$$\varphi_{n,n-1}(\pi_n(a)) = \pi_{n-1}(a). \qquad (1_n)$$

PROPOSITION 1.2.1. — *L'ensemble $\mathbf{Z}_p$ des éléments de $\mathscr{A} = \prod_{n \geqslant 1} \mathbf{Z}/p^n\mathbf{Z}$ qui satisfont les relations (1_n) pour $n \geqslant 2$ est un sous-anneau topologique compact de $\mathscr{A}$, contenant l'image $i(\mathbf{Z})$ de $\mathbf{Z}$.*

En effet, pour chaque indice $n \geqslant 2$, l'ensemble P_n des éléments de $\mathscr{A}$ qui satisfont la relation (1_n) est un sous-anneau compact de $\mathscr{A}$, car les applications $\varphi_{n,n-1}$, π_n et π_{n-1} sont continues et sont des morphismes d'anneaux. L'intersection $\mathbf{Z}_p$ des P_n est donc aussi un sous-anneau compact de $\mathscr{A}$. Enfin nous avons déjà remarqué que, pour $n \geqslant 2$, $i(\mathbf{Z}) \subseteq P_n$.

DÉFINITION 1.2.2. — *L'anneau topologique $\mathbf{Z}_p$ est appelé anneau des entiers p - adiques.*

Nous identifierons le plus souvent $\mathbf{Z}$ et son image dans $\mathbf{Z}_p$ par l'isomorphisme i.

Soit $a = (a_n)_{n \geqslant 1}$ un point de $\mathscr{A}$, on sait que lorsque K parcourt l'ensemble des parties finies de N, la famille :

$$W_K(a) = \bigcap_{n \in K} \pi_n^{-1}(a_n)$$

parcourt une base de voisinages de a dans $\mathscr{A}$. Supposons maintenant que $a \in \mathbf{Z}_p$ et soit $k = \operatorname{Sup}_{n \in K} n$, alors, pour $n \leqslant k$, $\pi_n^{-1}(a_n) \cap \mathbf{Z}_p \supseteq \pi_k^{-1}(a_k) \cap \mathbf{Z}_p$, donc :

$$W_K(a) \cap \mathbf{Z}_p = \pi_k^{-1}(a_k) \cap \mathbf{Z}_p = \{x \in \mathbf{Z}_p \mid \pi_k(x) = \pi_k(a)\}.$$

On voit ainsi que, pour $a \in \mathbf{Z}_p$, la suite :

$$V_k(a) = \{x \in \mathbf{Z}_p \mid \pi_k(x) = \pi_k(a)\}, \quad k \geqslant 1,$$

constitue une base de voisinages de a dans $\mathbf{Z}_p$.

PROPOSITION 1.2.3. — *$\mathbf{Z}$ est dense dans $\mathbf{Z}_p$.*

Soient en effet $a \in \mathbf{Z}_p$ et $k \geqslant 1$: il existe un entier $b \in \mathbf{Z}$ tel que $p_k(b) = \pi_k(a)$. Pour un tel b, $i(b) \in V_k(a)$, d'où la proposition.

EXEMPLE. — Reprenons l'exemple étudié en 1, de la suite de congruences $x^2 \equiv -1 \bmod. 5^n$. Les suites de classes de solutions α_n et β_n définissent deux entiers p - adiques a et b. On a, pour $n \geqslant 1$:

$$\pi_n(a^2) = \pi_n(b^2) = -1.$$

Donc, pour $n \geqslant 1$, $a^2 + 1 \in V_n(0)$ et $b^2 + 1 \in V_n(0)$. Comme $\mathbf{Z}_5$ est séparé, il en résulte que :

$$a^2 + 1 = b^2 + 1 = 0.$$

De plus $a \neq b$ car $\pi_1(a) \neq \pi_1(b)$, a et b sont donc les deux solutions dans $\mathbf{Z}_5$ de l'équation $x^2 + 1 = 0$. On vérifiera de même que la suite de classes de solutions des congruences $P(X) \equiv 0 \bmod. p^n$ étudiées à l'exercice 1.1 définit une solution dans $\mathbf{Z}_p$ de l'équation $P(X) = 0$.

1.3. DÉVELOPPEMENT DE HENSEL DES ENTIERS P - ADIQUES

Convenons de représenter les éléments de $A_n = \mathbf{Z}/p^n\mathbf{Z}$ par les entiers compris entre 0 et $p^n - 1$: alors chaque entier p - adique $x = (x_n)_{n \geqslant 1}$ peut être représenté par une suite d'entiers $(a_n)_{n \geqslant 1}$ définis par :

$0 \leqslant a_n < p^n$

$a_n \in x_n$ (ou, ce qui est équivalent, $\pi_n(i(a_n)) = x_n = \pi_n(x)$).

Comme $x \in \mathbf{Z}_p$, on a pour $n \geqslant 1$: $p^n \mid a_{n+1} - a_n$. Il existe donc une suite $b_0, \ldots, b_n, \ldots$ de chiffres modulo p $(0 \leqslant b_n < p)$ tels que :

$$a_n = b_0 + b_1 p + \ldots + b_{n-1} p^{n-1}.$$

Or, par définition, $i(a_n) \in V_n(x)$, donc la suite $i(a_n)$ converge vers x dans $\mathbf{Z}_p$. En d'autres termes la série $\sum_{n \geqslant 0} b_n p^n$ est convergente dans $\mathbf{Z}_p$ et a pour somme x.

PROPOSITION 1.3.1. — *Soit $x \in \mathbf{Z}_p$, il existe une unique suite $(b_n)_{n \geqslant 0}$, $0 \leqslant b_n < p$, telle que la série $\sum_{n \geqslant 0} b_n p^n$ converge vers x. Cette série est appelée* DÉVELOPPEMENT DE HENSEL *de x.*

Nous avons prouvé ci-dessus l'existence d'un développement du type indiqué. L'unicité se déduira du lemme suivant.

LEMME 1.3.2. — *Soit $(b_n)_{n \geqslant 0}$ une suite d'entiers p - adiques, la série $\sum_{n \geqslant 0} b_n p^n$ converge dans $\mathbf{Z}_p$, soit x sa somme. Supposons de plus que $b_n = 0$ pour $n < n_0$ et $\pi_1(b_{n_0}) \neq 0$, alors $\pi_{n_0}(x) \neq 0$ et $\pi_n(x) = 0$ pour $n < n_0$.*

Soient en effet :

$$S_n = b_0 + \ldots + b_{n-1} p^{n-1} \quad \text{et} \quad x_n = \pi_n(S_n)$$

on vérifie immédiatement que $x = (x_n)_{n \geqslant 1}$ est dans $\mathbf{Z}_p$. De plus, pour $k \geqslant n$, $S_k \in V_n(x)$: donc la suite S_k converge vers x. Si de plus $b_n = 0$ pour $n < n_0$, $\pi_n(S_k) = 0$ pour $n < n_0$ et pour tout k. Or, $\pi_n^{-1}(0) = V_n(0)$ est fermé, donc $x \in V_n(0)$ et, pour $n < n_0$, $\pi_n(x) = 0$. Enfin, pour tout $k \geqslant n_0$:

$$\pi_{n_0}(S_k) = \pi_{n_0}(S_{n_0}) \neq 0$$

comme $\pi_{n_0}^{-1}(\pi_{n_0}(S_{n_0}))$ est fermé, on a encore $\pi_{n_0}(x) \neq 0$, d'où le lemme.

Supposons maintenant que $x \in \mathbf{Z}_p$ admette deux développements distincts :

$$x = \sum_{n \geqslant 0} b_n p^n = \sum_{n \geqslant 0} c_n p^n \quad \text{avec} \quad 0 \leqslant b_n < p \quad \text{et} \quad 0 \leqslant c_n < p.$$

Soit $n_0 = \operatorname{Inf}\{n \mid b_n \neq c_n\}$ et soit $y = \sum_{n \geqslant 0} (b_n - c_n) p^n$, d'après le lemme, $\pi_{n_0}(y) \neq 0$; d'autre part $y = 0$, ce qui est impossible, d'où la proposition.

Remarquons que le développement de Hensel généralise aux entiers p - adiques le développement en numération à base p des entiers positifs. Plus précisément, soient $N \geqslant 0$ et $N = n_0 + n_1 p + \ldots + n_h p^h$ sa représentation en numération à base p. Posons $a_i = n_i$ pour $i \leqslant h$ et $a_i = 0$ pour $i > h$, alors $i(N) = \sum_{n \geqslant 0} a_n p^n$, et les conditions $0 \leqslant a_n < p$ assurent que cette série est le développement de Hensel de N dans $\mathbf{Z}_p$. Il faut noter par contre que pour un entier négatif, disons $-N$, le développement de Hensel a une infinité de termes non nuls; par exemple $-1 = (p-1) + \ldots + (p-1)p^n + \ldots$

On voit que la série introduite formellement à l'exemple 1.1 pour représenter les suites de solutions des suites de congruences étudiées n'était autre que le développement de Hensel dans $\mathbf{Z}_5$ des solutions de l'équation $x^2 + 1 = 0$.

1.4. LA VALUATION DE $\mathbf{Z}_p$

Soient $a \in \mathbf{Z}_p$, $a \neq 0$, et $a = \sum_{n \geqslant 0} a_n p^n$ son développement de Hensel. Les chiffres a_n ne sont pas tous nuls : on associe à a l'entier positif $v(a)$ défini par :

$$v(a) = \mathrm{Inf}\{n \mid a_n \neq 0\} \tag{4}$$

Il est immédiat que cette définition équivaut à :

$$v(a) = \mathrm{Inf}\{n \mid \pi_{n+1}(a) \neq 0\} = \mathrm{Sup}\{n \mid \pi_n(a) = 0\} \quad (4\ bis)$$

On convient de plus de poser $v(0) = +\infty$: ceci définit sur $\mathbf{Z}_p$ une fonction à valeurs dans $\mathbf{N} \cup \{+\infty\}$. Par définition on convient que, pour tout $n \in \mathbf{N}$, $n < +\infty$, $n + (+\infty) = +\infty$, $(+\infty) + (+\infty) = +\infty$, ce qui fait de $\mathbf{N} \cup (+\infty)$ un monoïde totalement ordonné.

DÉFINITION 1.4.1. — *La fonction v définie ci-dessus s'appelle la* VALUATION P - ADIQUE.

On vérifiera que la restriction de v à $\mathbf{Z}$ est aussi définie, pour $a \neq 0$, par $v(a) = \mathrm{Sup}\{n \mid p^n \mid a\}$ (où l'on convient que $p^0 = 1$, $1 \mid a$ pour $a \neq 0$).

PROPOSITION 1.4.2. — *La valuation* p - *adique possède les propriétés suivantes :*

V1 : *pour tout* $x \in \mathbf{Z}_p$, $v(x) = +\infty \Leftrightarrow x = 0$;

V2 : *pour tous* x *et* $y \in \mathbf{Z}_p$, $v(xy) = v(x) + v(y)$;

V3 : *pour tous* x *et* $y \in \mathbf{Z}_p$, $v(x+y) \geqslant \mathrm{Inf}\,(v(x), v(y))$.

La propriété V1 est évidente, de plus V2 et V3 sont visiblement satisfaites si x ou y est nul. Supposons donc $x \neq 0$ et $y \neq 0$. Remarquons d'abord que :

$$v(x) \geqslant n \Leftrightarrow x \in \pi_n^{-1}(0),$$

et que $\pi_n^{-1}(0)$ est un sous-groupe (et même un idéal) de $\mathbf{Z}_p$. La propriété V3 en résulte aussitôt : soit

$$k = \mathrm{Inf}\,(v(x), v(y)),$$

alors $v(x) \geqslant k$ et $v(y) \geqslant k$, donc $x \in \pi_k^{-1}(0)$ et $y \in \pi_k^{-1}(0)$, donc aussi $x + y \in \pi_k^{-1}(0)$ et $v(x+y) \geqslant k$.

Pour prouver V2, remarquons d'abord que $v(x) = 0$ et $v(y) = 0 \Rightarrow v(xy) = 0$. En effet, $v(x) = 0 \Leftrightarrow \pi_1(x) \neq 0$, or $A_1 = \mathbf{Z}/p\mathbf{Z}$ est intègre, donc $\pi_1(x) \neq 0$ et $\pi_1(y) \neq 0$ entraînent $\pi_1(xy) \neq 0$, soit $v(xy) = 0$. Remarquons d'autre part que si $x = \sum_{n \geqslant 0} x_n p^n$ et $v(x) = h$, alors $x = \sum_{n \geqslant h} x_n p^n$, et si on pose $x' = \sum_{n \geqslant 0} x_{n+h} p^n$, on a $x = p^h x'$ et $v(x') = 0$. Soient de même $k = v(y)$ et $y = p^k y'$ avec $v(y') = 0$, alors $xy = p^{h+k} x' y'$ avec $v(x'y') = 0$. Il reste donc à montrer que si $x = p^h x'$ et $v(x') = 0$ alors $v(x) = h$. Or $x' = x'_0 + \ldots + x'_n p^n + \ldots$ avec $x'_0 \neq 0$, $v(x') = 0$ et $v(x) = v(p^h) + v(x')$, donc $v(x) = h$.

COROLLAIRE 1.4.3. — *Soient x et y dans $\mathbf{Z}_p$, si :*

$$v(x) \neq v(y), \qquad v(x+y) = \mathrm{Inf}\,(v(x), v(y)).$$

Supposons par exemple que $k = v(x) < v(y)$, alors $\pi_k(x) \neq 0$ et $\pi_k(y) = 0$, donc :

$$\pi_k(x+y) = \pi_k(x) + \pi_k(y) = \pi_k(x) \neq 0$$

et : $\quad v(x+y) \leqslant k, \quad$ d'où $\quad v(x+y) = k.$

COROLLAIRE 1.4.4. — *L'anneau $\mathbf{Z}_p$ est intègre.*

En effet, si x et y sont non nuls :

$$v(xy) = v(x) + v(y) \neq +\infty, \qquad \text{donc} \qquad xy \neq 0.$$

Nous avons déjà remarqué que $\pi_n^{-1}(0) = V_n(0)$ est un idéal : nous allons maintenant décrire les relations de divisibilité dans $\mathbf{Z}_p$, et les idéaux de $\mathbf{Z}_p$.

PROPOSITION 1.4.5. — *Soit $a \in \mathbf{Z}_p$, les conditions suivantes sont équivalentes :*

(i) *a est une unité, c'est-à-dire un élément inversible, de $\mathbf{Z}_p$;*

(ii) $\pi_1(a) \neq 0$ *(dans $\mathbf{Z}/p\mathbf{Z}$)*;

(iii) $v(a) = 0$.

Nous avons déjà remarqué l'équivalence des conditions (ii) et (iii). Supposons a inversible dans $\mathbf{Z}_p$, alors pour tout n, $\pi_n(a)$ est inversible dans A_n, et en particulier $\pi_1(a) \neq 0$. Réciproquement, supposons que :

$$a_1 = \pi_1(a) \neq 0,$$

alors pour tout n, $a_n = \pi_n(a)$ est inversible dans A_n, on vérifie aisément que la suite des inverses définit un entier p - adique b tel que $\pi_n(ab) = 1$ pour tout n, donc $ab = 1$.

COROLLAIRE 1.4.6. — *L'ensemble* M *des éléments* x *de* $\mathbf{Z}_p$ *tels que* $v(x) > 0$ *est un idéal maximal de* $\mathbf{Z}_p$, *c'est aussi l'ensemble des éléments non inversibles de* $\mathbf{Z}_p$, *c'est l'unique idéal maximal de* $\mathbf{Z}_p$, *il est principal, ses générateurs sont les éléments* p' *tels que* $v(p') = 1$.

D'abord M est, par définition de v, l'idéal $\pi_1^{-1}(0)$. L'équivalence des propriétés (i) et (ii) dans la proposition 1.4.5 prouve que c'est aussi l'ensemble des éléments non inversibles de $\mathbf{Z}_p$. Soit N un idéal de A : N ne peut contenir aucun élément inversible, donc $N \subseteq M$, ce qui montre que M est maximal et est le seul idéal maximal. Soit $x \in M$, $x = \sum_{n \geqslant 1} x_n p^n$ et soit $x' = \sum_{n \geqslant 1} x_n p^{n-1}$, alors $x = px'$, donc $M \subseteq pZ_p$, or $p \in M$, d'où $M = pZ_p$. M est donc principal, ses générateurs sont les éléments $p' = up$ où u est une unité, donc aussi les éléments de valuation $v(p') = 1$.

COROLLAIRE 1.4.7. — *L'anneau* $\mathbf{Z}_p$ *est principal, ses idéaux sont les puissances* M^n *de* M. *Pour que* x *divise* y *dans* $\mathbf{Z}_p$ *il faut et il suffit que* $v(x) \geqslant v(y)$.

Prouvons d'abord la seconde assertion : si $x = yz$, $v(x) = v(y) + v(z) \geqslant v(y)$. Réciproquement, si :

$$v(x) \geqslant v(y) = h,$$

soient $x = \sum_{n \geqslant h} x_n p^n$ et $y = \sum_{n \geqslant h} y_n p^n$, $y_h \neq 0$, les développements de Hensel de x et y. On sait que $y' = \sum_{n \geqslant h} y_n p^{n-h}$ est inversible, soit z son inverse et soit $x' = \sum_{n \geqslant h} x_n p^{n-h}$, on a $x = p^h x' = p^h y' zx' = y(zx')$, donc x divise y. En particulier x et y sont associés (c'est-à-dire engendrent le même idéal) si et seulement si $v(x) = v(y)$.

Soit maintenant N un idéal propre de $\mathbf{Z}_p$:

$$k = \mathrm{Inf}\{v(x) \mid x \in N\}.$$

Alors $N \subseteq M$ et $k \geqslant 1$, soit $n \in N$ tel que $v(n) = k$, p^k et n sont associés, donc $p^k \mathbf{Z}_p = M^k = n\mathbf{Z}_p \subseteq N$. Si $x \in N$, $v(x) \geqslant k$, donc x divise p^k et $x \in p^k \mathbf{Z}_p$: ainsi $N = M^k = p^k \mathbf{Z}_p$.

Rappelons aussi que :

$$p^k \mathbf{Z}_p = \{x \mid v(x) \geqslant k\} = \pi_k^{-1}(0) = V_k(0).$$

On voit que la famille des idéaux de $\mathbf{Z}_p$ est aussi la famille des noyaux des projections π_k, ou encore la base canonique de voisinages de 0 dans $\mathbf{Z}_p$.

DÉFINITION 1.4.8. — *On dit qu'un anneau commutatif principal* A *est un* ANNEAU DE VALUATION DISCRÈTE *si l'ensemble des éléments non inversibles de* A *constitue un idéal* M. *On appelle* M L'IDÉAL DE VALUATION.

Il est clair que si l'ensemble des éléments non inversibles d'un anneau A est un idéal M, celui-ci est maximal et est l'unique idéal maximal : tout idéal propre N de A, puisqu'il ne contient aucun élément inversible, est contenu dans M.

Soient $I = \bigcap_{n \geqslant 1} M^n$, x un générateur de I et m un générateur de M. Pour $n \geqslant 1$ il existe a_n tel que $x = a_n m^n$, si $x \neq 0$ la suite des idéaux $a_n A$ est strictement croissante, non stationnaire, ce qui est impossible puisque A est principal, donc $x = 0$ et $I = \{0\}$. Donc, si $x \in A$, $x \neq 0$, $v(x) = \mathrm{Sup}\{n \mid x \in M^n\}$ existe.

PROPOSITION 1.4.9. — *Soient* A *un anneau de valuation discrète,* M *son idéal de valuation et* v *la fonction définie sur* A

par : $v(x) = \mathrm{Sup}\{n \mid x \in \mathrm{M}^n\}$ *si* $x \neq 0$ *et* $v(0) = +\infty$, *alors* :

(i) *la fonction v est une valuation, c'est-à-dire qu'elle satisfait les propriétés* V1, V2, V3 *définies en* 1.4.2.
(ii) *tout idéal propre de* A *est de la forme* M^n, $n \geqslant 1$.

La démonstration de cette proposition, tout à fait analogue à celles faites ci-dessus dans le cas particulier de l'anneau $\mathbf{Z}_p$, est laissée aux soins du lecteur.

EXEMPLES. — 1. Soit $\mathrm{A} = \mathrm{K}[[\mathrm{X}]]$ l'anneau des séries formelles en une indéterminée, à coefficients dans le corps K. Les éléments non inversibles de A sont les séries $f = \sum_{n \geqslant 0} a_n \mathrm{X}^n$ dont le terme constant a_0 est nul. Ils constituent l'idéal $\mathrm{M} = \mathrm{XA}$. L'anneau A est un anneau de valuation discrète et la valuation d'un élément f non nul est :

$$v(f) = \mathrm{Inf}\{n \mid a_n \neq 0\} = \mathrm{Sup}\{n \mid a_i = 0 \text{ pour } i < n\}.$$

2. Soient a un point du plan complexe $\mathbf{C}$ et A l'anneau des fonctions définies dans au moins un disque ouvert centré en a et holomorphes dans ce disque. Les éléments non inversibles de A sont les fonctions nulles au point a. Elles constituent un idéal principal engendré par $z - a$, A est un anneau de valuation discrète, la valuation d'un élément f de A est l'ordre de a en tant que zéro de f.

3. Un anneau nœthérien A dans lequel les éléments non inversibles constituent un idéal principal est un anneau de valuation discrète.

4. Soient p un nombre premier, A_p le sous-anneau de $\mathbf{Q}$ constitué des rationnels p-entiers, c'est-à-dire des rationnels a/b où $(b, p) = 1$. Les éléments non inversibles de A_p sont les a/b tels que $(b, p) = 1$ et $p \mid a$: c'est l'idéal $p\mathrm{A}_p$. Tout nombre a/b de A_p s'écrit $a/b = p^h a'/b$, où $(a', p) = (b, p) = 1$, alors $v(a/b) = h$. L'isomorphisme canonique i de $\mathbf{Z}$ dans $\mathbf{Z}_p$ se prolonge de façon unique en un homomorphisme d'anneaux de A_p dans $\mathbf{Z}_p$:

soit encore i ce prolongement, et $b \in \mathbf{Z}$, $(b, p) = 1$, alors $i(b)$ est inversible dans $\mathbf{Z}_p$ et nécessairement :

$$i(a/b) = i(a)\,(i(b))^{-1}.$$

On vérifie que i, ainsi prolongé à A_p, est encore un isomorphisme et que l'image par i de la valuation de A n'est autre que la restriction à $i(\mathrm{A}_p)$ de la valuation p-adique sur $\mathbf{Z}_p$.

5. Soient K un corps de nombres algébriques, B l'anneau des entiers de K, $\mathfrak{P}$ un idéal premier de B. On note $\mathrm{B}_{\mathfrak{P}}$ le localisé de B par rapport à $\mathfrak{P}$, c'est-à-dire le sous-anneau de K constitué des éléments $x = a/b$ où $a \in \mathrm{B}$ et $b \in \mathrm{B} - \mathfrak{P}$. Les éléments non inversibles de l'anneau $\mathrm{A} = \mathrm{B}_{\mathfrak{P}}$ sont les a/b tels que $b \in \mathrm{B} - \mathfrak{P}$ et $a \in \mathfrak{P}$. Ils constituent un idéal, qui est l'idéal $\mathfrak{P}\mathrm{A}$ engendré par $\mathfrak{P}$ dans A. On montre aisément que, B étant nœthérien, $\bigcap_{n \geqslant 1} \mathfrak{P}^n = 0$. On en déduit que $\bigcap_{n \geqslant 1} (\mathfrak{P}\mathrm{A})^n = 0$ et que A est un anneau de valuation discrète (cf. *infra*, 1.8).

1.5. LE CORPS $\mathbf{Q}_p$ DES NOMBRES P-ADIQUES

Nous avons montré que l'anneau $\mathbf{Z}_p$ est intègre.

DÉFINITION 1.5.1. — *Le corps des fractions de* $\mathbf{Z}_p$, *noté* $\mathbf{Q}_p$, *est appelé* CORPS DES NOMBRES P-ADIQUES.

Les propriétés ci-dessous de $\mathbf{Q}_p$ se déduisent aisément des propriétés déjà prouvées de $\mathbf{Z}_p$.

1.5.2. *Tout* $x \in \mathbf{Q}_p^*$ *admet une unique représentation* $x = p^n u$, *où* $n \in \mathbf{Z}$ *et* u *est une unité de* $\mathbf{Z}_p$.

En effet si $x = a/b$ où a et $b \in \mathbf{Z}_p$, on sait que $a = p^h a'$ et $b = p^k b'$ où a' et b' sont des unités de $\mathbf{Z}_p$, donc $x = p^{n-k} a'/b'$. Si $p^n u = p^m v$ où u et v sont des unités de $\mathbf{Z}_p$, supposons par exemple que $n \geqslant m$, alors $p^{n-m} = vu^{-1}$ est une unité, et $n - m = v(p^{n-m}) = 0$, d'où $u = v$, ce qui prouve l'unicité.

1.5.3. — *La fonction v définie sur $\mathbf{Q}_p$ par $x = p^{v(x)}u$, u unité de $\mathbf{Z}_p$, pour $x \neq 0$ et $v(0) = +\infty$, est une valuation sur $\mathbf{Q}_p$, c'est-à-dire une application de $\mathbf{Q}_p$ dans $\mathbf{Z} \cup \{+\infty\}$ satisfaisant les propriétés* V1, V2 *et* V3.

Vérification immédiate.

1.5.4. *L'injection canonique de $\mathbf{Z}$ dans $\mathbf{Z}_p$ se prolonge de façon unique en un isomorphisme de $\mathbf{Q}$ sur un sous-corps de $\mathbf{Q}_p$.*

1.5.5. *Soient :*

$$a \in \mathbf{Q}_p, \quad n \in \mathbf{Z}, \quad V_n(a) = \{x \in \mathbf{Q}_p \mid v(x-a) \geqslant n\}.$$

La topologie pour laquelle $V_n(a)$ est une base de voisinages de a fait de $\mathbf{Q}_p$ un corps topologique localement compact. L'application $y \to p^{-n}(y-a)$ est un homéomorphisme de $V_n(a)$ sur $\mathbf{Z}_p = V_0(0)$.

1.5.6. *Tout $x \in \mathbf{Q}_p$ admet un unique développement de Hensel $x = \sum_{n \geqslant n_0} a_n p^n$ où $0 \leqslant a_n < p$ et $n_0 \in \mathbf{Z}$. Si $a_{n_0} \neq 0$, $n_0 = v(x)$.*

Résulte de 1.5.3 et des propriétés du développement de Hensel dans $\mathbf{Z}_p$.

1.5.7. *L'image canonique de $\mathbf{Q}$ dans $\mathbf{Q}_p$ est dense.*

Soient en effet $a \in \mathbf{Q}_p$, $a = \sum_{n \geqslant n_0} a_n p^n$ son développement de Hensel et soit $k \in \mathbf{Z}$: le voisinage $V_k(a)$ de a contient l'image du rationnel $\sum_{n_0 \leqslant n < k} a_n p^n$.

1.5.8. *Soient x un rationnel non nul, $v_p(x)$ l'exposant de p dans la décomposition de x en facteurs premiers : $v_p(x)$ est la valuation de l'image de x dans $\mathbf{Q}_p$.*

Exercice. — Soit $a = \sum_{n \geqslant n_0} a_n p^n$ le développement de Hensel du nombre p - adique a. On dit que ce développement est périodique s'il existe n_1 et k tels que, pour $n \geqslant n_1$, $a_{n+k} = a_n$.

1. Si le développement de a est périodique, a est rationnel.

2. Soit y un entier positif premier à p, il existe h tel que y divise $p^h - 1$.

3. En déduire que le développement de Hensel d'un nombre p - adique a est périodique si et seulement si a est rationnel.

1.6. L'ESPACE MÉTRIQUE $\mathbf{Q}_p$

Rappelons qu'une VALEUR ABSOLUE sur un corps K est une application $x \to |x|$ de K dans $\mathbf{R}^+$, qui satisfait :

VA1 : $|x| = 0 \Leftrightarrow x = 0$;

VA2 : $|xy| = |x|\,|y|$;

VA3 : $|x+y| \leqslant |x| + |y|$.

A une valeur absolue on associe la distance d définie par $d(x,y) = |x-y|$, cette distance munit K d'une structure de corps topologique.

PROPOSITION 1.6.1. — *La fonction définie sur $\mathbf{Q}_p$ par $|0| = 0$ et $|x| = p^{-v(x)}$ pour $x \neq 0$ est une valeur absolue, elle satisfait la relation :*

VA' 3 : $|x+y| \leqslant \mathrm{Max}\,(|x|, |y|)$.

La topologie définie sur $\mathbf{Q}_p$ par cette valeur absolue est la même que celle de 1.5.5.

Les propriétés VA1, VA2 et VA' 3 se déduisent immédiatement des propriétés V1, V2 et V3 satisfaites par la valuation v. Il est clair que V' 3 entraîne V3, on a donc bien une valeur absolue. Soit $a \in \mathbf{Q}_p$, la famille des boules :

$$V_n(a) = \{x \in \mathbf{Q}_p \mid |x-a| \leqslant p^{-n}\} = \{x \in \mathbf{Q}_p \mid v(x-a) \geqslant n\}$$

est une base de voisinages de a pour la topologie associée à la valeur absolue, et aussi pour la topologie définie précédemment.

On dit qu'une distance d qui satisfait l'inégalité $d(x,y) \leqslant \mathrm{Max}\,(d(x,z), d(y,z))$ est ULTRAMÉTRIQUE; on appelle cette inégalité inégalité ultramétrique.

Une valeur absolue sur un corps K qui satisfait la relation VA' 3 est aussi dite ultramétrique ou NON ARCHIMÉDIENNE.

LEMME 1.6.2. — *Soit* $x \to |x|$ *une valeur absolue non archimédienne, alors :*

$$|x| \neq |y| \Rightarrow |x+y| = \text{Max}\,(|x|, |y|).$$

On remarque d'abord que pour toute valeur absolue $|-1| = 1$: en effet $|-1|^2 = 1$ et $|-1| \geqslant 0$. Soient x et y tels que, par exemple, $|x| < |y|$, alors :

$|x+y| \leqslant \text{Max}\,(|x|, |y|)$ et $|y| \leqslant \text{Max}\,(|-x|, |x+y|)$

entraînent :

$$\text{Max}\,(|-x|, |x+y|) = |x+y| = |y|.$$

LEMME 1.6.3. — *Toute boule de l'espace métrique* $\mathbf{Q}_p$ *en est une partie à la fois ouverte et fermée.*

Notons $B(a, r)$ (resp. $B'(a, r)$) la boule ouverte (resp. fermée) de centre a et de rayon r. Si $x \in \mathbf{Q}_p$:

$$|x| \in \{p^n \mid n \in \mathbf{Z}\},$$

soient donc n et n' définis par :

$$p^n < r \leqslant p^{n+1} \quad \text{et} \quad p^{n'} \leqslant r < p^{n'+1},$$

alors : $B(a, r) = B(a, p^{n+1}) = B'(a, p^n)$

et : $B'(a, r) = B'(a, p^{n'}) = B(a, p^{n'+1})$,

d'où le lemme.

Remarquons d'ailleurs que :

$$B(a, p^{n+1}) = B'(a, p^n) = \pi_n^{-1}(\pi_n(a)),$$

pour : $a \in \mathbf{Z}_p$ et $n \geqslant 0$.

Or $\pi_n(a)$ et son complémentaire sont des fermés de A_n, ce qui donne une autre preuve du lemme, compte tenu du fait que deux boules sont homéomorphes.

COROLLAIRE 1.6.4. — *L'espace* $\mathbf{Q}_p$ *est totalement discontinu.*

Rappelons en effet qu'un espace topologique séparé est totalement discontinu si tout point possède une base de voisinages à la fois ouverts et fermés. Dans un tel espace la composante connexe d'un point est réduite à ce point : nous verrons que tout corps muni d'une valeur absolue non archimédienne a cette propriété.

EXERCICES 1.6. — 1. Soient G un groupe commutatif ordonné noté additivement, 0 son élément neutre, on dit que G est archimédien si, pour tout couple a, b tel que $b > 0$, il existe $n \in \mathbf{N}$ tel que $nb > a$. On dit de même qu'une valeur absolue est archimédienne si, pour tout couple a, b tel que $|b| > 1$, il existe $n \in \mathbf{N}$ tel que $|nb| > |a|$. Montrer que les valeurs absolues ultramétriques ne sont pas archimédiennes.

2. Dans un espace ultramétrique :

$$d(x,y) \neq d(y,z) \Rightarrow d(x,z) = \text{Max}\,(d(x,y), d(y,z)).$$

3. Dans un espace ultramétrique, $b \in B(a, r) \Rightarrow B(a, r) = B(b, r)$ (resp. $b \in B'(a, r) \Rightarrow B'(a, r) = B'(b, r)$), autrement dit : tout point d'une boule en est un centre.

4. Etant donné deux boules d'un espace ultramétrique, ou bien elles sont disjointes, ou bien l'une est contenue dans l'autre.

5. Un espace ultramétrique est totalement discontinu.

6. Soient E un espace ultramétrique, $r > 0$, $\mathscr{R}_r$ la relation définie sur E par $x \mathscr{R}_r y \Leftrightarrow d(x, y) \leqslant r$. La relation $\mathscr{R}_r$ est une relation d'équivalence, l'espace quotient de E par $\mathscr{R}_r$ muni de la distance $d(\bar{x}, \bar{y}) = \text{Max}\,(0, d(x, y) - r)$ où $x \in \bar{x}$ et $y \in \bar{y}$ est un espace ultramétrique.

Nous avons construit le corps $\mathbf{Q}_p$ qui est un corps muni d'une valeur absolue, complet pour cette valeur absolue, et contenant un sous-corps dense isomorphe à $\mathbf{Q}$. On sait que le corps $\mathbf{R}$ des nombres rationnels a aussi ces propriétés. Soit K un corps de caractéristique 0 muni d'une valeur absolue : la valeur absolue de K induit sur le sous-corps de K isomorphe à $\mathbf{Q}$ une valeur absolue. Pour décrire les corps de caractéristique zéro munis d'une valeur absolue, nous allons d'abord décrire les valeurs absolues de $\mathbf{Q}$, puis celles des extensions algébriques de $\mathbf{Q}$. Au chapitre 2 nous étudierons les corps valués (*i.e.* munis d'une valeur absolue) de façon plus générale.

1.7. LES VALEURS ABSOLUES DE $\mathbf{Q}$

Nous savons définir sur $\mathbf{Q}$ trois sortes de valeurs absolues :

— la valeur absolue triviale : $|0| = 0$ et $|x| = 1$ pour $x \neq 0$;

— la valeur absolue usuelle : $|x| = \mathrm{Sup}\,(x, -x)$ que nous appellerons aussi valeur absolue réelle et que nous noterons $|x|_\infty$;

— pour chaque nombre premier p, la valeur absolue p - adique, notée $|x|_p$: $|0|_p = 0$, et pour $x \neq 0$, $|x|_p = p^{-v_p(x)}$ où $v_p(x)$ est l'exposant de p dans la décomposition de x en facteurs premiers.

Le théorème d'Ostrowski, joint à la proposition 1.7.5 ci-dessous, montre que ces valeurs absolues sont « essentiellement » les seules possibles, en ce sens que les topologies définies sur $\mathbf{Q}$ par des valeurs absolues sont définies par l'une de celles décrites.

THÉORÈME 1.7.1 (Ostrowski). — *Soit $x \to |x|$ une valeur absolue non triviale sur $\mathbf{Q}$, alors :*

— *s'il existe un entier n tel que $0 < |n| < 1$, il existe un nombre premier p et un réel a, $0 < a < 1$, tels que pour tout $x \in \mathbf{Q}^*$, $|x| = a^{v_p(x)}$;*

— *sinon il existe un réel α tel que, pour tout x, $|x| = |x|_\infty^\alpha$, et $0 < \alpha \leqslant 1$.*

Remarquons d'abord qu'une fonction définie sur $\mathbf{N}$ et y satisfaisant les propriétés VA1, VA2 et VA3 se prolonge de façon unique en une valeur absolue de $\mathbf{Q}$: nous ne considérerons donc que la restriction à $\mathbf{N}$ de la valeur absolue étudiée.

D'autre part, pour $n \in \mathbf{N}$, l'inégalité triangulaire (VA3) montre que :

$$|n| \leqslant 1 + |n - 1| \leqslant n.$$

Supposons d'abord qu'il existe $n \in \mathbf{Z}$ tel que :

$$0 < |n| < 1$$

il existe alors un facteur premier p de n tel que $|p| < 1$.

LEMME 1.7.2. — *S'il existe un nombre premier p tel que $|p| < 1$, alors $|b| \leqslant 1$ pour tout $b \in \mathbf{N}$.*

Soient en effet $b \in \mathbf{N}$, $b = b_0 + b_1 p + \ldots + b_h p^h$ sa représentation en numération à base p (où $0 \leqslant b_i < p$, $b_h \neq 0$), alors :

$$|b| \leqslant |b_0| + |b_1 p| + \ldots + |b_h p^h| \leqslant |b_0| + |b_1| + \ldots + |b_h| \leqslant (1 + h)\,\mathrm{M},$$

où $\mathrm{M} = \mathrm{Sup}\,(1, |2|, \ldots, |p - 1|)$.

Soit de même h_k l'indice du dernier chiffre non nul dans la représentation de b^k en numération à base p, alors $|b|^k = |b^k| \leqslant (1 + h_k)\,\mathrm{M}$. Mais h_k est défini par $h_k \leqslant \mathrm{Log}\, b^k / \log p < 1 + h_k$, posons $\mathrm{B} = \mathrm{Log}\, b / \mathrm{Log}\, p$, on a donc $h_k \leqslant k\mathrm{B}$, d'où :

$$|b|^k \leqslant \mathrm{M}(1 + k\mathrm{B})$$

et : $|b| \leqslant \mathrm{M}^{1/k}(1 + k\mathrm{B})^{1/k}$ pour tout $k \geqslant 1$.

Or, pour $k \to \infty$, $\mathrm{M}^{1/k}(1 + k\mathrm{B})^{1/k}$ tend vers 1, d'où le lemme.

LEMME 1.7.3. — *Soit p un nombre premier tel que $|p| < 1$, alors pour tout entier q tel que $(q, p) = 1$, on a $|q| = 1$.*

Soit en effet $n \geqslant 1$, p^n et q^n sont premiers entre eux, donc il existe des entiers naturels u_n et v_n tels que :

$$u_n p^n + v_n q^n = 1.$$

D'après le lemme 1.7.2, $|q^n| \leqslant 1$, $|u_n| \leqslant 1$ et $|v_n| \leqslant 1$. Supposons que $|q| < 1$, on en déduirait que pour n assez grand :

$$1 = |1| \leqslant |u_n p^n| + |v_n q^n| \leqslant |p^n| + |q^n| < 1,$$

ce qui est impossible.

Supposons donc qu'il existe $n \in \mathbf{Z}$ tel que $0 < |n| < 1$ et soit p l'unique nombre premier tel que $|p| < 1$, soit $a = |p|$, alors tout entier $m \in \mathbf{N}$ s'écrit de façon unique $m = p^{v_p(m)} m'$ où $(m', p) = 1$, et nécessairement :

$$|m| = a^{v_p(m)} |m'| = a^{v_p(m)},$$

ce qui prouve la première assertion du théorème.

Supposons maintenant que pour tout entier $n \in \mathbf{N}$, $n > 0$, $|n| \geqslant 1$: alors il existe un entier $a \in \mathbf{N}$ tel que $|a| > 1$, sinon la valeur absolue étudiée serait triviale. Posons $\alpha = \text{Log}\,|a|/\text{Log}\,a$: $0 < \alpha < 1$, car nous avons remarqué que $|x| \leqslant a$. Soient :

$$c \in \mathbf{N} \quad \text{et} \quad c = c_0 + \ldots + c_h a^h,$$
$$c_h \neq 0 \quad \text{et} \quad 0 \leqslant c_i < a,$$

sa représentation en numération à base a. Posons :

$$M = \text{Max}\,(1, |2|, \ldots, |a - 1|) \quad \text{et} \quad C = \text{Log}\,c/\text{Log}\,a,$$

on a, comme ci-dessus :

$$|c| = |c_0 + c_1 a + \ldots + c_h a^h|$$
$$\leqslant (1 + |a| + \ldots + |a^h|)\, M = M(|a|^{h+1} - 1)/(|a| - 1),$$

et : $\quad |c|^k = |c^k| \leqslant M(|a|^{h_k+1} - 1)/(|a| - 1)$

avec : $\quad h_k \leqslant kC, \quad$ pour $\quad k \geqslant 1.$

On en déduit :

$$|c| \leqslant M^{1/k}[(|a|^{kC+1} - 1)/(|a| - 1)]^{1/k},$$

et en faisant tendre k vers l'infini :

$$|c| \leqslant a^C = c^\alpha.$$

Nous avons ainsi montré que si a est tel que $|a| > 1$, on a pour tout entier c :

$$\text{Log}\,|c|/\text{Log}\,c \leqslant \text{Log}\,|a|/\text{Log}\,a = \alpha.$$

Il en résulte, en échangeant les rôles de a et c, que si $|c| > 1$, $\text{Log}\,|c|/\text{Log}\,c = \alpha$. Or, s'il existe $c > 1$ tel

que $|c| = 1$, le calcul fait dans la première partie de la démonstration prouve qu'alors $|a| \leqslant 1$ pour tout entier a, ce qui achève la démonstration.

Remarquons que le théorème d'Ostrowski n'indique que des conditions nécessaires pour que $|x|$ soit une valeur absolue : on montrera à titre d'exercice que $a^{v_p(m)}$ et $|x|_\infty^\alpha$ définissent effectivement des valeurs absolues de $\mathbf{Q}$ pour $0 < a < 1$ et $0 < \alpha \leqslant 1$.

Nous allons maintenant comparer les différentes topologies définies sur $\mathbf{Q}$ par les valeurs absolues.

DÉFINITION 1.7.4. — *Deux valeurs absolues $|x|_1$ et $|x|_2$ sur un corps K sont dites* ÉQUIVALENTES *si elles définissent la même topologie.*

On appelle PLACES du corps K les classes d'équivalences de valeurs absolues, c'est-à-dire les topologies définies sur K par les valeurs absolues.

PROPOSITION 1.7.5. — *Les valeurs absolues $|x|_1$ et $|x|_2$ sur le corps K sont équivalentes si et seulement s'il existe une constante positive b telle que, pour tout x de K, $|x|_1 = |x|_2^b$.*

Supposons d'abord que $|x|_1 = |x|_2^b$, $b > 0$, alors la famille des boules centrées en un point a définie par l'une des distances associées coïncide avec celle définie par l'autre distance : les deux topologies sont identiques.

Réciproquement, supposons $|x|_1$ et $|x|_2$ équivalentes : l'ensemble des $x \in K$ tels que $|x|_1 < 1$ est l'ensemble des x tels que $x^n \to 0$ quand $n \to \infty$, pour la topologie $\mathcal{E}_1$ définie par $|x|_1$. Donc $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$. Soit :

$$M = \{x \in K \mid |x|_1 < 1\} = \{x \in K \mid |x|_2 < 1\}.$$

Si $M = \{0\}$, les valeurs absolues considérées sont triviales car si $x \neq 0$, $|x| \geqslant 1$ et $|x^{-1}| \geqslant 1$ entraînent $|x| = 1$, toute constante $b > 0$ est alors telle que :

$$|x|_1 = |x|_2^b.$$

Soient $a \neq 0$, $a \in M$, et soit $b = \text{Log}\,|a|_1/\text{Log}\,|a|_2$. Soient $x \in K$ et (m, n) un couple d'entiers, alors les conditions suivantes sont équivalentes :

$$|x|_1^n < |a|_1^m; \quad x^n/a^m \in M; \quad |x|_2^n < |a|_2^m;$$

$$n\,\text{Log}\,|x|_1 < m\,\text{Log}\,|a|_1; \quad n\,\text{Log}\,|x|_2 < m\,\text{Log}\,|a|_2.$$

On en déduit que :

$$\text{Log}\,|x|_2/\text{Log}\,|a|_2 = \text{Log}\,|x|_1/\text{Log}\,|a|_1,$$

soit : $$|x|_1 = |x|_2^b.$$

COROLLAIRE 1.7.6. — *Les topologies définies sur* $\mathbf{Q}$ *par des valeurs absolues non triviales sont :*

— *la topologie réelle, définie par* $|x|_\infty$*;*
— *pour tout nombre premier* p*, la topologie* p-*adique, définie par* $|x|_p$*, et induite par l'inclusion canonique dans* $\mathbf{Q}_p$.

On voit donc que si K est un corps de caractéristique zéro muni d'une valeur absolue, elle induit sur le sous-corps de K isomorphe à $\mathbf{Q}$ l'une des topologies ci-dessus décrites, en particulier :

COROLLAIRE 1.7.7. — *Soit* K *un corps de caractéristique zéro muni d'une valeur absolue ultramétrique, alors il existe un unique nombre premier* p *tel que* $|p| < 1$.

Soit $x \in \mathbf{Q}$: il n'existe qu'un nombre fini de nombres premiers p pour lesquels $v_p(x) \neq 0$, soit P l'ensemble des nombres premiers, dans le produit $\prod_{p \in P} |x|_p$, les termes sont presque tous égaux à 1. Soit $x = \varepsilon \prod_{p \in P} p^{v_p(x)}$ la décomposition de x en facteurs premiers (où les $v_p(x)$ sont presque tous nuls), alors $\prod_{p \in P} |x|_p = \prod_{p \in P} p^{-v_p(x)} = |x|_\infty^{-1}$, d'où la :

PROPOSITION 1.7.8 (FORMULE DU PRODUIT). — *Soit* $x \in \mathbf{Q}^*$, *alors* $|x|_\infty \prod_{p \in P} |x|_p = 1$.

EXERCICES 1.7. — 1. Soient k un corps fini, l une extension algébrique de k, montrer que toute valeur absolue sur l est triviale.

2. Soient K un corps, K[X] l'anneau des polynômes en une indéterminée à coefficients dans K, K(X) le corps des fractions rationnelles à coefficients dans K (corps des fractions de K[X]). On dit que deux polynômes sont équivalents s'ils définissent le même idéal de K[X], et on note S un système de représentants des classes de polynômes irréductibles.

a) Toute f non nulle de K(X) admet une unique représentation $f = a \prod p^{v_p(f)}$ où $a \in K^*$, p parcourt S et les $v_p(f)$ sont des entiers relatifs presque tous nuls.

b) Soient $p \in S$, a_p un réel $0 < a_p < 1$, montrer que l'application $f \to |f|_p$ définie par $|f|_p = a_p^{v_p(f)}$ est une valeur absolue ultramétrique sur K(X).

c) Soient $f = A/B$ un élément non nul de K(X), A et $B \in K[X]$, on pose $w(f) = \text{dg}\,B - \text{dg}\,A$, $w(f)$ ne dépend pas du choix de la représentation A/B. Soit r un réel, $0 < r < 1$, on pose $|f|_\infty = r^{w(f)}$, montrer que cela définit une valeur absolue ultramétrique sur K(X).

d) On suppose maintenant que le corps K est fini, soit q son cardinal. On choisit $r = 1/q$, et pour $p \in S$, si $n = \text{dg}\,p$, $a_p = q^{-n}$. Montrer qu'avec ce choix on a la formule du produit : pour $f \in K(X)^*$:

$$|f|_\infty \prod_{p \in S} |f|_p = 1.$$

e) Déterminer toutes les valeurs absolues de K(X).

3. Les topologies définies sur un corps K par deux valeurs absolues non équivalentes ne sont pas comparables.

1.8. LES VALEURS ABSOLUES DES CORPS DE NOMBRES

Rappelons qu'un CORPS DE NOMBRES K est une extension algébrique finie de $\mathbf{Q}$. Il existe un polynôme P unitaire et irréductible dans $\mathbf{Q}[X]$ tel que $K = \mathbf{Q}[X]/P\mathbf{Q}[X]$. Le degré d'un tel polynôme est appelé degré de K : c'est aussi la dimension du $\mathbf{Q}$-espace vectoriel K, on le note $[K : \mathbf{Q}]$. Les ENTIERS de K sont les éléments satisfaisant une équation $f(X) = 0$ où f est un polynôme unitaire à coefficients entiers. L'ensemble des entiers de K est un sous-anneau B de K dont K est le corps de fractions, B est un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. L'anneau B est nœthérien, ses idéaux premiers sont maximaux. Une partie M de K est un IDÉAL FRACTIONNAIRE si c'est un

B-module et s'il existe $b \in K$ tel que $bM \subseteq B$. En particulier les idéaux de B sont des idéaux fractionnaires : on les appelle aussi idéaux entiers. Si $x \in K$, xB est un idéal fractionnaire, il est entier si et seulement si x est entier. Soient M et M' des idéaux fractionnaires, on note MM' l'ensemble des mm' où $m \in M$ et $m' \in M'$: c'est encore un idéal fractionnaire. L'anneau B est unité pour la multiplication des idéaux fractionnaires. L'ensemble des idéaux fractionnaires non nuls de K est un GROUPE pour la multiplication. On démontre (cf., par exemple, [7], chap. 3) le :

THÉORÈME 1.8.1. — *Soit* K *un corps de nombres,* B *l'anneau des entiers de* K, P(K) *l'ensemble des idéaux premiers de* B. *Tout idéal fractionnaire non nul* M *de* K *admet une unique décomposition :*

$$M = \prod_{\mathfrak{P} \in P(K)} \mathfrak{P}^{n_{\mathfrak{P}}(M)}$$

où les $n_{\mathfrak{P}}(M)$ *sont des entiers relatifs presque tous nuls.*

Soit M un idéal entier non nul de B, sa NORME est, par définition, le cardinal N(M) de B/M, on pose $N(\{0\}) = 0$. On a alors $N(MM') = N(M)\,N(M')$: ceci permet de prolonger l'application N en un homéomorphisme du groupe des idéaux fractionnaires non nuls de K dans $\mathbf{Q}^*$. D'autre part, si $x \in K$, sa NORME $N_{K/\mathbf{Q}}(x)$ est, par définition, la norme de l'opérateur de multiplication par x dans le $\mathbf{Q}$-espace vectoriel K : c'est un homomorphisme de K^* dans $\mathbf{Q}^*$. Si $x \in \mathbf{Q}$, $N_{K/\mathbf{Q}}(x) = x^n$ où $n = [K : \mathbf{Q}]$. On montre que, pour tout x dans K :

$$N(xB) = N_{K/\mathbf{Q}}(x).$$

Revenons maintenant aux valeurs absolues. Soient f un polynôme unitaire irréductible de $\mathbf{Q}[X]$ définissant K et ω la projection canonique de $\mathbf{Q}[X]$ sur $K = \mathbf{Q}[X]/f\mathbf{Q}[X]$. A une racine α_i de f dans $\mathbf{C}$ on peut associer un homomorphisme p_i de K dans $\mathbf{C}$ défini par $p_i(a) = a$ pour $a \in \mathbf{Q}$ et $p_i(\omega(X)) = \alpha_i$; p_i est un isomorphisme de K sur un sous-corps de $\mathbf{C}$. Pour $x \in K$, on posera :

$$|x|_i = |p_i(x)|_\infty$$

où $|z|_\infty$ désigne le module du nombre complexe z : il est clair que $|x|_i$ est une valeur absolue sur K dont la trace sur $\mathbf{Q}$ est $|x|_\infty$.

On convient d'indexer les n racines (distinctes) de f dans $\mathbf{C}$, $\alpha_1, \ldots, \alpha_n$, de telle sorte que $\alpha_i \in \mathbf{R}$ pour $i = 1, \ldots, r$ et $\alpha_i \neq \bar{\alpha}_i = \alpha_{i+s}$ pour $i = r+1, \ldots, r+s$ (alors $n = r + 2s$).

THÉORÈME 1.8.2. — *Les* $r+s$ *valeurs absolues* $|x|_i$, $i = 1, \ldots, r+s$, *sont deux à deux non équivalentes. Toute valeur absolue sur* K *induisant sur* $\mathbf{Q}$ *la topologie réelle est équivalente à l'une d'entre elles.*

On appelle PLACES INFINIES les classes de valeurs absolues induisant la topologie réelle sur $\mathbf{Q}$. Le théorème ci-dessus signifie donc que les $r+s$ valeurs absolues indiquées constituent un système de représentants des places infinies.

Supposons qu'il existe $i \neq j$ tels que $|x|_i \simeq |x|_j$: alors $p_i \circ p_j^{-1}$ se prolonge en un isomorphisme de corps topologiques de $K_j = \overline{p_j(K)}$ sur $K_i = \overline{p_i(K)}$. Les corps K_i et K_j sont des sous-corps complets de $\mathbf{C}$: ils sont donc égaux à $\mathbf{R}$ ou $\mathbf{C}$. Si l'un d'entre eux est $\mathbf{R}$, il n'existe pas d'isomorphisme de corps topologique autre que l'identité, donc $K_i = K_j = \mathbf{C}$; et $p_i \circ p_j^{-1}$ est la conjugaison dans $\mathbf{C}$: mais ceci est impossible car $\alpha_i = p_i \circ p_j^{-1}(\alpha_j) \neq \bar{\alpha}_j$ pour les indices i et j considérés.

Soient maintenant $|x|$ une valeur absolue sur K induisant sur $\mathbf{Q}$ la topologie réelle, $\hat{K}$ le complété de K pour $|x|$. Le corps $\hat{K}$ est une extension algébrique finie de $\mathbf{R}$, il est donc isomorphe (comme corps topologique) à $\mathbf{R}$ ou $\mathbf{C}$. Soit $a : \hat{K} \to \mathbf{C}$ un tel isomorphisme : $a(\omega(X))$ est une racine α_i de f dans $\mathbf{C}$. Notons $(K, |\ |)$ (resp. $(K, |\ |_i)$)

l'espace topologique « K muni de $|\ |$ » (resp. K muni de $|\ |_i$), alors $p_i \circ a^{-1}$ est l'identité de K, et c'est un homéomorphisme de $(K, |\ |)$ sur $(K, |\ |_i)$, ce qui prouve que $|x| \simeq |x|_i$.

Etudions maintenant les PLACES FINIES de K, c'est-à-dire celles qui induisent sur $\mathbf{Q}$ une topologie p - adique.

Faisons d'abord quelques remarques.

(i) Une fonction $|x|$ définie sur B et y satisfaisant VA1, VA2 et VA3 se prolonge de façon unique en une valeur absolue de K.

(ii) Deux valeurs absolues $|x|_1$ et $|x|_2$ telles que $\{x \in B \mid |x|_1 < 1\} = \{x \in B \mid |x|_2 < 1\}$ sont équivalentes. On voit en effet en reprenant la preuve de 1.7.5 qu'il existe $b > 0$ tel que, pour $x \in B$, $|x|_1 = |x|_2^b$.

(iii) Si $|x|$ appartient à une place finie :

$$B \subseteq \{x \in K \mid |x| \leqslant 1\}.$$

En effet, tout $x \in B$ satisfait une équation :

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \qquad a_i \in \mathbf{Z},$$

donc, pour $x \in B$, $|x^n| \leqslant 1 + |x| + \ldots + |x^{n-1}|$, ce qui entraîne $|x| < 2$. Or si b est tel que $|b| > 1$, il existe k tel que $|b^k| > 2$.

(iv) Si $|x|$ appartient à une place finie :

$$M = \{x \in B \mid |x| < 1\}$$

est un idéal premier de B. En effet, si $x \in M$ et $y \in M$, x^n et $y^n \to 0$ quand $n \to \infty$. On en déduit aisément que $(x+y)^n \to 0$, donc $x + y \in M$; si $b \in B$ et $x \in M$, $bx \in M$. Enfin, si x et $y \in B - M$, $|xy| = |x|\,|y| = 1$, $|xy| \notin M$.

(v) Soit $\mathfrak{P}$ un idéal premier de B. On pose, pour $x \in K$, $v_{\mathfrak{P}}(x) = n_{\mathfrak{P}}(xB)$ (cf. 1.8.1). On vérifie aisément que $v_{\mathfrak{P}}(x)$ définit une valuation sur K. En posant :

$$|x|_{\mathfrak{P}} = N(\mathfrak{P})^{-v_{\mathfrak{P}}(x)}$$

on définit une valeur absolue sur K, appelée VALEUR ABSOLUE $\mathfrak{P}$ - ADIQUE, qui induit sur $\mathbf{Q}$ la topologie p - adique où p est l'unique nombre premier tel que $p \in \mathfrak{P}$.

(vi) Pour chaque nombre premier p, l'ensemble des $\mathfrak{P}$ tels que $p \in \mathfrak{P}$ est fini : c'est l'ensemble des $\mathfrak{P}$ tels que $v_{\mathfrak{P}}(p) \neq 0$. On notera $p \mid \mathfrak{P}$ au lieu de $pB \mid \mathfrak{P}$ (ou $v_{\mathfrak{P}}(p) \neq 0$). Si $p \mid \mathfrak{P}$, $N(\mathfrak{P})$ est une puissance de p, car $B/\mathfrak{P}$ est un $\mathbf{Z}/p\mathbf{Z}$ espace vectoriel.

THÉORÈME 1.8.3. — *L'ensemble des valeurs absolues $\mathfrak{P}$ - adiques, où $\mathfrak{P}$ parcourt l'ensemble des idéaux premiers de* B, *est un système de représentants des places finies de* K.

En effet, si $\mathfrak{P} \neq \mathfrak{P}'$, les valeurs absolues $\mathfrak{P}$ - adique et $\mathfrak{P}'$ - adique ne sont pas équivalentes car :

$$\mathfrak{P} = \{x \in B \mid |x|_{\mathfrak{P}} < 1\}.$$

D'autre part, si $|x|$ est une valeur absolue appartenant à une place finie, nous avons vu que $M = \{x \in B \mid |x| < 1\}$ est un idéal premier de B (cf. (iv)), et, d'après la remarque (ii), $|x|$ est équivalente à $|x|_M$.

THÉORÈME 1.8.4. (Formule du produit). — *Pour tout* $x \in K$, $|x|_{\mathfrak{P}} = 1$ *pour presque tout* $\mathfrak{P} \in P(K)$, *et on a :*

$$\prod_{i=1}^{r+s} |x|_i^{N(i)} \times \prod_{\mathfrak{P} \in P(K)} |x|_{\mathfrak{P}} = 1,$$

où $N(i) = 1$ *si* $\alpha_i \in \mathbf{R}$ *et* $N(i) = 2$ *si* $\alpha_i \notin \mathbf{R}$.

Remarquons d'abord que :

$$\prod_{1 \leqslant i \leqslant r+s} |x|_i^{N(i)} = \prod_{1 \leqslant i \leqslant n} |p_i(x)|_\infty = |N_{K/\mathbf{Q}}(x)|_\infty.$$

Notons d'autre part $P(\mathbf{Q})$ l'ensemble des nombres premiers, on a :

$$N_{K/\mathbf{Q}}(x) = N(xB) = \prod_{\mathfrak{P} \in P(K)} N(\mathfrak{P})^{v_{\mathfrak{P}}(x)} = \prod_{p \in P(\mathbf{Q})} \Big(\prod_{p \mid \mathfrak{P}} N(\mathfrak{P})^{v_{\mathfrak{P}}(x)} \Big).$$

Il en résulte que :

$$v_p(N_{K/\mathbf{Q}}(x)) = \sum_{p \mid \mathfrak{P}} v_{\mathfrak{P}}(x)\, v_p(N(\mathfrak{P}))$$

et : $|N_{K/Q}(x)|_p = \prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}}$.

Alors :

$$\prod_{i=1}^{r+s} |x|_i^{N(i)} \times \prod_{\mathfrak{p} \in P(K)} |x|_{\mathfrak{p}} = |N_{K/Q}(x)|_\infty \times \prod_{p \in P(Q)} |N_{K/Q}(x)|_p ;$$

Or, pour $x \in K^*$, $N_{K/Q}(x) \in Q^*$, donc on peut appliquer la formule du produit 1.7.8, d'où le théorème.

REMARQUE. — Les valeurs absolues $|x|_i$ et $|x|_{\mathfrak{p}}$ définies ci-dessus, et qui sont un système de représentant des places non triviales de K, sont dites normalisées. Il faut noter que, si $|x|_i$ induit sur $\mathbf{Q}$ la valeur absolue $|x|_\infty$, $|x|_{\mathfrak{p}}$ n'induit généralement pas la valeur absolue p - adique. Plus précisément, soit $f(\mathfrak{P})$ le degré de $B/\mathfrak{P}$ sur $\mathbf{Z}/p\mathbf{Z}$, $N(\mathfrak{P}) = p^{f(\mathfrak{P})}$, alors, pour $x \in \mathbf{Q}$, $|x|_{\mathfrak{p}} = |x|_p^{f(\mathfrak{P})}$. On choisit parfois, comme représentant de la classe de $|x|_{\mathfrak{p}}$, la valeur absolue $|x|'_{\mathfrak{p}} = (|x|_{\mathfrak{p}})^{1/f(\mathfrak{P})}$ qui prolonge à K la valeur absolue p - adique de $\mathbf{Q}$. On obtient ainsi une autre expression de la formule du produit où $|x|_{\mathfrak{p}}$ est remplacée par $|x|'^{f(\mathfrak{P})}_{\mathfrak{p}}$.

CHAPITRE 2

Les corps valués ultramétriques

2.1. VALUATIONS ET VALEURS ABSOLUES ULTRAMÉTRIQUES

Rappelons que les valeurs absolues ultramétriques ont été définies en 1.6. Au chapitre 1 nous avons étudié des valuations à valeurs entières : on considère plus généralement des valuations à valeurs dans $\mathbf{R} \cup \{\infty\}$, muni de l'ordre et l'addition naturels.

DÉFINITION 2.1.1. — *Soit* K *un corps, une application* v *de* K *dans* $\mathbf{R} \cup \{+\infty\}$ *est une* VALUATION *si elle satisfait :*

V1 : *pour tout* $x \in K$, $v(x) = +\infty \Leftrightarrow x = 0$;
V2 : *pour tous* x *et* $y \in K$, $v(xy) = v(x) + v(y)$;
V3 : *pour tous* x *et* $y \in K$, $v(x+y) \geqslant \mathrm{Inf}\,(v(x), v(y))$.

Nous avons rencontré des exemples de valuation au chapitre 1, en particulier le corps des fractions d'un anneau de valuation discrète est canoniquement muni d'une valuation à valeurs entières.

Etant donné un corps K muni d'une valuation, l'image $v(K^*)$ du groupe multiplicatif de K est, d'après V2, un sous-groupe additif de $\mathbf{R}$ qu'on appelle GROUPE DE VALUATION. On sait, cf. par exemple exercice 2.1.1, qu'un sous-groupe additif de $\mathbf{R}$ est ou bien discret ou bien dense dans $\mathbf{R}$. On dit que la valuation v est DISCRÈTE OU DENSE suivant que $v(K^*)$ est discret ou dense. Tous les exemples

que nous avons rencontrés sont des valuations discrètes. Nous verrons des exemples de valuation dense d'abord dans l'exercice 2.1.7, puis au numéro 2.6.

PROPOSITION 2.1.2. — *Soient v une valuation sur le corps* K *et a un réel, $0 < a < 1$, alors la fonction $x \to |x|$ définie par $|0| = 0$ et $|x| = a^{v(x)}$ pour $x \neq 0$ est une valeur absolue ultramétrique sur* K.

Réciproquement, si $|x|$ est une valeur absolue ultramétrique sur K *et b un réel, $b > 0$, la fonction v définie par $v(0) = +\infty$ et $v(x) = -b \operatorname{Log} |x|$ pour $x \neq 0$ est une valuation.*

Vérification immédiate.

PROPOSITION 2.1.3. — *Soit v une valuation sur le corps* K, *alors :*

— *l'ensemble $A = \{x \in K \mid v(x) \geqslant 0\}$ est un sous-anneau unitaire de* K *appelé* ANNEAU DE LA VALUATION *v; pour tout $x \in K$, ou bien $x \in A$ ou bien $x^{-1} \in A$,* K *est le corps de fractions de* A;

— *l'ensemble $M = \{x \in K \mid v(x) > 0\}$ est l'unique idéal maximal de* A; *il est constitué des éléments non inversibles de* A, *on l'appelle* IDÉAL DE LA VALUATION *v.*

D'après V2, $v(1) = 0$, donc $1 \in A$. Si x et $y \in A$, $v(xy) \geqslant 0$ d'après V2 et $v(x+y) \geqslant 0$ d'après V3, donc A est un sous-anneau unitaire de K. Si $x \in K$, ou bien $v(x) \geqslant 0$, et $x \in A$, ou bien $v(x) < 0$, alors :

$$v(x^{-1}) = -v(x) > 0,$$

et $x \in M$, donc $x \in A$. Il est alors clair que K est le corps des fractions de A.

De même, M est un sous-groupe additif, d'après V3; si $x \in A$ et $y \in M$, $v(xy) \geqslant v(y) > 0$, donc M est un idéal de A. Enfin, si $x \in A$ et $x^{-1} \notin A$, $v(x) \geqslant 0$ et $-v(x) < 0$, donc $x \in M$: l'idéal M, constitué des éléments non inversibles de A, est l'unique idéal maximal de A (cf. 1.4.8).

Remarquons que si $|x| = a^{v(x)}$ est une valeur absolue associée à la valuation v, A est encore l'ensemble des $x \in K$ tels que $|x| \leqslant 1$: on l'appelle aussi la BOULE UNITÉ de K, tandis que $M = \{x \in K \mid |x| < 1\}$ est aussi appelé BOULE UNITÉ OUVERTE ou non circonférenciée.

COROLLAIRE 2.1.4.

(i) *Les valeurs absolues de* K *associées à une même valuation v sont équivalentes, v définit donc une topologie sur* K; *deux valuations sont dites* ÉQUIVALENTES *si elles définissent la même topologie.*

(ii) *Deux valuations sont équivalentes à la condition nécessaire et suffisante qu'elles soient proportionnelles, le coefficient de proportionnalité étant positif.*

(iii) *Deux valuations sont équivalentes à la condition nécessaire et suffisante qu'elles définissent le même anneau de valuation, ou le même idéal de valuation.*

Toutes ces affirmations ne sont que des reformulations de la proposition 1.7.5 compte tenu du « dictionnaire » fourni par 2.1.2.

DÉFINITION 2.1.5. — *Le corps quotient* A/M *s'appelle* CORPS RÉSIDUEL *de la valuation v.*

Ce corps peut être fini ou non.

EXEMPLES. — 1. Pour le corps $\mathbf{Q}_p$:

$$A = \mathbf{Z}_p, \quad M = p\mathbf{Z}_p = \pi_1^{-1}(0).$$

Le corps résiduel A/M est donc l'image :

$$\pi_1(\mathbf{Z}_p) = \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p,$$

corps à p éléments.

2. Si K est un corps de nombre muni de la valuation $v_{\mathfrak{P}}$ associée à un idéal premier, l'anneau de valuation A est le localisé $B_{\mathfrak{P}}$ de l'anneau B des entiers de K, c'est-à-dire le sous-anneau de K constitué des quotients x/y où $x \in B$ et $y \in B - \mathfrak{P}$. L'idéal de valuation M est l'idéal $\mathfrak{P}B_{\mathfrak{P}}$

engendré par $\mathfrak{P}$ dans $B_{\mathfrak{P}}$. Le corps résiduel $k = B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}}$ est $B/\mathfrak{P}$. Soient en effet π la projection canonique de $A = B_{\mathfrak{P}}$ sur k et π_B sa restriction à B, alors l'image de π_B est $B/\mathfrak{P}$, il suffit donc de montrer que l'image de π_B est k. Or, soit $y \in B - \mathfrak{P}$, alors $\pi_B(y)$ est inversible dans $B/\mathfrak{P}$, soit $z \in \pi_B(y)^{-1}$, $\pi(xz - x/y) = 0$, donc pour tout $x/y \in B_{\mathfrak{P}}$ il existe $a \in B$ tel que $\pi(x/y) = \pi(a)$.

3. On montrera à titre d'exercice que, pour le corps des fractions de l'anneau A étudié à l'exemple 1 de 1.4, l'anneau de valuation est A, l'idéal de valuation M, le corps résiduel est le corps K des scalaires, le groupe de valuation est Z. On voit ainsi qu'étant donné un corps K on peut construire un corps muni d'une valuation discrète ayant un corps résiduel isomorphe à K.

PROPOSITION 2.1.6. — *Soit* K *un corps muni d'une valuation discrète* v, *alors l'anneau de valuation* A *est un anneau de valuation discrète.*

Compte tenu de la proposition 2.1.3, il suffit de montrer que A est principal. Soient $\Gamma = v(K^*)$ le groupe de valuation et $a > 0$ l'unique réel positif tel que $\Gamma = a\mathbf{Z}$. Soient I un idéal propre de A et $ka = \mathrm{Inf}\{v(x) \mid x \in I\}$, alors $k > 0$. De plus, comme Γ est discret, il existe $i \in I$ tel que $v(i) = ka$; alors $iA \subset I$, mais si $x \in I$, $v(x) \geqslant v(i)$, donc $v(x/i) \geqslant 0$, $x/i \in A$ et $I \subseteq iA$. On voit en particulier que M est principal et que ses générateurs sont les éléments m tels que $v(m) = a$: on appelle un générateur de M une UNIFORMISANTE. On voit qu'une uniformisante est un élément $m \in K$ tel que $v(m) > 0$ et $v(K^*) = v(m)\,\mathbf{Z}$.

EXERCICES 2.1.7. — 1. Soit Γ un sous-groupe additif de R, montrer que :

— si O est point d'accumulation de Γ, Γ est dense dans R;
— sinon, il existe un unique réel positif a tel que $\Gamma = a\mathbf{Z}$.

2. Soit Γ un sous-groupe additif de R, on note $S(\Gamma)$ l'ensemble des « suites extraites de Γ tendant vers l'infini », c'est-à-dire l'ensemble des parties dénombrables de Γ dont l'intersection avec toute demi-droite $]-\infty, A]$ est finie.

On appelle séries formelles à exposants dans Γ et coefficients dans le corps K, et on note $L(\Gamma, K)$, ou L, l'ensemble des applications a de R dans K telles que :

$$\{x \in R \mid a(x) \neq 0\} \in S(\Gamma)$$

(on peut noter $a = \sum_{x \in R} a(x)\, X^x$ une telle a).

(i) Si a et $b \in L$, on note $a + b$ l'application définie par $(a + b)(x) = a(x) + b(x)$. Alors $a + b \in L$, et L est un groupe pour cette loi.

(ii) Si a et $b \in L$, pour tout $x \in R$, la somme $\sum_{y+z=x} a(y)\, b(z)$ a des termes presque tous nuls. On note ab l'application définie par $ab(x) = \sum_{y+z=x} a(y)\, b(z)$. Alors $ab \in L$, L est un anneau.

(iii) Si $f \in L$, $f \neq 0$, on pose $v(f) = \mathrm{Inf}\{x \in R \mid a(x) \neq 0\}$ et $v(0) = +\infty$: v est une valuation sur L.

(iv) L est un corps.

(v) Déterminer l'anneau, l'idéal et le groupe de valuation de v, et le corps résiduel.

2.2. PROPRIÉTÉS MÉTRIQUES

Soit K un corps muni d'une valeur absolue ultramétrique; sauf précision contraire nous conviendrons d'associer à cette valeur absolue la valuation $v(x) = -\mathrm{Log}\,|x|$.

De même, si K est muni d'une valuation v, nous lui associerons en général la valeur absolue $|x| = e^{-v(x)}$. Nous appellerons CORPS VALUÉ ou CORPS VALUÉ ULTRAMÉTRIQUE un corps muni d'une valeur absolue ultramétrique (ou d'une valuation) : il se trouvera par là même muni d'une valuation (ou d'une valeur absolue), ces données étant reliées soit par une convention explicite (par exemple pour $\mathbf{Q}_p$, $v(x) = -\log_p |x|$) ou sinon par la relation $v(x) = -\mathrm{Log}\,|x|$.

Un corps valué est donc un espace métrique, muni d'une distance *ultramétrique*. Nous avons indiqué en exercice au § 1.6 quelques propriétés des espaces ultramétriques dont la démonstration est facile :

1. Soient x, y et z tels que $d(x, y) \neq d(y, z)$, alors $d(x, z) = \mathrm{Max}\,(d(x, y), d(y, z))$.

2. Tout point d'une boule en est un centre.

3. Deux boules sont soit disjointes, soit comparables (pour l'inclusion).

PROPOSITION 2.2.1. — *Dans un espace ultramétrique, une boule est une partie à la fois ouverte et fermée.*

Soit $B'(a, r) = \{x \mid d(x, a) \leqslant r\}$ la boule fermée de centre a et de rayon r. Si $x \in B'(a, r)$:

$$B(x, r) \subseteq B'(x, r) = B'(a, r)$$

donc $B'(a, r)$ est un ouvert. De même la boule ouverte $B(a, r)$ est un ensemble fermé, car, si $b \notin B(a, r)$, la boule ouverte $B(b, r)$ ne rencontre pas $B(a, r)$.

COROLLAIRE 2.2.2. — *Un espace ultramétrique est totalement discontinu.*

En effet tout point a une base de voisinages à la fois ouverts et fermés.

Rappelons que dans un espace métrique une SUITE DE CAUCHY est une suite (a_n) telle que, quel que soit $\varepsilon > 0$, il existe $N(\varepsilon)$ tel que, pour $n \geqslant N(\varepsilon)$ et $m \geqslant N(\varepsilon)$, $d(a_n, a_m) \leqslant \varepsilon$. On dit qu'un espace métrique est COMPLET si toute suite de Cauchy y est convergente.

PROPOSITION 2.2.3. — *Dans un espace ultramétrique une suite (a_n) est une suite de Cauchy à la condition nécessaire et suffisante que $d(a_n, a_{n+1}) \to 0$ quand $n \to \infty$.*

Supposons que $d(a_n, a_{n+1}) \to 0$, alors pour tout $\varepsilon > 0$, $d(a_n, a_{n+1}) \leqslant \varepsilon$ pour $n \geqslant N(\varepsilon)$. Pour tout $k \geqslant 1$:

$$d(a_n, a_{n+k}) \leqslant \text{Max}\,(d(a_n, a_{n+k-1}), d(a_{n+k-1}, a_{n+k})),$$

d'où, par récurrence sur k, $d(a_n, a_{n+k}) \leqslant \varepsilon$ pour $n \geqslant N(\varepsilon)$, et la suite est de Cauchy. Réciproque évidente.

COROLLAIRE 2.2.4. — *Soit K un corps valué ultramétrique complet; pour que la série de terme général u_n soit convergente, il faut et il suffit que $u_n \to 0$.*

C'est une simple reformulation dans un cas particulier de la proposition 2.2.3.

PROPOSITION 2.2.5. — *Soient a_n une suite de Cauchy dans un espace ultramétrique et b un point tel que $d(b, a_n) \not\to 0$, alors la suite $d(b, a_n)$ est stationnaire.*

Soit en effet $r = \lim d(b, a_n)$, par hypothèse $r \neq 0$ ($d(b, a_n)$ est une suite convergente). Pour n assez grand, $d(a_n, a_{n+1}) < d(b, a_n)$, alors $d(b, a_{n+1}) = d(b, a_n)$.

COROLLAIRE 2.2.6. — *Soient K un corps muni d'une valuation v et K' un sous-corps dense de K, alors $v(K^*) = v(K'^*)$.*

Soient en effet $x \in K^*$ et x_n une suite de points de K' tendant vers x : alors $|x_n| \to |x| \neq 0$, donc la suite $|x_n| = d(x_n, 0)$ est stationnaire et, pour n assez grand, $v(x_n) = v(x)$.

Remarquons que toutes les propriétés indiquées dans ce paragraphe sont spécifiques du cas ultramétrique comme on s'en convaincra aisément en tentant de les traduire, par exemple, au cas de l'espace métrique **R** et de son sous-corps dense **Q**.

2.3. CORPS VALUÉS ULTRAMÉTRIQUES COMPLETS

Parmi les corps valués que nous avons étudiés, le corps **Q** muni de la valuation p - adique n'est pas complet. En effet, par exemple, un développement de Hensel $\sum_{n \geqslant 0} a_n p^n$ qui n'est pas périodique converge vers un élément de $\mathbf{Q}_p$ qui n'appartient pas à **Q** (cf. 1.5, exercice). Par contre $\mathbf{Q}_p$ est complet : en effet, si (a_n) est une suite de Cauchy dans $\mathbf{Q}_p$, il existe R tel que, pour tout n, $|a_n| \leqslant R$. La boule $B'(0, R)$ qui est homéomorphe à $\mathbf{Z}_p$ est compacte. La suite a_n a donc un point d'accumulation x dans $B'(0, R)$; comme c'est une suite de Cauchy, x est limite de (a_n). On peut en déduire que **Q** n'est pas complet : en effet, d'une

part, $\mathbf{Q} \neq \mathbf{Q}_p$, car $\mathbf{Q}_p$ a la puissance du continu (cela résulte de l'existence et unicité du développement de Hensel), d'autre part, $\mathbf{Q}$ n'est pas fermé dans $\mathbf{Q}_p$ puisqu'il y est dense, et que $\mathbf{Q}_p \neq \mathbf{Q}$.

PROPOSITION 2.3.1. — *Soient* K *un corps valué ultramétrique, v la valuation de* K.

(i) *Il existe un corps valué complet* K′, *v′ et une injection isométrique i de* K *dans* K′ *tels que* i(K) *soit dense dans* K′.

(ii) *Un tel corps* K′, *v′ est unique à isomorphisme isométrique près, on l'appelle le* COMPLÉTÉ *de* K *pour la valuation v.*

(iii) *Le groupe de valuation et le corps résiduel de* K′ *sont isomorphes à ceux de* K.

Indiquons d'abord le schéma de construction d'un corps valué K′, v' satisfaisant (i) :

— l'ensemble $K^{\mathbf{N}}$ des suites à valeurs dans K a une structure naturelle d'anneau;
— l'ensemble C(K) des suites de Cauchy de K est un sous-anneau de $K^{\mathbf{N}}$;
— l'ensemble I(K) des suites tendant vers 0 est un idéal maximal de C(K);
— soient K′ le corps quotient C(K)/I(K) et i l'homomorphisme de K dans K′ qui à $x \in K$ associe la classe $i(x)$ de la suite constante $x_n = x$, i est une injection;
— pour $x \in K'$, on pose $v'(x) = \lim v(x_n)$ où $(x_n) \in x$, v' est une valuation sur K′ et, pour $a \in K$, $v'(i(a)) = v(a)$;
— K′ est complet pour la valuation v' et i(K) est dense dans K′.

Les démonstrations des assertions ci-dessus sont de simples vérifications.

Soient K′, v' et i satisfaisant (i), K″, v'' et j y satisfaisant aussi. Alors $i \circ j^{-1} = \alpha$ est un isomorphisme isométrique de j(K) sur i(K) : α admet donc un unique prolongement continu à K″, on vérifie que ce prolongement est un isomorphisme algébrique en utilisant la continuité de l'addition et la multiplication dans un corps valué.

Enfin, les groupes de valuation de K et K′ sont isomorphes (corollaire 2.2.6). Soient A, M et k (resp. A′, M′ et k') l'anneau de valuation, l'idéal de valuation et le corps résiduel de K (resp. K′). On a $M = A \cap M'$, donc $k = A/M$ s'injecte canoniquement dans $k' = A'/M'$, et cette injection est surjective car toute classe modulo M′ dans A′ est un ouvert (c'est une boule ouverte de rayon 1), donc contient un élément de A.

EXERCICE 2.3.2. — Soient K un corps, $L = K(X)$ le corps des fractions rationnelles en une indéterminée sur K, P un polynôme irréductible et v_P la valuation de L associée à P (cf. exercice 1.7, n° 2). Déterminer l'anneau de valuation, l'idéal de valuation et le corps résiduel de v_P. Décrire le complété de L pour la valuation v_P lorsque $P = X$. En déduire une description du complété dans le cas général.

PROPOSITION 2.3.3. — *Soit* K *un corps valué complet, les conditions :*

(i) K *est localement compact;*
(ii) *le groupe de valuation est discret et le corps résiduel fini, sont équivalentes.*

Remarquons d'abord qu'il est nécessaire que K soit complet pour qu'il soit localement compact : cette hypothèse n'est donc pas restrictive.

D'autre part, K est localement compact si et seulement si les boules sont compactes. Enfin, pour que les boules soient compactes, il faut et il suffit que l'anneau de valuation A le soit : en effet, toute boule fermée est homéomorphe à A.

Supposons d'abord que $\Gamma = v(K^*)$ est discret et $k = A/M$ fini. Soient B une partie infinie de A et q le cardinal de k, et soit $a > 0$ un générateur de Γ. La partition de A en q classes modulo M induit une partition de B en q parties, dont l'une au moins, soit B_1, est infinie. Soit $b_1 \in B_1$, on a donc $B_1 \subseteq b_1 + M$. Supposons qu'on

ait construit une suite $b_1, b_2, \ldots, b_n$ de points deux à deux distincts de B ayant la propriété suivante :

(P) $B_i = B \cap (b_i + M^i)$ est infini et $B_{i+1} \subseteq B_i$.

La partition de $b_n + M^n$ en q classes modulo M^{n+1} induit une partition de B_n en q parties dont l'une au moins, soit B_{n+1}, est infinie. On peut alors choisir :

$$b_{n+1} \in B_{n+1}$$

de façon que $b_{n+1} \neq b_n$. On a ainsi une suite infinie de points b_i deux à deux distincts dans B, satisfaisant la propriété (P) pour $i \geqslant 1$. Or la suite b_i est une suite de Cauchy, car $b_{n+1} - b_n \in M^n$, donc $v(b_{n+1} - b_n) \geqslant na$. La limite b de b_i est un point d'accumulation de B dans A, donc A est compact.

Supposons maintenant que k soit infini : on peut trouver dans A une famille infinie B de points deux à deux distincts modulo M. Alors si b et $b' \in B$ et $b \neq b'$, $v(b - b') = 0$: on ne peut donc extraire de B aucune suite convergente, et A n'est pas compact.

De même, si Γ est dense, on peut extraire de Γ une suite décroissante $r_1, \ldots, r_n$, telle que, par exemple, $r_n \to 0$. Choisissons, pour $n \geqslant 1$, $a_n \in A$ tel que $v(a_n) = r_n$. Alors, pour $n \neq m$, $v(a_n - a_m) = \mathrm{Max}\,(r_n, r_m)$. On ne peut donc extraire de (a_n) une suite convergente et A n'est pas compact.

Exemple. — On sait que pour un corps de nombres K muni de la valuation $v_{\mathfrak{P}}$ associée à un idéal premier $\mathfrak{P}$, le corps résiduel $B/\mathfrak{P}$ est fini et le groupe de valuation est Z. Donc le complété de K pour la valuation $v_{\mathfrak{P}}$ est localement compact.

Exercices 2.3. — 1. A quelles conditions le complété de K(X) pour une valuation v_P (cf. exercice 2.3.2) est-il localement compact ?

2. Soient k un corps, a et b deux réels > 0. Soit $K = k(X, Y)$ le corps des fractions rationnelles à deux indéterminées sur k. Soit $P = \sum a_{mn} X^m Y^n$ un polynôme, on pose $v(P) = \mathrm{Inf}\{am + bn\}$, où (m, n) parcourt l'ensemble des couples tels que $a_{mn} \neq 0$, si $P \neq 0$, et $v(0) = +\infty$. Si $R = P/Q \in K$, où P et Q sont des polynômes, on pose :

$$v(R) = v(P) - v(Q).$$

a) v est une valuation, déterminer l'anneau et l'idéal de valuation ainsi que le corps résiduel.

b) Décrire le complété de K. A quelles conditions sur a, b et k est-il localement compact ?

2.4. Racines de l'unité

Nous étudierons au § 2.6 les extensions algébriques des corps valués : il sera commode à cet effet de savoir distinguer les polynômes irréductibles, ce que nous ferons au § 2.5. Une des formes les plus simples d'équations algébriques est celle des racines n-ièmes de l'unité, $X^n - 1 = 0$. Nous savons déjà que, si $n = p - 1$, l'équation :

$$X^{p-1} - 1 = 0$$

a, dans $\mathbf{Q}_p$, $p - 1$ racines distinctes (cf. exercice 1.1). Plus généralement :

Proposition 2.4.1. — *Soit* K *un corps valué complet de caractéristique* 0 *dont le corps résiduel* $k = A/M$ *est fini, et soit* q *le cardinal de* k, *alors :*

(i) *pour tout* $a \in A$ *tel que* $v(a) = 0$, *la suite* a^{q^n} *converge vers une racine* $b(a)$ *de l'équation* $X^{q-1} - 1 = 0$, *et* $b(a) - a \in M$;

(ii) *soit* n *un entier,* $(n, q) = 1$, *l'équation* $X^n - 1 = 0$ *a dans* K d *racines distinctes deux à deux incongrues modulo* M, *où* $d = (n, q - 1)$.

Nous noterons p l'unique nombre premier tel que $v(p) = r > 0$. Alors q est une puissance de p car l'image de p dans k est nulle.

Lemme 2.4.2. — *Si* $a \in A$, $a^q - a \in M$.

En effet, tout élément de k satisfait l'équation $x^q = x$, donc l'image de $a^q - a$ dans k est nulle.

LEMME 2.4.3. — *Soit* $u \in M$, *alors :*

$$v((1+u)^q - 1) \geqslant \mathrm{Inf}\,(r + v(u), qv(u)).$$

D'après la formule du binôme :

$$(1+u)^q - 1 = u^q + \sum_{1 \leqslant i \leqslant q-1} \binom{q}{i} u^i = u^q + U.$$

Or, $\binom{q}{i} = \binom{q-1}{i-1} q/i$, donc :

$$v\left(\binom{q}{i}\right) = v(q) - v(i) + v\left(\binom{q-1}{i-1}\right) \geqslant v(q) - v(i).$$

Pour $1 \leqslant i \leqslant q-1$, $v(q) - v(i) \geqslant v(p) = r$. D'où $v(U) \geqslant v(u) + r$, par application itérée de l'inégalité ultramétrique V3; alors :

$$v(u^q + U) \geqslant \mathrm{Inf}\,(r + v(u), qv(u)).$$

Soit donc $a \in A - M$, alors $a^q - a \in M$, mais $a \notin M$, donc $a^{q-1} - 1 \in M$. Soit $u_1 = a^{q-1} - 1$. De même, pour $n \geqslant 1$, $a^{q^n} - a^{q^{n-1}} \in M$, posons $a^{q^n} = a^{q^{n-1}}(1 + u_n)$, alors $u_n \in M$ et $u_{n+1} = (1+u_n)^q - 1$. D'après le lemme 2.4.3, $v(u_{n+1}) \geqslant \mathrm{Inf}\,(r + v(u_n), qv(u_n))$. Comme $v(u_1) > 0$, il en résulte que $v(u_n) \to +\infty$, donc a^{q^n} est une suite de Cauchy : elle a une limite $b(a)$, qui satisfait visiblement l'équation $b(a)^q = b(a)$. De plus, pour tout n :

$$a^{q^n} \equiv a^{q^{n-1}} \equiv a \bmod. M,$$

or $a + M$ est fermé, donc à la limite $a \equiv b(a)$ mod. M. En particulier, $b(a) \notin M$, donc $b(a) \neq 0$, d'où l'assertion (i).

Soient maintenant $n \geqslant 1$ et x une racine de :

$$X^n - 1 = 0,$$

alors $nv(x) = 0$, donc $v(x) = 0$. Soit π la projection canonique de A sur k, alors $\pi(x)^n = 1$ dans k. Cette dernière équation a, dans k, d racines distinctes $\alpha_1, \ldots, \alpha_d$. Soit $x_i \in \alpha_i$ l'unique racine de l'équation $X^{q-1} = 1$ appartenant à α_i, alors $x_i^d = 1$ (car le groupe des racines $(q-1)$-ièmes de 1 dans K est isomorphe à :

$$k^* \simeq \mathbf{Z}/(q-1)\,\mathbf{Z}),$$

donc $x_i^n = 1$. Nous avons donc trouvé d racines de $X^n - 1 = 0$, deux à deux distinctes modulo M. Soit x une racine de $X^n = 1$, alors nécessairement x appartient à l'une des classes α_i, soit par exemple α_1. Si $x \neq x_1$, soit $x = x_1(1+y)$, alors $y \in M$ et $y \neq 0$. Or y est solution de l'équation $(1+Y)^n = 1$; comme il est non nul, il satisfait $y^{n-1} + \binom{n}{1} y^{n-2} + \ldots + \binom{n}{2} y + \binom{n}{1} = 0$, ce qui est impossible car $\binom{n}{1} = n \notin M$, et tous les autres termes de l'équation sont dans M. D'où la proposition :

COROLLAIRE 2.4.4. — *Soit* U *le groupe multiplicatif des éléments inversibles de* A :

— *l'ensemble* $1 + M$ *des* $u \in U$ *tels que* $v(u-1) > 0$ *est un sous-groupe ouvert et fermé de* U;

— *l'ensemble* T *des racines* $(q-1)$*-ièmes de* 1 *est un sous-groupe* T *discret cyclique d'ordre* $q-1$;

— U *est produit direct* $U = T \times (1 + M)$.

L'ensemble $1 + M$ est une boule, donc est ouvert et fermé. Soit $a = 1 + u \in 1 + M$, alors :

$$a^{-1} = \lim (1 - u^n)/(1+u) \in 1 + M.$$

Si $a = 1 + u$ et $b = 1 + v \in 1 + M$:

$$ab = 1 + u + v + uv \in 1 + M$$

c'est donc un sous-groupe de U. Enfin, si $a \in U$:

$$a/b(a) \in 1 + M,$$

donc a admet une représentation $a = b(a)(1+u)$ où $b(a) \in T$ et $1 + u \in 1 + M$. Cette représentation est unique car $T \cap 1 + M = \{1\}$.

COROLLAIRE 2.4.5. — *Si* K *est à valuation discrète, le groupe multiplicatif* K^* *est produit direct* $G \times T \times (1 + M)$ *où* G *est le groupe engendré par une uniformisante* m :

$$G = \{m^n \mid n \in \mathbf{Z}\}.$$

Soient en effet $x \in K^*$, $v(x/m^{v(x)/v(m)}) = 0$, donc x admet une représentation $x = m^{v(x)/v(m)}\, a$ où $v(x)/v(m) \in \mathbf{Z}$

et $a \in U$. De plus le produit $K = GU$ est direct car $U \cap G = \{1\}$.

EXERCICE 2.4.6. — L'équation $x^p = 1$ n'a aucune racine autre que 1 dans $\mathbf{Q}_p$.

2.5. POLYNÔMES IRRÉDUCTIBLES

Une importante classe de polynômes irréductibles est décrite par le :

THÉORÈME 2.5.1 (CRITÈRE D'EISENSTEIN). — *Soient* K *un corps valué,* A *l'anneau de valuation,* M *l'idéal maximal de* A *et soit* P *un polynôme unitaire à coefficients dans* A :

$$P(X) = X^n + a_1 X^{n-1} + \ldots + a_n.$$

Si $a_i \in M$ *pour* $i = 1, \ldots, n$ *et* $a_n \notin M^2$, *le polynôme* P *est irréductible dans* K[X].

On appelle POLYNÔMES D'EISENSTEIN les polynômes satisfaisant à ce critère.

LEMME 2.5.2. — *Soient* B *et* C *deux polynômes unitaires dans* K[X] *tels que* $P = BC \in A[X]$, *alors* B *et* C *sont dans* A[X].

Si $B = \Sigma b_i X^i$ est un polynôme, notons :

$$w(B) = \operatorname{Inf} v(b_i).$$

Il est clair que si $a \in K$, $w(aB) = v(a) + w(B)$. Comme B et C sont unitaires, $w(B) \leqslant 0$ et $w(C) \leqslant 0$, soient b et $c \in K$ tels que :

$$v(b) = -w(B) \quad \text{et} \quad v(c) = -w(C)$$

de tels scalaires existent car $w(B)$ est borne inférieure d'un nombre fini d'éléments de $v(K^*)$. Soient $B' = bB$ et $C' = cC$, alors $w(B') = w(C') = 0$, c'est-à-dire que B' et C' sont à coefficients dans A, leurs coefficients n'étant pas tous dans M. Si $Q \in A[X]$, nous noterons $\overline{Q}$ son

image dans $k[X]$. On a alors $P' = bcP = B'C'$, donc $\overline{P}' = \overline{B}'\,\overline{C}'$. Or $\overline{B}'$ et $\overline{C}'$ sont non nuls et $k[X]$ est intègre, donc $\overline{P}'$ est non nul. Supposons par exemple que $B \notin A[X]$, alors $w(B) < 0$ et $b \in M$, alors $P' = bcP$ est à coefficients dans M, et $\overline{P}' = 0$, ce qui est impossible.

Prouvons maintenant le théorème. Supposons que P ne soit pas irréductible : il existe alors B et C unitaires, non constants, à coefficients dans A, tels que $P = BC$. Soient :

$$B(X) = b_0 + b_1 X + \ldots + b_k X^k$$

et :

$$C(X) = c_0 + c_1 X + \ldots + c_h X^h.$$

On a $b_0 c_0 = a_n$: donc, par exemple, $c_0 \in M$ et $b_0 \notin M$. Puis de $a_{n-1} = b_0 c_1 + b_1 c_0$ on déduit que $c_1 \in M$. On montre ainsi de proche en proche que $c_i \in M$ pour $i \leqslant h - 1$. Alors $a_{n-h} - b_0 c_h \in M$, donc $b_0 c_h \in M$. Or $b_0 \notin M$ et C est unitaire, donc $c_h = 1$, d'où le théorème.

REMARQUE. — Bien que cela ne figure pas explicitement dans les hypothèses, ce critère ne peut s'appliquer que si K est à valuation discrète. En effet l'existence de polynômes d'Eisenstein suppose que $M \neq M^2$: on montrera que cette condition équivaut au fait que K soit à valuation discrète.

EXERCICES 2.5. — 1. Pour $p \neq 2$, le polynôme :

$$P(X) = (1 - X^p)/(1 - X) = 1 + \ldots + X^{p-1}$$

est irréductible sur $\mathbf{Q}_p$ (on pourra examiner $P(1 + Y)$).

2. Soit G un groupe noté multiplicativement, on note G^p le sous-groupe constitué des x^p où $x \in G$. On se propose d'étudier $\mathbf{Q}_p^{*p}$ et $\mathbf{Q}_p^*/\mathbf{Q}_p^{*p}$.

a) Si G est produit direct des sous-groupes H_1 et H_2, G^p est produit direct $H_1^p \times H_2^p$.

b) Soient $a = 1 + p^2 b$, $b \in \mathbf{Z}_p$, montrer que l'équation

$$(1 + pX)^p = a$$

a une racine dans $\mathbf{Q}_p$ (on pourra s'inspirer de la méthode employée à l'exercice 1.1).

c) En déduire que, pour $p \neq 2$, $\mathbf{Q}_p^*/\mathbf{Q}_p^{*p} \simeq (\mathbf{Z}/p\mathbf{Z})^2$.

THÉORÈME 2.5.3. *(Lemme de Hensel).* — *Soient* K *un corps valué complet,* $P \in A[X]$ *un polynôme non nul,* $d = dg\, P$. *Supposons qu'il existe deux polynômes unitaires* g *et* h *dans* $A[X]$ *tels que :*

$$\overline{P} = \bar{g}\bar{h}, \quad dg\, g + dg\, h \leqslant d \quad et \quad (\bar{g}, \bar{h}) = 1.$$

Alors il existe G *et* H *dans* $A[X]$ *tels que :*

$$\overline{G} = \bar{g}, \quad \overline{H} = \bar{h}, \quad dg\, G = dg\, g \quad et \quad P = GH.$$

Rappelons que $\overline{P}$ désigne l'image de P dans $k[X]$.

La démonstration de ce théorème est assez longue : elle consiste à construire deux suites g_n et h_n, qui convergent au sens de la convergence simple des coefficients, et telles que $g_n h_n \to P$ pour cette même topologie.

LEMME 2.5.4. — *La fonction* v *définie sur* $K[X]$ *par* $v(\Sigma a_i X^i) = Inf\, v(a_i)$ *est une valuation sur* $K[X]$. *Elle munit* $K[X]$ *d'une topologie pour laquelle le sous-espace* $K[X]_n$ *des polynômes de degré au plus égal à* n *est complet. La topologie induite sur* $K[X]_n$ *est la topologie de la convergence simple des coefficients.*

Pour montrer que v est une valuation, la seule vérification non triviale concerne la relation :

$$v(PQ) = v(P) + v(Q).$$

Remarquons que si $P \neq 0$, il existe un scalaire $a \in K$ tel que $v(aP) = 0$. De plus, pour tout P et tout scalaire $a \in K$, $v(aP) = v(a) + v(P)$. Il suffit donc de montrer que V2 est satisfaite pour $v(P) = v(Q) = 0$. Or $v(P) = 0$ équivaut à « $P \in A[X]$ et $\overline{P} \neq 0$ ». Donc si :

$$v(P) = v(Q) = 0, \quad \overline{P} \neq 0 \quad et \quad \overline{Q} \neq 0,$$

donc $$\overline{PQ} \neq 0 \quad et \quad v(PQ) = 0.$$

On peut aussi remarquer que la relation V2 résulte du lemme 2.5.2.

La valuation v se prolonge au corps $K(X)$, elle en fait un corps valué, et la topologie induite sur $K[X]$ est la topologie définie par v. Soit P_k une suite de polynômes de degré au plus n convergeant vers un polynôme P : cela signifie que $v(P_k - P) \to +\infty$. Si $P = \Sigma a_i X^i$ et $P_k = \Sigma a_{ik} X^i$, cela équivaut encore à : pour $i = 0, \ldots, n$, $v(a_{ik} - a_i) \to +\infty$. Ceci montre que la topologie induite sur $K[X]_n$ est aussi la topologie de la convergence simple des coefficients. Or $K[X]_n$ est complet pour cette topologie, puisque isomorphe, comme espace vectoriel topologique, à K^{n+1}.

Soient g et h satisfaisant aux hypothèses du théorème, en particulier $(\bar{g}, \bar{h}) = 1$. Alors $\bar{g}k[X] + \bar{h}k[X] = k[X]$, c'est-à-dire qu'il existe $\bar{u}$ et $\bar{v}$ dans $k[X]$ tels que $dg\, \bar{u} < dg\, \bar{h}$, $dg\, \bar{v} < dg\, \bar{g}$, $\bar{u}\bar{g} + \bar{v}\bar{h} = 1$ (identité de Bezout). Nous choisissons, une fois pour toutes, $u \in \bar{u}$ et $v \in \bar{v}$ dans $A[X]$ avec $dg\, u < dg\, g$ et $dg\, v < dg\, h$, et nous posons :

$$\mu = v(ug + vh - 1);$$

alors $\mu > 0$ car l'image de $ug + vh - 1$ dans $k[X]$ est nulle.

LEMME 2.5.5 *(Continuité de la division euclidienne).* — *Soient* l *un polynôme unitaire à coefficients dans* A *et* $Q \in K[X]$. *L'unique couple* q, r *de polynômes satisfaisant* $Q = ql + r$ *et* $dg\, r < dg\, l$ *satisfait de plus à* $v(q) \geqslant v(Q)$ *et* $v(r) \geqslant v(Q)$.

Si Q est nul, q et r aussi, et les inégalités sont triviales. Sinon il existe $b \in K$ tel que $v(bQ) = 0$, et il suffit de montrer les inégalités $v(q) \geqslant 0$ et $v(r) \geqslant 0$ lorsque $v(Q) = 0$. Or, si $v(Q) = 0$, $Q \in A[X]$, le polynôme l étant unitaire on voit que l'algorithme de division euclidienne donne pour q et r des coefficients dans A.

LEMME 2.5.6. — *Soit* Q *un polynôme tel que :*

$$dg\, Q < dg\, g + dg\, h.$$

Il existe deux polynômes U *et* V *tels que :*

$$v(Ug + Vh - Q) \geqslant \mu + v(Q)$$

avec : $v(U) \geqslant v(Q)$, $v(V) \geqslant v(Q)$,
$dg\,U < dg\,h$ *et* $dg\,V < dg\,g$.

Soient en effet :

$R = ug + vh - 1$, $\mu = v(R)$ et $dg\,R < dg\,g + dg\,h$.

Soient $uQ = u'h + U$ et $vQ = v'g + V$ les identités de division euclidienne de uQ et vQ par h et g respectivement : alors $v(U)$, $v(V)$, $v(u')$ et $v(v')$ sont minorés par $v(Q)$. On a :

$$RQ = (u' + v')\,gh + Ug + Vh - Q.$$

Or, $dg(Ug + Vh - Q) < dg\,g + dg\,h$, donc :

$$Ug + Vh - Q$$

est le reste de la division euclidienne de RQ par gh. Il satisfait donc $v(Ug + Vh - Q) \geqslant v(RQ) = v(R) + v(Q)$.

COROLLAIRE 2.5.7. — *Soit* $Q \in K[X]$, *il existe deux polynômes* U *et* V *tels que :*

$$v(Ug + Vh - Q) \geqslant \mu + v(Q)$$

avec :

$$dg\,V < dg\,g, \quad dg\,U < Max\,(dg\,h, dg\,Q - dg\,g),$$
$$v(U) \geqslant v(Q) \quad et \quad v(V) \geqslant v(Q).$$

Soit en effet $Q = qgh + Q_1$ l'identité de division euclidienne de Q par gh, soient U_1 et V_1 satisfaisant aux conclusions du lemme 2.5.6 appliqué à Q_1 : on vérifie que $U = U_1 + qh$ et $V = V_1$ satisfont les conditions annoncées.

LEMME 2.5.8. — *Soient* $\lambda = v(P - gh)$ *et* $\nu = Inf\,(\lambda, \mu)$, *il existe deux suites* g_n *et* h_n *de polynômes telles que* $g_0 = g$, $h_0 = h$ *et, pour* $n \geqslant 1$:

(i)$_n$ $v(P - g_n h_n) \geqslant (n+1)\,\nu$;
(ii)$_n$ $v(g_n - g_{n-1}) \geqslant n\nu$, $v(h_n - h_{n-1}) \geqslant n\nu$, $dg\,g_n = dg\,g$, $dg\,h_n \leqslant dg\,P - dg\,g$.

PREUVE. — Soit $P_1 = P - gh$, en appliquant le lemme 2.5.7 à P_1, on obtient deux polynômes U_1 et V_1 tels que :

$$dg\,V_1 < dg\,g, \quad dg\,U_1 < dg\,P - dg\,g, \quad v(U_1) \geqslant \nu,$$
$$v(V_1) \geqslant \nu \quad et \quad v(U_1 g + V_1 h - P) \geqslant 2\nu.$$

Alors $g_1 = g + V_1$ et $h_1 = h + U_1$ satisfont les conditions (i)$_1$ et (ii)$_1$.

Supposons que $g_1, \ldots, g_n$ et $h_1, \ldots, h_n$ satisfassent les conditions (i)$_k$ et (ii)$_k$ pour $k \leqslant n$. Soient $P_{n+1} = P - g_n h_n$, U_{n+1} et V_{n+1} deux polynômes satisfaisant au corollaire 2.5.7 pour $Q = P_{n+1}$, et posons $g_{n+1} = g_n + V_{n+1}$ et $h_{n+1} = h_n + U_{n+1}$: alors les conditions (ii)$_{n+1}$ sont satisfaites. De plus :

$$\begin{aligned} P - g_{n+1}h_{n+1} &= P_{n+1} - h_n V_{n+1} - g_n U_{n+1} + U_{n+1}V_{n+1} \\ &= (P_{n+1} - hV_{n+1} - gU_{n+1}) \\ &\quad + (h - h_n)\,V_{n+1} + (g - g_n)\,U_{n+1} \\ &\quad + U_{n+1}V_{n+1}. \end{aligned}$$

Or, la valuation de chacun des termes de la dernière somme est au moins égale à $(n+2)\,\nu$, donc la condition (i)$_{n+1}$ est satisfaite.

PREUVE DU THÉORÈME 2.5.3. — Chacune des suites g_n et h_n converge, coefficient par coefficient, vers deux polynômes G et H. On a $dg\,H \leqslant dg\,P - dg\,g$, $dg\,G = dg\,g$ (car, pour tout n, le terme de plus haut degré de g_n a un coefficient appartenant à $1 + M$). On voit de plus, en appliquant l'inégalité ultramétrique, que $v(G - g_n) \geqslant n\nu$ et $v(H - h_n) \geqslant n\nu$. Or :

$$P - GH = P - g_n h_n + (g_n - G)\,h_n + (h_n - H)\,G,$$

donc, pour tout n, $v(P - GH) \geqslant n\nu$, et $P = GH$.

COROLLAIRE 2.5.9. — *Soit* $P \in \mathbf{Z}_p[X]$, *supposons qu'il existe* $\bar{a} \in \mathbf{F}_p$ *tel que* $\bar{P}(\bar{a}) = 0$ *et* $\bar{P}'(\bar{a}) \neq 0$; *alors il existe* $a \in \mathbf{Z}_p$, $a \in \bar{a}$, *tel que* $P(a) = 0$ (cf. exercice 1.1).

Soit en effet $b \in \bar{a}$:

$$g(X) = X - b \quad \text{et} \quad h(X) = (P(X) - P(b))/(X - b)$$

on vérifie que P, g et h satisfont les hypothèses du lemme de Hensel, alors $P = GH$ où $G(X) = uX + c$ et $\bar{G} = \bar{g}$, donc $G(X) = u(X - a)$ avec $a \in \bar{a}$.

COROLLAIRE 2.5.10. — *Soit* $P \in K[X]$ *un polynôme irréductible et unitaire tel que* $P(0) \in A$, *alors* $P \in A[X]$.

Soit en effet $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, $a_0 \in A$. Supposons que $v(P) < 0$, et soient i et j tels que $v(a_k) \geqslant 0$ pour $k > i$ ou $k < j$, $v(a_i) = v(a_j) = v(P)$, alors $0 < j \leqslant i < n$. Soient :

$$Q = a_i^{-1}P, \quad Q(X) = b_n X^n + \ldots + b_0,$$

alors :

$$\bar{Q} = X^j(\bar{b}_j + \ldots + X^{i-j}), \quad \text{où} \quad \bar{b}_j \neq 0.$$

Soient $g(X) = X^j$ et $h(X) = b_j + \ldots + X^{i-j}$, alors $(\bar{g}, \bar{h}) = 1$, et il existe G et H tels que $Q = GH$, avec $\deg G = j$, $j \neq 0, n$. Donc Q n'est pas irréductible, et P non plus.

Remarquons que, tant pour le lemme de Hensel que pour ses corollaires, il est essentiel de supposer K complet. On trouve en effet aisément des contre-exemples aux énoncés ci-dessus si on ne suppose plus K complet. Par exemple, soient $p \neq 2$ et $\mathbf{Q}$ muni de la topologie p-adique. Le polynôme :

$$P(X) = X^2 + 2/p\,X - 1 = (X + 1/p)^2 - (1 + p^2)/p^2$$

est irréductible sur $\mathbf{Q}$ car $1 + p^2 \equiv 2 \bmod 4$, donc $1 + p^2$ ne peut pas être un carré dans $\mathbf{Q}$. Par contre P n'est pas irréductible sur $\mathbf{Q}_p$ puisque $P(0) = 1 \in \mathbf{Z}_p$ mais $P \notin \mathbf{Z}_p[X]$ (exercice : montrer « directement » que $1 + p^2$ est un carré dans $\mathbf{Q}_p$).

Nous disposons donc d'un critère d'irréductibilité (Eisenstein) et d'un critère de réductibilité (Hensel) : évidemment, ces deux critères ne sont pas suffisants pour déterminer tous les polynômes irréductibles (cf. en particulier la proposition 2.6.8) : ils sont cependant précieux pour beaucoup d'applications.

2.6. EXTENSIONS ALGÉBRIQUES FINIES D'UN CORPS ULTRAMÉTRIQUE

Soient K un corps valué ultramétrique et L une extension algébrique finie de K, $n = [L : K]$. Nous noterons B la clôture intégrale de A dans L, c'est-à-dire l'ensemble des éléments $x \in L$ satisfaisant une équation $P(x) = 0$ où P est un polynôme unitaire, $P \in A[X]$. On appelle aussi B l'anneau des ENTIERS de L. Soit $x \in L$, nous noterons $N_{L/K}(x)$ (ou $N(x)$ si aucune confusion n'est à craindre) le déterminant de l'endomorphisme du K-espace vectoriel L défini par la multiplication par x. Le polynôme caractéristique de cet endomorphisme :

$$X^n + \ldots + (-1)^n N(x)$$

est annulé par x. C'est une puissance du polynôme minimal de x sur K, on l'appelle polynôme normal de x dans L. Il est équivalent de dire que x est un entier de L ou que son polynôme normal est à coefficients dans A. On vérifiera que $A = B \cap K$: on appelle aussi entiers de K les éléments de A.

PROPOSITION 2.6.1. — *Soient* K *un corps valué ultramétrique complet et* L *une extension algébrique de degré* n *de* K, *la relation :*

$$w(x) = 1/n\, v(N_{L/K}(x))$$

définit l'unique valuation w *de* L *prolongeant la valuation* v *de* K.

Remarquons d'abord que w prolonge v : si $x \in K$, $N(x) = x^n$, donc $w(x) = (1/n)\, nv(x) = v(x)$.

Nous devons donc montrer que w est une valuation, et que c'est la seule qui prolonge v.

LEMME 2.6.2. — *Soient :*

$$Q \in K[X], \quad Q(X) = X^d + \ldots + a_d,$$

si $v(a_d) > 0 = \underset{1 \leqslant i \leqslant d-1}{Inf} \{v(a_i)\}$, *Q n'est pas irréductible.*

La démonstration est tout à fait analogue à celle de 2.5.10.

LEMME 2.6.3. — *Soit w une valuation de* L *prolongeant v, alors* B *est contenu dans l'anneau de la valuation w.*

Soit en effet $x \in B$, il satisfait une équation :

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \quad a_i \in A.$$

Donc :

$$w(x^n) = nw(x) \geqslant \mathrm{Inf}\,(v(a_1) + (n-1)\,w(x), \ldots, v(a_n)) \geqslant \mathrm{Inf}\,(0, (n-1)\,w(x)),$$

d'où $w(x) \geqslant 0$.

LEMME 2.6.4. — *Soient w une valuation prolongeant v et* $x \in B$ *tel que* $x^{-1} \notin B$, *alors* $w(x) > 0$.

Soit en effet $P(X) = X^d + \ldots + a_d$ le polynôme minimal de x sur K, $P \in A[X]$ puisque $x \in B$. Si $v(a_d) = 0$, le polynôme réciproque $Q(X) = X^d a_d^{-1} P(1/X)$ est le polynôme minimal de x^{-1}, et il est à coefficients dans A. Donc si $x^{-1} \notin B$, $v(a_d) > 0$. Or P est irréductible, alors $v(a_i) > 0$ pour $i = 1, \ldots, d-1$ (lemme 2.6.2). De $P(x) = 0$ et $w(x) \geqslant 0$ on déduit :

$$dw(x) \geqslant \mathrm{Inf}\,(v(a_1), \ldots, v(a_d)) > 0, \quad \text{d'où} \quad w(x) > 0.$$

COROLLAIRE 2.6.5. — *Pour toute valuation w prolongeant v,* B *est l'anneau de valuation. Il existe au plus une valuation sur* L *prolongeant v.*

Soit w prolongeant v : nous avons vu que B est contenu dans l'anneau de valuation, et que :

$$x^{-1} \notin B \Rightarrow w(x) > 0 \Rightarrow x^{-1}$$

n'est pas dans l'anneau de valuation. Or si $x \in K$, x ou $x^{-1} \in B$: soit en effet $P(X) = X^d + \ldots + a_d$ le polynôme minimal de x. Si $P \in A[X]$, $x \in B$, sinon, $a_d \notin A$ (corollaire 2.5.10), alors le polynôme réciproque :

$$Q(X) = a_d^{-1} X^d P(1/X)$$

est irréductible, unitaire, et $Q(0) = a_d^{-1} \in A$, donc :

$$Q \in A[X] \quad \text{et} \quad x^{-1} \in B.$$

Si B′ est l'anneau de valuation de w on a donc $B \subseteq B'$ (2.6.3) et $\mathfrak{C}B \subseteq \mathfrak{C}B'$ (2.6.4), d'où $B = B'$. Donc deux valuations w et w' prolongeant v ont même anneau de valuation : elles sont équivalentes, donc proportionnelles, mais elles coïncident sur K, donc elles sont égales.

LEMME 2.6.6. — *La fonction* $w(x) = 1/n\, v(N(x))$ *est une valuation sur* L.

En effet, $w(x) = +\infty$ équivaut à $N(x) = 0$, ce qui signifie que la multiplication par x est un endomorphisme non inversible du K-espace vectoriel L, donc que $x = 0$.

Il est clair, par définition, que $N(xy) = N(x)\,N(y)$, donc $w(xy) = w(x) + w(y)$.

Reste à prouver l'inégalité triangulaire : elle est triviale si x ou y est nul. Supposons $xy \neq 0$, et, par exemple, $w(y) \geqslant w(x)$. Soit $z = y/x$, alors :

$$w(x+y) = w(x) + w(1+y/x),$$

il suffit donc de montrer que $w(1+y/x) \geqslant 0$. Or $N(z) = N(y)/N(x) \in A$, car $v(N(y)) \geqslant v(N(x))$. Soit :

$$P(X) = X^d + \ldots + a_d$$

le polynôme minimal de z, alors $N(z) = \pm a_d^{n/d}$ (car le polynôme normal de z est $P^{n/d}$). Donc si $N(z) \in A$, $a_d \in A$. Alors, d'après 2.5.10, $P \in A[X]$, donc $z \in B$, alors $1 + z \in B$, $N(1+z) \in A$, et $w(1+z) \geqslant 0$, ce qui achève la démonstration.

REMARQUES. — 1. Si on suppose K localement compact, la preuve de l'unicité du prolongement est plus simple. En effet L n'a qu'une topologie de K-espace vectoriel, or une valuation prolongeant v munit L d'une telle topologie : donc deux prolongements w et w' de v sont équivalents, et égaux puisqu'ils coïncident sur K.

2. Si on ne suppose pas que K soit complet, il n'y a plus unicité du prolongement : on s'en convaincra par exemple en relisant le § 1.8.

Nous noterons désormais v l'unique prolongement de v à L. Par définition, $v(L^*) \subseteq 1/n\, v(K^*)$. Si $\Gamma = v(K^*)$ est discret, $\Gamma \subseteq v(L^*) \subseteq 1/n\Gamma$ entraîne que Γ est un sous-groupe de $v(L^*)$, d'indice fini. Soit e cet indice : $e \mid n$.

DÉFINITION 2.6.7. — *L'indice e de $v(K^*)$ dans $v(L^*)$ s'appelle* INDICE DE RAMIFICATION *de* L *sur* K. *On appelle* DEGRÉ RÉSIDUEL *de* L *sur* K *le quotient $f = n/e$. On dit que* L *est* TOTALEMENT RAMIFIÉE *si $e = n$ et* NON RAMIFIÉE *si $e = 1$.*

Les extensions totalement ramifiées sont décrites par la :

PROPOSITION 2.6.8. — *Soit* K *un corps ultramétrique complet à valuation discrète.*

(i) *Soit* P *un polynôme d'Eisenstein de* K[X], P *définit une extension totalement ramifiée* L *de* K *et une racine x de* P *dans* L *est une uniformisante de* L.

(ii) *Soient* L *une extension totalement ramifiée de degré n de* K *et x une uniformisante de* L, *le polynôme normal de x dans* L *est un polynôme d'Eisenstein, et x est de degré n.*

Soit $a > 0$ un générateur de $v(K^*)$, $v(K^*) = a\mathbf{Z}$. Soient P un polynôme d'Eisenstein et $n = \deg P$. P définit une extension L de K, $[L : K] = n$. Soit x une racine de P dans L, P est le polynôme normal de x dans L, donc $N(x) = (-1)^n P(0)$, et $v(x) = (1/n)\, v(P(0)) = a/n$, $v(L^*) = v(K^*)/n$, et $v(x)$ engendre $v(L^*)$, d'où l'assertion (i).

Réciproquement, si L est totalement ramifiée de degré n, soit x une uniformisante, alors $v(x) = a/n$. Soit :

$$P(X) = X^n + \ldots + a_n$$

le polynôme normal de x dans L, alors P est irréductible. En effet si $L' \subseteq L$ est le sous-corps de L engendré par x et n' son degré, $n' \mid n$ et $v(x) \in v(L'^*) \subseteq v(K^*)/n'$, donc $n' = n$, P est le polynôme minimal de x. Or $|a_n| = |N(x)|$, donc $v(a_n) = a$. Il en résulte que $v(a_i) \geqslant a$ pour $i = 1, \ldots, n-1$ (lemme 2.6.2), P est un polynôme d'Eisenstein.

EXEMPLE. — Soit L l'extension de $\mathbf{Q}_p$ par les racines p-ièmes de l'unité : L est définie par le polynôme irréductible $Q(X) = (X^p - 1)/(X - 1)$. Or $Q(1 + Y)$ est un polynôme d'Eisenstein, donc L est totalement ramifiée de degré $p - 1$. Si x est une racine primitive p-ième de 1, $x - 1$ est une uniformisante de L et $v(x - 1) = 1/p - 1$.

EXERCICE 2.6.9. — Soit $n \geqslant 1$, L_n l'extension de $\mathbf{Q}_p$ par les racines p^n-ièmes de 1. L_n est totalement ramifiée de degré $p^{n-1}(p-1)$. Si x est une racine primitive p^n-ième de 1, $v(x-1) = 1/p^{n-1}(p-1)$.

PROPOSITION 2.6.10. — *Soient* K *un corps valué ultramétrique complet et* $\widetilde{K}$ *une clôture algébrique de* K. *Il existe sur* $\widetilde{K}$ *une unique valuation prolongeant la valuation v de* K, *soit encore v ce prolongement. Si $x \in \widetilde{K}$ et si* L *est un sous-corps de* $\widetilde{K}$ *tel que $x \in L$ et $[L : K] = n$, $v(x) = 1/n\, v(N_{L/K}(x))$. Le groupe de valuation, $v(\widetilde{K}^*)$, est contenu dans $v(K^*) \otimes_{\mathbf{Z}} \mathbf{Q}$. Si $v(K^*)$ est discret alors $v(\widetilde{K}^*) = v(K^*) \otimes_{\mathbf{Z}} \mathbf{Q}$.*

Il est clair qu'il existe au plus une valuation sur $\widetilde{K}$ prolongeant v : $\widetilde{K}$ est réunion d'extensions finies de K, et sur chaque extension finie le prolongement est unique. Si L' et L sont deux extensions finies de K telles que $L' \supset L \supset K$, le prolongement de v à L' induit sur L une valuation prolongeant v : il induit donc sur L l'unique valuation prolongeant v. Donc la valeur $v(x)$ introduite dans la proposition ne dépend que de x et non du corps $L \ni x$ choisi. La fonction v ainsi définie sur $\widetilde{K}$ est une

valuation, car si x et $y \in \widetilde{K}$, il existe une extension finie L de K contenant x et y, donc $v(xy) = v(x) + v(y)$ et $v(x+y) \geqslant \mathrm{Inf}\,(v(x), v(y))$.

Rappelons que $v(K^*) \underset{\mathbf{Z}}{\otimes} \mathbf{Q} = \{ar \mid a \in \mathbf{Q} \text{ et } r \in v(K^*)\}$. Il est donc évident que, pour tout $x \in \widetilde{K}$:

$$v(x) \in \widetilde{\Gamma} = v(K^*) \underset{\mathbf{Z}}{\otimes} \mathbf{Q}.$$

Supposons maintenant que $\Gamma = v(K^*)$ soit discret. Alors, pour tout n, il existe un polynôme d'Eisenstein de degré n : donc il existe un $x \in K$ tel que $v(x) = a/n$, où a est un générateur positif de Γ. Alors $v(\widetilde{K}^*)$ est un sous-groupe de $\mathbf{R}$, contenu dans $\widetilde{\Gamma}$, et contenant Γ/n pour tout n, donc $v(\widetilde{K}^*) = \widetilde{\Gamma}$.

COROLLAIRE 2.6.11. — *La clôture algébrique de $\mathbf{Q}_p$ n'est pas localement compacte.*

En effet, son groupe de valuation est $\mathbf{Q}$, qui n'est pas discret dans $\mathbf{R}$.

PROPOSITION 2.6.12. — *Soient* K *un corps valué complet à valuation discrète,* L *une extension finie de* K, $n = [L : K]$. *L'anneau* B *des entiers de* K *est un* A*-module libre de rang* n.

Nous noterons $\mathscr{B}$ l'ensemble des bases $X = (x_1, \ldots, x_n)$ du K-espace vectoriel L. Si $X \in \mathscr{B}$ et $Y \in \mathscr{B}$, $D(Y/X)$ désigne le déterminant de Y sur X : soit $Y_i = \Sigma a_{ij} x_j$, $D(Y/X)$ est le déterminant des (a_{ij}). Pour X et $Y \in \mathscr{B}$, $D(Y/X) \in K^*$. Nous noterons A(Y) le A-module engendré par $y_1, \ldots, y_n$. Si $Y \in \mathscr{B}$, $A(Y) = y_1 A \oplus \ldots \oplus y_n A$. Enfin $\mathscr{B}'$ désignera l'ensemble des bases dont les éléments sont des entiers de L, $\mathscr{B}' = \mathscr{B} \cap B^n$.

LEMME 2.6.13. — *Soient* X *un élément fixé de* $\mathscr{B}$, $w = \underset{Y \in \mathscr{B}'}{Inf}\, v(D(Y/X))$. *Si* $Y \in \mathscr{B}'$ *est tel que* $v(D(Y/X)) = w$, *alors* $B = A(Y)$.

Il est clair que si $Y \in \mathscr{B}'$, $A(Y) \subseteq B$. Supposons que $A(Y) \neq B$ et soit $b \in B - A(Y)$. Alors :

$$b = b_1 y_1 + \ldots + b_n y_n$$

où $b_i \in K$, et l'un au moins des b_i n'est pas dans A. Si, par exemple, $b_1 \notin A$, soit $Y' = (b, y_2, \ldots, y_n)$, alors $Y' \in \mathscr{B}'$, et $D(Y'/Y) = b_1$, donc :

$$D(Y'/X) = D(Y'/Y)\, D(Y/X) = b_1 D(Y/X)$$

et : $$v(D(Y'/X)) < v(D(Y/X))$$

ceci est impossible si $v(D(Y/X)) = w$, d'où le lemme.

Pour prouver la proposition, il suffit de montrer qu'il existe $Y \in \mathscr{B}'$ qui rende $v(D(Y/X))$ minimum : comme $v(K^*)$ est discret, il suffit de voir que $\{v(D(Y/X))\}$ où $Y \in \mathscr{B}'$ est minoré. Pour $Y \in K^n$, posons $||Y|| = \mathrm{Max}\,|y_i|$. On vérifie aisément que $d(Y, Z) = ||Y - Z||$ définit une distance sur K^n, pour laquelle l'application $Y \to D(Y/X)$ est uniformément continue. Or B^n est une partie bornée pour cette distance, donc l'image de $\mathscr{B}'$ est une partie bornée de K, d'où la proposition.

COROLLAIRE 2.6.14. — *Soient* K *un corps valué complet à valuation discrète,* L *une extension finie de* K, $n = [L : K]$, *e l'indice de ramification et* $f = n/e$ *le degré résiduel. Le corps résiduel* l *de* L *est extension algébrique de degré* f *du corps résiduel* k *de* K.

Soient A, M, a (resp. B, M, b) l'anneau de valuation, l'idéal de valuation et une uniformisante de K (resp. L). On a $v(a) = ev(b)$, $M = aA$, $N = bB$, donc :

$$N^e = b^e B = aB.$$

Il est clair que l est un k-espace vectoriel. Comme B est un A-module libre de rang n, B/aB est un A/aA-module libre de rang n. Donc $B/aB = B/N^e = l^e \simeq k^n$ en tant que k-espaces vectoriels. Il en résulte que $l \simeq k^{n/e} = k^f$. Or, si un corps l est un espace vectoriel de dimension finie f sur k, l est extension algébrique de degré f de k.

Cette propriété est évidemment à l'origine du terme « degré résiduel ».

COROLLAIRE 2.6.15. — *Soient* K *un corps valué complet localement compact et* $n \geqslant 1$, *il existe une extension* L *de* K, *non ramifiée et de degré* n.

Il suffit de montrer qu'il existe une extension L de degré n dont le corps résiduel est de degré n. Si P est un polynôme unitaire et $P \in A[X]$, supposons que $\overline{P}$ soit irréductible, alors P est irréductible : en effet si $P = GH$ où G et H sont des polynômes non constants, $\overline{P} = \overline{G}\,\overline{H}$ et $\overline{G}$, $\overline{H}$ sont non constants car :

$$\operatorname{dg} \overline{P} = \operatorname{dg} P = \operatorname{dg} G + \operatorname{dg} H = \operatorname{dg} \overline{G} + \operatorname{dg} \overline{H}$$

et : $$\operatorname{dg} \overline{G} \leqslant \operatorname{dg} G, \quad \operatorname{dg} \overline{H} \leqslant \operatorname{dg} H,$$

donc $\operatorname{dg} \overline{G} = \operatorname{dg} G$ et $\operatorname{dg} \overline{H} = \operatorname{dg} H$. Soient L l'extension de K définie par un tel P, et a une racine de P dans L, alors $\bar{a}$ est racine de l'équation de degré $n = \operatorname{dg} P$, $\overline{P}(\bar{a}) = 0$ et cette équation est irréductible sur k, donc $\bar{a}$ est de degré n sur k et le degré de l sur k est n. Le corps k est fini, il suffit donc de savoir que si k est fini il existe un polynôme irréductible de degré n dans $k[X]$. Or, si $q = \operatorname{card} k$, il existe un corps l, unique à isomorphisme près, ayant q^n éléments. En particulier il existe un tel l dans la clôture algébrique de k : c'est alors une extension algébrique de k de degré n, et si b est un générateur du groupe multiplicatif de l le polynôme minimal de b sur k est de degré n (pour les démonstrations des propriétés des corps finis que nous utilisons, voir, par exemple, [9], chap. 1).

COROLLAIRE 2.6.16. — *Le corps résiduel de la clôture algébrique d'un corps valué complet* K *est la clôture algébrique du corps résiduel de* K.

Soient $\widetilde{K}$, $\widetilde{A}$ et $\widetilde{M}$ la clôture algébrique de K, son anneau et son idéal de valuation. Soient $\bar{k} = \widetilde{A}/\widetilde{M}$ et $\tilde{k}$ la clôture algébrique de k. Si $x \in \widetilde{A}$, il existe un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$, alors $\overline{P}(\bar{x}) = 0$, et $\overline{P} \neq 0$, donc $\bar{x}$ est algébrique sur k : $\bar{k}$ est extension algébrique de k. Soit $\overline{P} \in k[X]$ un polynôme irréductible, et soit P unitaire, $P \in \overline{P}$, alors P a une racine dans $\widetilde{K}$, soit x et $\overline{P}(\bar{x}) = 0$, donc $\overline{P}$ a une racine dans $\bar{k}$. Alors $\bar{k}$ est une extension algébrique de k dans laquelle tout polynôme à coefficients dans k a une racine : $\bar{k} \simeq \tilde{k}$.

2.7. CORPS VALUÉS COMPLETS ALGÉBRIQUEMENT CLOS

Nous avons montré que si K est un corps valué complet, sa clôture algébrique $\widetilde{K}$ est canoniquement munie d'une structure de corps valué pour laquelle nous connaissons le corps résiduel, et le groupe de valuation si K est à valuation discrète. Généralement $\widetilde{K}$ n'est pas complet (cf. exercice 2.7.4). Soit L le complété de $\widetilde{K}$: nous ne savons pas si L est ou non algébriquement clos. Le théorème suivant nous permet de répondre affirmativement.

THÉORÈME 2.7.1 *(Lemme de Krasner).* — *Soient* K *un corps valué complet de caractéristique nulle, a un élément algébrique sur* K, $a = a_1, a_2, \ldots, a_n$ *les conjugués de a sur* K. *Soit b algébrique sur* K *tel que, pour* $i = 2, \ldots, n$:

$$v(b - a) > v(b - a_i) \quad \text{et} \quad [K(b) : K] \leqslant n,$$

alors les extensions de K *par a et b coïncident.*

Rappelons que, si K est une clôture algébrique de K, les conjugués de a sont les racines dans K du polynôme minimal P de a sur K. Si K est de caractéristique 0, des éléments conjugués sont deux à deux distincts car, P étant irréductible, $P' \neq 0$, $(P, P') = 1$. On a noté $K(b)$ le plus petit sous-corps de K contenant K et b : son degré sur K est le degré de b. Soit $L = K(b)$, L est une exten-

sion finie de K, c'est donc un corps valué complet. D'autre part a est algébrique sur L. Soit :

$$P(X) = (X - a_1)(X - a_2) \dots (X - a_n)$$

le polynôme minimal de a sur K et Q le polynôme minimal de a sur L, alors $Q \mid P$. Soit $s = \deg Q$, et supposons que $a_1, a_2, \dots, a_s$ soient les conjugués de a sur L (c'est-à-dire celles parmi les racines de P dans K qui sont racines de Q). Alors $Q(b + Y)$ est irréductible dans $L[Y]$ et ses racines dans K sont $y_1, \dots, y_s$ où $y_i = a_i - b$. Pour $i = 1, \dots, s$, $v(y_i) = 1/s\ v(Q(b))$. Si $s > 1$, on a donc :

$$v(a_s - b) = v(a - b),$$

ce qui est incompatible avec les hypothèses. Donc $s = 1$, et $a \in L$, or nous savons que $K(a)$ est de degré n, L de degré $\leqslant n$, donc $L = K(a)$.

COROLLAIRE 2.7.2. — *Soient* K *un corps valué complet de caractéristique* 0, P *un polynôme unitaire irréductible dans* K[X]. *Il existe une constante* M(P) *telle que tout polynôme* Q *unitaire de degré n satisfaisant* $v(Q - P) \geqslant M(P)$ *soit irréductible et ait une racine dans l'extension de* K *par* P.

Soient $a_1, \dots, a_n$ les racines de P dans K et soit $r = \mathrm{Inf}\,(v(a_i - a_j))$, la borne inférieure étant prise sur les couples $i \neq j$. Soient Q unitaire de degré n et $b_1, \dots, b_n$ les racines de Q dans $\widetilde{K}$, comptées avec leur multiplicité. Posons $D = \prod_i Q(a_i) = \prod_{i,j} (a_i - b_j)$, où $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$. Si $v(D) > n^2 r$, il existe un couple (i, j) tel que $v(a_i - b_j) > r$. On peut alors appliquer le lemme de Krasner à $a = a_i$ et $b = b_j$, alors $K(a_i) = K(b_j)$, donc Q est irréductible et a une racine dans :

$$K(a) = K[X]/PK[X].$$

Soit E l'espace des polynômes unitaires de degré n, muni de la topologie induite par v : alors D est une fonction continue du couple $(P, Q) \in E^2$, car c'est un polynôme par rapport aux coefficients de P et Q. Or :

$$D(P, P) = 0,$$

il existe donc un voisinage de P dans E :

$$V(P) = \{Q \in E \mid v(Q - P) \geqslant M(P)\}$$

tel que pour $Q \in V(P)$, $v(D) > n^2 r$.

On appelle parfois ce corollaire « lemme de continuité des racines » : il signifie en effet que si Q est assez proche de P, pour la topologie de la convergence simple des coefficients, il existe une racine b de Q « proche » d'une racine a de P.

COROLLAIRE 2.7.3. — *Le complété d'un corps valué algébriquement clos de caractéristique* 0 *est algébriquement clos.*

Soient en effet K algébriquement clos, K′ son complété, et soit P un polynôme irréductible et unitaire dans K′[X]. Comme K est dense dans K′, il existe Q unitaire de même degré n que P satisfaisant $v(Q - P) \geqslant M(P)$, alors Q est irréductible sur K′ : il est *a fortiori* irréductible sur K. Comme K est algébriquement clos, $\deg Q = 1 = \deg P$, et K′ est algébriquement clos.

On voit que le complété de la clôture algébrique d'un corps valué complet de caractéristique nulle est algébriquement clos : nous noterons $\mathbf{C}_p$ le complété de la clôture algébrique de $\mathbf{Q}_p$; nous verrons que, dans la théorie des fonctions analytiques p - adiques, $\mathbf{C}_p$ a un rôle analogue à celui de $\mathbf{C}$ dans la théorie usuelle. Remarquons que $\mathbf{C}$ est aussi complété de la clôture algébrique de $\mathbf{Q}$, pour la topologie réelle.

EXERCICES 2.7.4. — 1. On se propose de montrer que la clôture algébrique $\widetilde{\mathbf{Q}}_p$ de $\mathbf{Q}_p$ n'est pas complète. Soient $\mathbf{C}_p$ le complété de $\widetilde{\mathbf{Q}}_p$, q un entier tel que $(q, p) = 1$ et $q > p$, on suppose $p \neq 2$.

a) Soient Y_n une racine primitive n-ième de 1, $u_n = Y_n^{q^n}$, $s_n = u_1 + \dots + u_n$, s la limite de s_n dans $\mathbf{C}_p$, $r_n = s - s_n$. Evaluer $v(r_n)$.

b) Montrer que pour $a_0, \dots, a_k \in \mathbf{Z}_p$ et pour n assez grand en fonction de k :

$$v(a_0 + a_1 s_n + \dots + a_k s_n^k) = \mathrm{Inf}\,(v(a_i) + iv(s_n)) \leqslant v(a_0).$$

c) En déduire que si :

$$P(X) = b_0 + \ldots + b_k X^k \in Z_p[X], \quad v(P^i(s_n)/i!) \leqslant v(b_i).$$

En utilisant la formule de Taylor, montrer que $P(s) \neq 0$.

d) S'inspirer de l'exemple ci-dessus pour énoncer un critère de transcendance sur Q_p pour les éléments de C_p.

e) Montrer, à l'aide du théorème de Baire, que $\widetilde{Q}_p$, étant réunion dénombrable de fermés d'intérieur vide, n'est pas complet.

2. Si $a \in Q_p$, on pose $P_a(X) = X^p - a$, $p \neq 2$.

a) Si $v(a-1) = 1$, P_a est irréductible sur Q_p.

b) Si $v(a-1) = v(b-1) = 1$, il existe un entier k tel que $v(a^k/b-1) \geqslant 2$.

c) En déduire l'existence d'une extension L de Q_p, de degré $\leqslant p^2$, telle que, pour tout $a \in Q_p$, P_a ait une racine dans L.

COROLLAIRE 2.7.5. — *Soient* K *un corps valué localement compact de caractéristique nulle et* $n > 1$. *Il existe une extension finie* L *de* K *telle que tout polynôme de* K[X] *de degré au plus* n *ait une racine dans* L.

Nous ne donnerons que le schéma de la démonstration.

a) Toute extension totalement ramifiée de K peut être définie par un polynôme d'Eisenstein (2.6.8).

b) L'ensemble des polynômes d'Eisenstein d'un degré donné est une partie compacte de l'ensemble des polynômes de ce degré. D'après 2.7.2 cet ensemble admet un recouvrement ouvert fini $U_1, \ldots, U_k$ tel que, si P et $Q \in U_k$, ils définissent la même extension de K. L'ensemble des extensions totalement ramifiées d'un degré donné est fini.

c) Soit L une extension non ramifiée de degré d de K : il existe $P \in A[X]$, unitaire de degré d, définissant L, et tel que, si a et b sont deux racines distinctes de P, $v(b-a) = 0$, par exemple le polynôme construit dans la démonstration de 2.6.15.

d) Soit P satisfaisant *c)*, il suffit que $v(Q-P) > 0$ pour que le polynôme unitaire Q de degré d définisse la même extension que P (voir la démonstration de 2.7.2). Il n'existe qu'un nombre fini d'extensions non ramifiées de degré donné.

e) Soient L une extension finie de K, e et f l'indice de ramification et le degré résiduel de L sur K. Il existe un sous-corps L′ de L tel que $[L' : K] = f$, L′ non ramifiée sur K et L totalement ramifiée sur L′ (prendre L′ définie par un polynôme unitaire P de degré f tel que $\overline{P}$ définisse l sur k).

f) Soient $n > 1$, L une extension de K de degré au plus n, f le degré résiduel de L sur K, et L′ le sous-corps non ramifié de degré f construit ci-dessus. Soit N_n l'ensemble des extensions non ramifiées de degré au plus n : N_n est fini, d'après *d)*, donc $L' \in N_n$. Or chaque $L' \in N_n$ n'a qu'un nombre fini d'extensions totalement ramifiées de degré au plus n, soit T l'ensemble des extensions totalement ramifiées de degré au plus n des corps $L' \in N_n$, T est donc fini, et $L \in T$. Donc l'ensemble des extensions de degré au plus n de K est fini, soient $L_1, \ldots, L_k$ ces extensions. Il existe un sous-corps L de K, de degré fini sur K, et contenant tous les L_i, alors tout polynôme de degré au plus n à coefficients dans K a une racine dans L.

EXERCICES 2.7.6. — 1. Soient K un corps valué complet localement compact, $\{a_1, \ldots, a_q\} = \mathscr{A}$ un système de représentants de k dans A, contenant 0. Montrer que tout $x \in K$ admet un unique « développement de Hensel » : $x = \sum_{n \geqslant n_0} b_n a^n$, où $b_n \in \mathscr{A}$ et a est une uniformisante fixée de K.

2. Soient K un corps de nombres, B l'anneau des entiers de K, $n = [K : Q]$, P un polynôme irréductible unitaire à coefficients entiers définissant K.

a) Les facteurs irréductibles de P dans $Q_p[X]$ sont deux à deux distincts. Soit $P = P_1 \ldots P_k$ la décomposition de P en facteurs irréductibles unitaires de $Q_p[X]$, $P_i \in Z_p[X]$.

b) Soient K_i l'extension de Q_p par P_i, $n_i = [K_i : Q_p]$, e_i l'indice de ramification, f_i le degré résiduel, M_i l'idéal de valuation de K_i. Le corps K_i contient un sous-corps dense isomorphe à K, soit g_i un isomorphisme de K sur ce sous-corps de K_i. Alors :

$$\mathfrak{P}_i = g_i^{-1}(g_i(K) \cap M_i)$$

est un idéal premier de K, ne dépendant que de i (et non du choix de g_i), $p \mid \mathfrak{P}_i$ et $N(\mathfrak{P}_i) = p^{f_i}$.

c) La décomposition de pB en produit de puissances d'idéaux premiers est :

$$p\mathrm{B} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_k^{e_k}$$

d) Montrer que, en tant que $\mathbf{Q}_p$-espaces vectoriels :

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_p \simeq K_1 \oplus \ldots \oplus K_k.$$

En déduire la relation $e_1 f_1 + \ldots + e_k f_k = n$.

e) Trouver une condition nécessaire et suffisante, portant sur l'idéal $\mathfrak{p}B$, pour que la valuation p - adique admette un unique prolongement à K.

f) Le nombre premier p étant fixé, caractériser les polynômes unitaires irréductibles de $\mathbf{Z}[X]$ définissant une extension K de $\mathbf{Q}$ telle que dans K :

— $\mathfrak{p}B$ soit puissance d'un idéal premier;
— $\mathfrak{p}B$ soit premier;
— $\mathfrak{p}B$ soit produit d'idéaux premiers deux à deux distincts.

g) Soit $K = \mathbf{Q}(\sqrt{2})$. Classifier les nombres premiers suivant que la valuation p - adique de $\mathbf{Q}$ admet :

— un prolongement unique à K tel que $v(K^*) = \mathbf{Z}$;
— un prolongement unique tel que $v(K^*) \neq \mathbf{Z}$;
— deux prolongements distincts.

3. Soient K un corps complet à valuation discrète, L une extension de degré n de K, e l'indice de ramification, f le degré résiduel de L sur K, A (resp. B) et M (resp. N) l'anneau et l'idéal de valuation de K (resp. L). Soient a une uniformisante de L et $b \in B$, la famille $(b^i a^j)$, $0 \leqslant i < f$, $0 \leqslant j < e$, est une base du A-module B à la condition nécessaire et suffisante que l'image $\bar{b}$ de b dans $l = B/N$ engendre l'extension l de $k = A/M$.

CHAPITRE 3

Espaces de Banach ultramétriques

3.1. ESPACES DE BANACH

Un espace vectoriel E sur le corps valué K est muni d'une NORME ULTRAMÉTRIQUE, s'il est muni d'une norme $x \to |x|$, satisfaisant l'inégalité ultramétrique :

$$|x + y| \leqslant \mathrm{Max}\,(|x|, |y|).$$

On dit que E *est un* ESPACE DE BANACH *sur* K, *s'il est complet pour sa norme.*

Dans un espace de Banach, on a les propriétés suivantes (vérification triviale) :

1. Pour qu'une série converge il faut et il suffit que son terme général tende vers 0.

2. Soient $\sum_{n \geqslant 0} u_n$ une série convergente, S sa somme, alors $|S| \leqslant \max_n (|u_n|)$, de plus, s'il n'y a qu'un seul indice n_0 tel que $|u_{n_0}| = \mathrm{Max}\,(|u_n|)$, alors $|S| = |u_{n_0}|$.

3. Soit A l'anneau de valuation de K, toute boule centrée à l'origine est un A-module, ou, ce qui est équivalent, toute boule contenant l'origine est un A-module.

3.1.1. *Exemples*

1. Soient L un corps valué, K un sous-corps de L muni de la valeur absolue induite. La valeur absolue de L

le munit d'une structure d'espace normé ultramétrique sur K.

2. Dans l'exemple 1, si K est complet et [L : K] fini, L est un espace de Banach.

3. Soient X un ensemble, K un corps valué, B(X, K) l'espace des applications bornées de X dans K, muni de la norme de la convergence uniforme sur X : c'est un K-espace normé ultramétrique, il est complet si et seulement si K l'est ($X \neq \varnothing$!).

4. Si X est un espace topologique, le sous-espace C(X, K) de B(X, K) constitué des fonctions continues et bornées est fermé dans B(X, K) : c'est donc un espace de Banach si K est complet.

5. Si X est localement compact, soit $C_0(X, K)$ le sous-espace de C(X, K) constitué des fonctions tendant vers zéro à l'infini (c'est-à-dire, tendant vers 0 suivant le filtre des complémentaires de parties compactes de X), $C_0(X, K)$ est un sous-espace fermé de C(X, K), donc, si K est complet, c'est un espace de Banach.

6. Soit I un ensemble; on note $b_K(I)$, ou $b(I)$ si aucune confusion n'est possible, l'espace B(I, K) : c'est l'espace des familles bornées $(b_i)_{i\in I}$ d'éléments de K, muni de la norme $\operatorname{Sup}_{i\in I} |b_i|$. C'est aussi C(I, K) pour la topologie discrète de I. On note $c_K(I)$, ou $c(I)$, l'espace $C_0(I, K)$ défini par la topologie discrète de I. C'est donc l'ensemble des familles $(c_i)_{i\in I}$ d'éléments de K, indexées dans I, tendant vers 0 à l'infini (*i.e.* tendant vers 0 suivant le filtre des complémentaires des parties finies de I, ce que l'on notera $c_i \to 0$ quand $i \to \infty$).

7. Soit F un espace de Banach sur K, les espaces B(X, F), C(X, F), $C_0(X, F)$, $b_F(I)$ et $c_F(I)$ définis comme dans les exemples 3 à 6 sont encore des espaces de Banach.

8. Soit $E = K[X]$ l'espace des polynômes à coefficients dans K, muni de la norme $|\Sigma a_i X^i| = \operatorname{Sup} |a_i|$. C'est une norme ultramétrique : si K n'est pas discret, E n'est pas complet pour cette norme. Soit en effet $(p_n)_{n\geqslant 0}$ une suite non stationnaire de scalaires tendant vers 0, et soit $P_n(X) = p_0 + \ldots + p_n X^n$. Alors :

$$|P_{n+1} - P_n| = |p_{n+1}|,$$

donc P_n est une suite de Cauchy. Soit $Q \in E$, $Q = \Sigma q_n X^n$, alors, pour que $Q = \lim P_n$, il est nécessaire que, pour tout n, $q_n = p_n$. Comme la suite (p_n) est non stationnaire, les p_n ne sont pas presque tous nuls, donc (P_n) n'a pas de limite dans E. On vérifiera que l'espace $E' = K\{X\}$ des séries restreintes à coefficients dans K, constitué des séries entières $\Sigma a_n X^n$ telles que $a_n \to 0$, muni de la norme $\operatorname{Sup} |a_n|$, est un espace de Banach dont E est un sous-espace dense.

9. Dans l'espace $c_K(N)$ des suites de scalaires tendant vers 0, notons e_n la suite $e_n = (\delta_{kn})_{k\in N}$ où $\delta_{kn} = 1$ si $k = n$ et 0 sinon, et soit $c = (c_n) \in c_K(N)$. La série de terme général $c_n e_n$ est convergente, car $|c_n e_n| = |c_n| \to 0$. Soit $S_k = c_0 e_0 + \ldots + c_k e_k$ la somme partielle de rang k, alors $|c - S_k| = \operatorname{Sup}_{n>k} |c_n| \to 0$, donc $c = \sum_{n\geqslant 0} c_n e_n$.

10. Rappelons que dans un espace de Banach F une famille $(c_i)_{i\in I}$ est dite SOMMABLE et de somme $S \in F$ si, quel que soit $\varepsilon > 0$, il existe une partie finie J de I telle que, pour toute partie finie J' de I telle que $J' \supseteq J$, $|\sum_{i\in J'} c_i - S| \leqslant \varepsilon$. On vérifie que l'espace des familles sommables d'éléments de F indexées dans I coïncide avec l'espace $c_F(I)$ défini en 7, lorsque F est ultramétrique (et complet).

11. Soient E et F deux espaces de Banach sur K, l'espace L(E, F) des applications linéaires continues de E dans F est canoniquement muni de la norme :

$$|a| = \operatorname{Sup}_{|x|\leqslant 1} |a(x)|.$$

On vérifie que c'est une norme ultramétrique sur L(E, F) et que L(E, F) est complet pour cette norme (il suffit d'observer que, si $E_0 = \{x \in E \mid |x| \leqslant 1\}$, la norme

ainsi définie est la restriction à $L(E, F)$ de la norme de la convergence uniforme sur E_0, et que $L(E, F)$ est fermé dans $C(E_0, F)$). En particulier, si $F = K$, l'espace $E' = L(E, K)$ des *formes linéaires continues* sur E se trouve ainsi muni d'une structure canonique d'espace de Banach. On observera que $L(E, F)$ est complet dès que F l'est, que E soit complet ou non. En particulier, si K est complet et si E_1 est le complété de l'espace normé E, $E'_1 = E_1$.

DÉFINITION 3.1.2. — *Soit* E *un espace de Banach sur* K, *on dit qu'une famille* $(e_i)_{i\in I}$ *d'éléments de* E *est une* BASE NORMALE *de* E *si tout* $x \in E$ *admet une unique représentation* $x = \sum_{i\in I} x_i e_i$, *où* $x_i \in K$ *et* $x_i \to 0$ *quand* $i \to \infty$, *satisfaisant* $|x| = \operatorname{Sup}_{i\in I} |x_i|$.

Nous avons montré au n° 9 ci-dessus que la famille $(e_n)_{n\in\mathbf{N}}$ est une base normale de $c_K(\mathbf{N})$, ou, du moins, nous avons montré que tout x admet une représentation du type annoncé, mais nous ne savons pas s'il y a unicité de la représentation. Cela résulte de la remarque suivante : *si la famille* (e_i) *est telle que tout* x *admette une représentation* $x = \Sigma x_i e_i$ *et que, pour toute famille de scalaires* $(x_i)_{i\in I} \in c_K(I)$, $|\Sigma x_i e_i| = Sup\, |x_i|$, *alors* (e_i) *est une base normale de* E. Il suffit en effet de montrer l'unicité de la représentation $\Sigma x_i e_i$ d'un élément x. Or si $\Sigma x_i e_i = \Sigma x'_i e_i$:

$$0 = \Sigma(x_i - x'_i)\, e_i, \qquad \text{et} \qquad |0| = \operatorname{Sup} |x_i - x'_i|.$$

On vérifie plus généralement que la famille $(\varepsilon_i)_{i\in I}$ de $c_K(I)$ définie par $\varepsilon_i = (\delta_{ij})_{j\in I}$ est une base normale de $c_K(I)$, qu'on appellera la base normale canonique.

PROPOSITION 3.1.3. — *Soient* E *un espace de Banach sur* K, $(e_i)_{i\in I}$ *une base normale de* E.

(i) *Il existe une unique application linéaire continue* f *de* E *dans* $c_K(I)$ *telle que* $f(e_i) = \varepsilon_i$ *pour tout* $i \in I$.

(ii) f *est un isomorphisme d'espaces de Banach, c'est-à-dire à la fois un isomorphisme de* K*-espaces vectoriels et une isométrie.*

En effet, une application linéaire continue est uniformément continue. Pour toute partie finie J de I :

$$f\Big(\sum_{i\in J} x_i e_i\Big) = \sum_{i\in J} x_i \varepsilon_i$$

et, nécessairement, $f(\sum_{i\in I} x_i e_i) = \sum_{i\in I} x_i \varepsilon_i = (x_i)_{i\in I}$, par continuité uniforme et passage à la limite suivant le filtre des complémentaires de parties finies de I. Il suffit de vérifier que l'application f ainsi définie est linéaire et continue, ce qui est trivial, pour avoir prouvé (i).

Soit $x \in E$, $x = \Sigma x_i e_i$, alors $|x| = \operatorname{Sup} |x_i|$, et $|f(x)| = |(x_i)_{i\in I}| = \operatorname{Sup} |x_i|$, donc f est une isométrie. Il reste à montrer que f est surjective, or si $c = (c_i)_{i\in I} \in c_K(I)$, soit $x = \Sigma c_i e_i$ (comme $c_i \to 0$, la famille $c_i e_i$ est sommable dans E), alors $f(x) = c$, d'où la proposition.

Nous appellerons isomorphisme canonique de E sur $c_K(I)$ défini par la base normale (e_i) l'isomorphisme f défini en 3.1.3. On pourra vérifier à titre d'exercice que, si f est un isomorphisme d'espaces de Banach de E sur $c_K(I)$, la famille $(f^{-1}(\varepsilon_i))_{i\in I}$ est une base normale de E : nous dirons encore que c'est la base normale canoniquement définie par f.

EXEMPLE. — Soit E un espace de Banach sur K, et soit $(e_i)_{i\in I}$ une base normale de E. Le dual $E' = L(E, K)$ de E contient en particulier les formes linéaires $g_i(x) = x_i$, où $x = \Sigma x_i e_i$ est la représentation de x sur la base (e_i). On a $|g_i(x)| = |x_i| \leqslant |x|$ et $g_i(e_i) = 1$, donc $|g_i| = 1$. Soient F un autre espace de Banach et $h \in L(E, F)$. Posons $h_i = h(e_i)$, alors $|h_i| \leqslant |h|$, mais, pour :

$$x = \Sigma x_i e_i \in E, \quad |h(x)| = |\Sigma x_i h(e_i)| \leqslant |x| \operatorname{Sup} |h_i|,$$

donc $|h| = \operatorname{Sup} |h_i|$. Soit ω l'application de $L(E, F)$ dans $b_F(I)$ qui à h associe $\omega(h) = h' = (h_i)_{i\in I}$, c'est une application linéaire et $|\omega(h)| = |h|$. De plus ω est surjective car si $h' = (h_i)_{i\in I} \in b_F(I)$, pour tout $x \in E$, la série $\Sigma g_i(x)\, h_i$ est convergente, sa somme $h(x)$ est telle que

$|h(x)| \leqslant \mathrm{Sup}\,|g_i(x)\,h_i| \leqslant \mathrm{Sup}\,(|x|\,|g_i|\,|h_i|) \leqslant |x|\,|h'|$. L'application $x \to h(x)$ ainsi définie est un élément de $\mathrm{L}(\mathrm{E}, \mathrm{F})$ tel que $\omega(h) = h'$. Nous avons ainsi montré que ω est un *isomorphisme d'espaces de Banach* de $\mathrm{L}(\mathrm{E}, \mathrm{F})$ sur $b_{\mathrm{F}}(\mathrm{I})$. En particulier, une base normale $(e_i)_{i\in\mathrm{I}}$ définit canoniquement un isomorphisme de $\mathrm{E}' = \mathrm{L}(\mathrm{E}, \mathrm{K})$ sur $b_{\mathrm{K}}(\mathrm{I})$.

Remarquons que si $c = (c_i) \in c_{\mathrm{K}}(\mathrm{I})$, $c \neq 0$, il existe $i_0 \in \mathrm{I}$ tel que $|c| = |c_{i_0}|$. Donc, si un espace de Banach a une base normale, sa norme satisfait la condition :

(N) *pour tout* $x \in \mathrm{E}$, *il existe* $a \in \mathrm{K}$ *tel que* $|x| = |a|$,

ou, ce qui est équivalent :

(N) *pour tout* $x \in \mathrm{E}$, $x \neq 0$, *il existe* $b \in \mathrm{K}$ *tel que* $|bx| = 1$.

Nous allons montrer que cette condition, nécessaire pour que E possède une base normale, est aussi suffisante lorsque K est à valuation discrète.

NOTATIONS 3.1.4. — Soient E un espace de Banach sur K, A l'anneau de valuation, M l'idéal de valuation et k le corps résiduel de K, nous noterons :

$\mathrm{E}_0 = \{x \in \mathrm{E} \mid |x| \leqslant 1\}$, E_0 est un A-module;

$\mathrm{E}'_0 = \{x \in \mathrm{E} \mid |x| < 1\}$, $\mathrm{E}'_0 = \mathrm{ME}_0$. Si K est à valuation discrète, soit a une uniformisante; alors $\mathrm{E}'_0 = a\mathrm{E}_0$;

$\overline{\mathrm{E}} = \mathrm{E}_0/\mathrm{E}'_0$, c'est un k-espace vectoriel, nous noterons p à la fois la projection canonique de E_0 sur $\overline{\mathrm{E}}$ et celle de A sur k.

PROPOSITION 3.1.5. — *Soit* E *un espace de Banach sur* K. *Si* K *est à valuation discrète et si* E *satisfait la condition* (N), *alors pour une famille* $(e_i)_{i\in\mathrm{I}}$ *d'éléments de* E_0 *les conditions suivantes sont équivalentes :*

(a) $(e_i)_{i\in\mathrm{I}}$ *est une base normale de* E;

(b) $(p(e_i))_{i\in\mathrm{I}}$ *est une base du* k*-espace vectoriel* $\overline{\mathrm{E}}$.

Remarquons d'abord que, si (e_i) est une base normale, $|e_i| = 1$ pour tout i : le choix de la famille (e_i) dans E_0 n'est donc pas une restriction.

Si $(e_i)_{i\in\mathrm{I}}$ satisfait *(a)*, soit $\bar{x} \in \overline{\mathrm{E}}$ et soit $x \in \mathrm{E}_0$ tel que $p(x) = \bar{x}$. On sait que x admet une représentation $\Sigma x_i e_i$, pour laquelle $x_i \to 0$, donc les $p(x_i)$ sont presque tous nuls, alors $p(x) = \Sigma p(x_i)\,p(e_i)$, donc la famille $p(e_i)$ engendre $\overline{\mathrm{E}}$. Soit $\Sigma a_i p(e_i) = 0$ une relation de dépendance linéaire entre les $p(e_i)$, $a_i \in k$. Choisissons des représentants x_i de a_i de façon que $x_i = 0$ si $a_i = 0$, et soit $x = \Sigma x_i e_i$; alors $p(x) = 0$, donc $|x| < 1$, et $|x| = \mathrm{Sup}\,|x_i|$, donc $a_i = 0$ pour tout i : $p(e_i)$ est une base de $\overline{\mathrm{E}}$.

Réciproquement, supposons *(b)* satisfaite. D'abord, pour toute famille (x_i) de scalaires tendant vers 0, $\Sigma x_i e_i = \mathrm{Sup}\,|x_i|$. On peut en effet, quitte à multiplier par un scalaire, se ramener au cas où $\mathrm{Sup}\,|x_i| = 1$. Alors $x = \Sigma x_i e_i \in \mathrm{E}_0$ et $p(x) = \Sigma p(x_i)\,p(e_i)$, où les $p(x_i)$ ne sont pas tous nuls, donc $p(x) \neq 0$ et $|x| = 1$.

Soit $x \in \mathrm{E}_0$; il existe des scalaires x_{i1} dans A, presque tous nuls, tels que :

$$p(x) = \Sigma p(x_{i1})\,p(e_i).$$

Posons $y_1 = \Sigma x_{i1} e_i$ et $x_1 = a^{-1}(x - y_1)$, alors $x_1 \in \mathrm{E}_0$. Supposons qu'on ait construit $x = x_0, x_1, \ldots, x_n$ dans E_0 tels que, pour $1 \leqslant j \leqslant n$:

$$x_{j-1} = ax_j + y_j$$

où y_j est une combinaison linéaire finie des e_i,

$$y_j = \Sigma x_{ij} e_i,$$

les $(x_{ij})_{i\in\mathrm{I}}$ étant presque tous nuls.

Il existe une famille de scalaires presque tous nuls dans A, $(x_{i,n+1})_{i\in\mathrm{I}}$, tels que :

$$p(x_n) = \Sigma p(x_{i,n+1})\,p(e_i).$$

En posant $y_{n+1} = \Sigma x_{i,n+1} e_i$ on voit que :

$$x_{n+1} = a^{-1}(x_n - y_n) \in \mathrm{E}_0.$$

On peut donc construire une suite infinie (x_n) satisfaisant pour tout j les conditions ci-dessus. Soient alors :

$$z_n = y_1 + \ldots + a^{n-1}y_n \quad \text{et} \quad a_i = \sum_{n \geqslant 0} x_{i,n}a^n.$$

D'une part, $x - z_n = a^n x_n$, donc $|x - z_n| \leqslant |a^n|$ et $z_n \to x$. D'autre part :

$$|a_i| \leqslant |a|^{k(i)} \quad \text{où} \quad k(i) = \mathrm{Inf}\{n \,|\, x_{i,n} \neq 0\},$$

donc $a_i \to 0$, soit $x' = \Sigma a_i e_i$, alors :

$$x' - z_n = \sum_{i \in I} \Big(\sum_{k > n} x_{i,k}a^k \Big) e_i,$$

donc :

$$|x' - z_n| \leqslant |a|^{n+1};$$

alors $z_n \to x'$, d'où $x' = x$. On voit que tout $x \in E_0$ admet une représentation $\Sigma a_i e_i$, où $a_i \to 0$. En multipliant par un scalaire convenable, on en déduit l'existence d'une telle représentation pour tout $x \in E$. L'unicité résulte de ce que $|\Sigma a_i e_i| = \mathrm{Sup}\,|a_i|$, donc (e_i) est une base normale.

COROLLAIRE 3.1.6. — *Tout espace de Banach* E *sur le corps valué à valuation discrète* K, *dont la norme satisfait la condition* (N), *possède une base normale. Deux bases normales de* E *ont même cardinal.*

En effet $\overline{E}$ a une base, et deux bases de $\overline{E}$ ont même cardinal.

Nous allons maintenant décrire une méthode générale pour définir sur un espace vectoriel une norme satisfaisant la condition (N).

PROPOSITION 3.1.7. — *Soit* E *un espace vectoriel sur le corps valué* K, *alors :*

(i) *pour toute norme* $x \to |x|$, *ultramétrique sur* E, *la boule unité* $E_0 = B$ *satisfait* (C) B *est un* A*-module ne contenant aucun sous-espace vectoriel non nul et* $E = \bigcup_{k \in K} kB$;

(ii) *si* K *est à valuation discrète, soit* B *une partie de* E *satisfaisant* (C), *alors* $|x|_B = Inf\{|b| \,|\, b \in K^* \text{ et } b^{-1}x \in B\}$ *définit sur* E *une norme ultramétrique* $|x|_B$ *satisfaisant la condition* (N).

L'assertion (i) est évidente. Soit B une partie de E satisfaisant (C). Remarquons d'abord que, pour tout $x \in K$, $M(x) = \{k \in K \,|\, kx \in B\}$ est un sous-A-module de K, et que $|x|_B = (\mathrm{Sup}_{k \in M(x)} |k|)^{-1}$. Donc :

$$|x|_B = 0 \Leftrightarrow M(x) = K \Leftrightarrow Kx \subseteq B \Leftrightarrow x = 0.$$

Si $b \in K$, $M(bx) = b^{-1}M(x)$, donc $|bx|_B = |b|\,|x|_B$. De plus $M(x+y) \supseteq M(x) \cap M(y)$, d'où l'inégalité ultramétrique. Que K soit ou non à valuation discrète, $|x|_B$ définit une norme ultramétrique sur E. Si K est à valuation discrète, $|K| = \{|k| \,|\, k \in K\}$ n'a que 0 comme point d'accumulation, donc, si $x \neq 0$, $|x|_B \in |K|$, ce qui prouve que $|x|_B$ satisfait (N).

COROLLAIRE 3.1.8. — *Soit* E *un espace vectoriel sur le corps valué* K, *et soit* $x \to |x|$ *une norme ultramétrique sur* E, E_0 *la boule unité de* E. *La norme* $|x|_{E_0}$ *associée à* E_0 *est équivalente à* $|x|$. *Si* K *est à valuation discrète, il existe une norme ultramétrique sur* E, *équivalente à* $|x|$ *et satisfaisant la condition* (N).

Evident.

EXERCICES 3.1.9. — 1. Soient K à valuation discrète et L une extension finie de K munie de la valeur absolue prolongeant celle de K (K complet). A quelle condition L admet-elle une base normale ? Soit B l'anneau de valuation de L, que sont les bases normales de L relativement au A-module B ?

2. Soient $r > 1$ un réel, E un espace de Banach sur le corps valué K. On dira que $(e_i)_{i \in I}$ est une base r-normale de E si tout $x \in E$ admet une unique représentation $x = \Sigma x_i e_i$, $x_i \in K$, $x_i \to 0$, et $\mathrm{Max}\,|x_i| \leqslant |x| < r\,\mathrm{Max}\,|x_i|$. On suppose E séparable.

a) Si K est à valuation discrète, tout espace E admet une base r-normale pour $r = |a|^{-1}$, où a est une uniformisante de K.

b) Si K est à valuation dense, E admet une base r-normale pour tout $r > 1$.

3.2. EXEMPLES DE BASES NORMALES

3.2.1. *Dimension finie*

Soit E un espace de dimension n sur K, dont la norme satisfait la condition (N). Une base normale de E est aussi une base du K-espace vectoriel E. C'est aussi une base du A-module E_0. Soit $f = (f_1, \ldots, f_n) \in E_0^n$, et soit $e = (e_1, \ldots, e_n)$ une base normale de E. Soit $f_j = \Sigma a_{ij} e_i$, alors pour que f soit une base normale il faut et il suffit que la matrice $a = (a_{ij})$, qui est à coefficients dans A, soit telle que $\bar{a} = (\bar{a}_{ij})$ soit une matrice inversible à coefficients dans k. Donc le groupe des automorphismes de E transformant bases normales en bases normales (groupe unitaire) s'identifie au groupe $GL_n(A)$ des matrices inversibles de $M_n(A)$.

On remarque que si B est un sous-A-module de E, la condition (C) de la proposition 3.1.7 est équivalente à : B est un sous-A-module de rang n. Cette remarque fournit une nouvelle démonstration du fait que l'anneau de valuation E d'une extension finie L d'un corps valué complet K est un A-module libre de rang n (proposition 2.6.12).

3.2.2. *Espaces de fonctions continues*

Soient X un espace topologique séparé, K un corps valué ultramétrique complet, C(X, K) l'espace des fonctions continues et bornées, muni de la norme de la convergence uniforme sur X. Si f est continue, f est constante sur les composantes connexes de X, car, pour tout $x \in K$, $f^{-1}(x)$ est ouvert et fermé. Soit X' le quotient de X par la relation « x et y sont équivalents s'ils appartiennent à la même composante connexe », alors X' est un espace totalement discontinu et $C(X', K) \simeq C(X, K)$: nous supposerons donc désormais que X est totalement discontinu.

Soit $E = C(X, K)$, alors $E_0 = C(X, A)$ est le A-module des fonctions continues sur X à valeurs dans A, $E_0' = C(X, M)$, et $\bar{E} = E_0/E_0'$ s'identifie à l'espace C(X, k)

des fonctions continues sur X et à valeurs dans k, k étant muni de la topologie discrète. Soient $\bar{f} \in \bar{E}$ et $\bar{x} \in k$, alors $\bar{f}^{-1}(\bar{x})$ est une partie de X à la fois ouverte et fermée, et il existe un recouvrement de X par des parties ouvertes et fermées (U_i) telles que $\bar{f}$ soit constant sur chaque U_i. Donc $\bar{E}$ s'identifie à l'espace des fonctions de X dans k, localement constantes sur X.

Supposons maintenant que X soit compact, et plus précisément que X soit un espace métrique compact. Pour $r > 0$, nous noterons $\bar{E}(r)$ le sous-espace de $\bar{E}$ constitué des $\bar{f} \in \bar{E}$ telles que $\bar{f}$ soit constante sur toute boule de rayon r. Alors $\bar{E} = \bigcup_{r>0} \bar{E}(r)$. Or chaque espace $\bar{E}(r)$ est de dimension finie, et $r \leqslant r' \Rightarrow \bar{E}(r) \supseteq \bar{E}(r')$: on en déduit que $\bar{E}$ est de dimension au plus dénombrable. Donc, *si* X *est un espace métrique compact totalement discontinu et* K *un corps valué complet à valuation discrète, l'espace* $E = C(X, K)$ *admet une base normale dénombrable.*

Soit par exemple $X = \mathbf{Z}_p$: c'est un espace métrique compact totalement discontinu.

PROPOSITION 3.2.2.1. — *Soit* K *un corps valué complet à valuation discrète,* $E = C(\mathbf{Z}_p, K)$. *Pour* $N \geqslant 0$, *on note* $h(N)$ *l'entier défini par* $p^{h(N)-1} \leqslant N < p^{h(N)}$ *et on note* f_N *la fonction caractéristique de* $N + p^{h(N)}\mathbf{Z}_p$. *Alors* $(f_N)_{N \geqslant 0}$ *est une base normale de* E.

Soit $\bar{E}_h$ le sous-espace $\bar{E}(p^{-h})$ de $\bar{E}$: $\bar{E}_h$ est de dimension p^h. Notons $\varphi_{i,h}$ la fonction caractéristique de $i + p^h\mathbf{Z}_p$, alors $(\varphi_{i,h})$ pour $0 \leqslant i < p^h$ est une base de $\bar{E}_h$. Nous allons montrer que (f_N), $0 \leqslant N < p^h$ est aussi une base de $\bar{E}_h$. Comme $\bar{E} = \bigcup_{n \geqslant 0} \bar{E}_h$, la proposition en découle aussitôt (on a ici identifié f et $\bar{f}$ lorsque f est une fonction caractéristique).

D'abord, il est clair par la définition des f_N que, pour $0 \leqslant N < p^h$, $f_N \in \bar{E}_h$. Soit :

$$f_N = a_{0,N}\varphi_{0,h} + \ldots + a_{i,N}\varphi_{i,h} + \ldots + a_{p^h-1,N}\varphi_{p^h-1,h}$$

la représentation de f_N sur la base $\varphi_{i,h}$ de $\overline{E}_h$. On a $a_{i,N} = f_N(i)$, donc, en particulier, pour $p^{h-1} \leqslant N < p^h$, $a_{i,N} = \delta_{N,i}$. Supposons qu'on ait montré que, pour $0 \leqslant N < p^{h-1}$, f_N est une base de $\overline{E}_{h-1}$: il suffit alors de montrer que le sous-espace de $\overline{E}_h$ engendré par les $(\varphi_{i,h})$ pour $p^{h-1} \leqslant i < p^h$ est supplémentaire de $\overline{E}_{h-1}$. Cette dernière propriété résulte aisément des relations :

$$\varphi_{i,h-1} = \sum_{0 \leqslant j < p} \varphi_{i+jp^{h-1},h}.$$

Soit $f \in E$; d'après la proposition ci-dessus, il existe une unique suite de scalaires $(a_N)_{N \geqslant 0}$, $a_N \to 0$, telle que $f = \Sigma a_N f_N$, cette série étant uniformément convergente. Remarquons que, pour $i < N$, $f_N(i) = 0$. Donc, pour tout entier N :

$$f(N) = \sum_{0 \leqslant n \leqslant N} a_n f_n(N).$$

On pourra montrer à titre d'exercice que :

$$a_n = f(n) - f(r(n))$$

où $r(n)$ est le reste de n dans la division par $p^{h(n)-1}$.

Supposons maintenant que le corps K des scalaires contienne $\mathbf{Q}_p$. Alors les polynômes à coefficients dans $\mathbf{Q}$ définissent des fonctions continues sur $\mathbf{Z}_p$. Nous allons montrer que les polynômes engendrent un sous-espace dense de E (théorème de Weierstrass) et, plus précisément, qu'il existe une base normale de E constituée de polynômes (nous ne distinguerons pas les polynômes des fonctions polynomiales sur $\mathbf{Z}_p$, ce qui est licite puisque $\mathbf{Q}_p$ est un corps infini).

PROPOSITION 3.2.2.2. — *Soit* K *un corps valué complet à valuation discrète contenant* $\mathbf{Q}_p$. *On pose* $Q_0(X) = 1$ *et, pour* $n \geqslant 1$, $Q_n(X) = \binom{X}{n} = \dfrac{X(X-1)\dots(X-n+1)}{n!}$.

La suite $(Q_n)_{n \geqslant 0}$ *est une base normale de* $E = C(\mathbf{Z}_p, K)$.

Remarquons d'abord que, pour $N \in \mathbf{N}$, et pour tout

$n \geqslant 0$, $Q_n(N) \in \mathbf{N}$, donc $|Q_n(N)| \leqslant 1$. Or $\mathbf{N}$ est dense dans $\mathbf{Z}_p$, donc $|Q_n| \leqslant 1$. Pour simplifier les notations nous supposerons que la valeur absolue et la valuation de K prolongent celles de $\mathbf{Q}_p$, et que, par conséquent, $v(p) = 1$ et $|p| = p^{-1}$.

LEMME 3.2.2.3. — *Soit* $n < p^h$, *alors :*

$$v(x-y) \geqslant h \Rightarrow v(Q_n(x) - Q_n(y)) \geqslant 1.$$

Nous utiliserons l'identité polynomiale élémentaire :

$$Q_n(X+Y) = \sum_{k=0}^{n} Q_k(X)\, Q_{n-k}(Y).$$

Elle se montre par exemple en remarquant que, pour des valeurs entières x et y de X et Y, l'égalité des valeurs prises par les deux membres résulte de ce qu'ils sont coefficient de T^n dans les polynômes $(1+T)^{n+y}$ et $(1+T)^n (1+T)^y$ respectivement. Deux polynômes en deux variables qui prennent les mêmes valeurs sur $\mathbf{N}^2$ coïncident.

Soient $n < p^h$, $x \in \mathbf{Z}_p$ et $y = x + p^h z$, $z \in \mathbf{Z}_p$, alors :

$$Q_n(y) = Q_n(x) + \sum_{k=1}^{n} Q_k(p^h z)\, Q_{n-k}(x).$$

Or, pour $k \geqslant 1$, $Q_k(u) = \dfrac{u}{k} Q_{k-1}(u-1)$, donc :

$$v(Q_k(p^h z)) \geqslant v(p^h z) - v(k) \geqslant h - v(k).$$

Si $k \leqslant n < p^h$, $v(k) < h$, donc $v(Q_k(p^h z)) \geqslant 1$, d'où le lemme.

Il en résulte que, pour $n < p^h$, $\overline{Q}_n \in \overline{E}_h$. Nous allons montrer que les $(\overline{Q}_n)$ forment, pour $0 \leqslant n < p^h$, une base de $\overline{E}_h$, la proposition en résulte comme dans la démonstration précédente. Notons g_i la fonction caractéristique de $i + p^h \mathbf{Z}_p$, on sait que (g_i), $0 \leqslant i < p^h$, est une base de $\overline{E}_h$. Or, pour $0 \leqslant n < p^h$:

$$\overline{Q}_n = \sum_{0 \leqslant i < p^h} \overline{Q_n(i)}\, g_i,$$

où $Q_n(i) = 0$ pour $i < n$ et $Q_n(n) = 1$. Donc la matrice représentant les $\overline{Q}_n$ sur les g_i est triangulaire, ses termes diagonaux sont égaux à 1 : elle est inversible, ce qui prouve la proposition.

On a donc montré que toute fonction continue $f \in E$ admet une unique représentation :

$$f = \sum_{n \geqslant 0} a_n Q_n, \quad \text{où} \quad a_n \to 0 \quad \text{et} \quad |f| = \operatorname{Sup} |a_n|.$$

Si $k \in \mathbf{N}$, $Q_n(k) = 0$ pour $n > k$, on a donc :

$$f(k) = \sum_{0 \leqslant n \leqslant k} a_n \binom{k}{n}.$$

Cela s'exprime encore par le fait que le polynôme $f_k(X) = \sum_{0 \leqslant n \leqslant k} a_n Q_n(X)$ prend les mêmes valeurs que f aux entiers $n = 0, \ldots, k$. Donc f_k est le polynôme d'interpolation de f sur les $k+1$ premiers entiers, et :

$$a_n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(i) \qquad \text{(I)}$$

La formule (I), qui est une formule classique d'interpolation « de Newton », peut être vérifiée aisément. En effet, f_k est défini par les conditions « $f_k(i) = f(i)$ pour $i \leqslant k$ et $\operatorname{dg} f_k \leqslant k$ ». Il suffit donc de vérifier que le polynôme $f_k = a_0 Q_0 + \ldots + a_k Q_k$, où a_n est donné par la formule (I), satisfait ces conditions.

COROLLAIRE 3.2.2.4. — *Soit f une application de* $\mathbf{N}$ *dans* K, *alors f est prolongeable en une fonction continue g de* $\mathbf{Z}_p$ *dans* K *à la condition nécessaire et suffisante que la suite* (a_n) *définie par* (I) *tende vers* 0. *S'il en est ainsi,* $g = \sum_{n \geqslant 0} a_n Q_n$, *cette série étant uniformément convergente.*

Supposons que f soit la restriction à $\mathbf{N}$ d'une fonction $g \in E$, alors le développement $g = \sum a_n Q_n$ de g sur la base normale (Q_n) est tel que $a_n \to 0$. De plus a_n satisfait la formule (I) puisque, pour $i \in \mathbf{N}$, $f(i) = g(i)$. Réciproquement, soit f définie sur $\mathbf{N}$, supposons que la

suite $a_n \to 0$, alors la série $\sum a_n Q_n$ converge vers un élément g de E, et, pour $k \in \mathbf{N}$, $g(k) = f(k)$.

Soit par exemple $a \in \mathbf{C}_p$, et soit K le plus petit sous-corps complet de $\mathbf{C}_p$ qui contienne a et $\mathbf{Q}_p$: K est à valuation discrète. En effet, si $K' = \mathbf{Q}_p(a)$, $v(K'^*)$ est discret et K est la fermeture de K′ dans $\mathbf{C}_p$, donc $v(K^*) = v(K'^*)$. Soit f définie sur $\mathbf{N}$ par $f(n) = a^n$, les coefficients a_n associés à f sont :

$$a_n = \sum_{0 \leqslant i \leqslant n} (-1)^{n-i} \binom{n}{i} a^i = (a-1)^n.$$

Pour que $a_n \to 0$, il faut et il suffit que $v(a-1) > 0$, alors f est prolongeable en une fonction continue sur $\mathbf{Z}_p$ que nous noterons a^w, qui est somme de la série uniformément convergente $a^w = \sum_{n \geqslant 0} (a-1)^n \binom{w}{n}$.

Nous allons maintenant montrer que les résultats ci-dessus, valables pour les espaces de Banach sur un corps à valuation discrète, peuvent souvent être étendus à des espaces sur un corps quelconque, grâce aux propriétés des produits tensoriels d'espaces de Banach.

3.2.3. *Sommes directes*

Soient E et F deux espaces de Banach sur le même corps valué K. On munit canoniquement la somme directe $E \oplus F$ de la norme $|x+y| = \operatorname{Max}(|x|, |y|)$, $x \in E$, $y \in F$. On vérifie immédiatement que c'est une norme ultramétrique et que $E \oplus F$ est complet pour cette norme.

De même soit $(E_i)_{i \in I}$ une famille, finie ou non, d'espaces de Banach sur K, on munit leur somme directe $E = \bigoplus_{i \in I} E_i$ de la norme $|\sum_{i \in I} x_i| = \operatorname{Max}_{i \in I} |x_i|$, où $x_i \in E_i$ et les x_i sont presque tous nuls. On vérifie que c'est une norme ultramétrique sur E. Si I n'est pas fini, E n'est pas complet pour cette norme. Soit E′ le complété de E,

on note $E' = \widehat{\bigoplus_{i\in I}} E_i$, et on l'appelle somme directe complétée des E_i.

PROPOSITION 3.2.3.1. — *Soit $(E_i)_{i\in I}$ une famille d'espaces de Banach sur K, alors $\widehat{\bigoplus_{i\in I}} E_i$ est canoniquement isomorphe à l'espace des familles $x = (x_i)_{i\in I}$, $x_i \in E_i$, telles que $x_i \to 0$, muni de la norme $|x| = Sup\ |x_i|$.*

Soient $F = \prod_{i\in I} E_i$ et F_0 le sous-espace de F constitué des familles bornées (x_i). Muni de la norme $|x| = \mathrm{Sup}\,|x_i|$, F_0 est complet, et l'image canonique de $\bigoplus_{i\in I} E_i$ dans F est contenue dans F_0. La fermeture dans F_0 de cette image est l'espace des suites (x_i) qui tendent vers 0.

EXERCICES 3.2.3. — 1. Soit E un espace de Banach sur le corps complet K, satisfaisant la condition (N) ; E est somme directe complétée de droites à la condition nécessaire et suffisante qu'il ait une base normale.

2. Deux sous-espaces F et G de E sont dits orthogonaux si, pour tous $x \in F$ et $y \in G$:

$$|x+y| = \mathrm{Max}\,(|x|, |y|).$$

a) Soient $x \in E$ et $y_0 \in F$; si $|x-y_0| = \underset{y\in F}{\mathrm{Inf}}\,|x-y|$, F et $(x-y_0)\,K$ sont orthogonaux.

b) Si K est à valuation discrète, pour tout sous-espace fermé F de E il existe un sous-espace G tel que $E = F \oplus G$.

3. Soient $E = C(Z_p, Q_p)$, E_0 sa boule unité, et $B = K[X] \cap E_0$ le A-module des polynômes $P \in K[X]$ tels que $x \in Z_p \Rightarrow P(x) \in A$. On appelle aussi B le A-module des polynômes à valeurs entières. Soit $(P_n)_{n\geqslant 0}$ une base du K-espace vectoriel K[X] constituée d'éléments de B. Alors $(P_n)_{n\geqslant 0}$ est une base du A-module B à la condition nécessaire et suffisante que $(P_n)_{n\geqslant 0}$ soit une base normale de E.

3.3. PRODUITS TENSORIELS

Soient E et F deux espaces de Banach sur K et $G = E \otimes F$. Tout élément z de G admet des représentations comme somme finie d'éléments décomposables $x \otimes y$.

Nous noterons $\Sigma' x_i \otimes y_i$ une telle somme : le signe ′ indique que les $x_i \otimes y_i$ sont presque tous nuls. On pose :

$$|z| = \mathrm{Inf}\,(\mathrm{Max}\,(|x_i||y_i|)),$$

où la borne inférieure est prise sur les représentations $z = \Sigma' x_i \otimes y_i$ de z.

PROPOSITION 3.3.1. — *L'application $z \to |z|$ définit sur $G = E \otimes F$ une norme ultramétrique.*

On vérifie facilement que $|az| = |a|\,|z|$ pour $a \in K$ et $z \in G$, et que $|z+z'| \leqslant \mathrm{Max}\,(|z|, |z'|)$. Soit :

$$H = B(E \times F, K)$$

l'espace des formes bilinéaires continues sur $E \times F$, si $h \in H$ on pose $|h| = \mathrm{Sup}\,(|h(x,y)|)$, pour :

$$(x,y) \in E_0 \times F_0,$$

ce qui définit sur H une norme ultramétrique pour laquelle il est complet. Soit $G' = L'(G, K)$ l'espace des formes linéaires sur G. Si $h \in H$, il existe une unique $h' \in G'$ telle que $h'(x \otimes y) = h(x,y)$ (par définition du produit tensoriel $G = E \otimes F$). Soient :

$$z \in G, \qquad z = \Sigma' x_i \otimes y_i,$$

alors :

$$|h'(z)| = |\Sigma' h(x_i, y_i)| \leqslant \mathrm{Max}\,(|h(x_i, y_i)|) \leqslant |h|\,\mathrm{Max}\,(|x_i|\,|y_i|),$$

donc :

$$|h'(z)| \leqslant |h|\,|z|.$$

Pour montrer que $|z|$ est une norme, il suffit donc de montrer que, pour $z \neq 0$, il existe $h \in H$ telle que $h'(z) \neq 0$, ce qui résultera de 3.3.2. Soient X l'espace vectoriel libre sur K engendré par $E \times F$, p sa projection canonique sur G et $N = \mathrm{Ker}\,p$. Alors $X = \bigoplus_{i\in E\times F} K_i$, où K_i est un espace de dimension 1 sur K, muni d'un isomorphisme canonique sur K. Soient, pour $a_i \in K_i$, $|a_i|_i = |a_i|\,||i||$, où $i = (x,y)$, $x \in E$ et $y \in F$, et

$||i|| = |x|\,|y|$; alors L muni de la norme de somme directe des espaces de Banach K_i (où K_i est muni de $|a_i|_i$) est un espace normé ultramétrique, et la norme $|z|$ définie sur G est $|z| = \mathrm{Inf}\{|Z|\}$ pour $Z \in p^{-1}(z)$. Les éléments $h \in H$ sont en bijection canonique avec les formes linéaires continues sur X, nulles sur N, et tout revient à montrer que, si $Z \in X$ est tel que $Z \notin N$, il existe une forme linéaire continue X′ sur X, nulle sur N, et telle que $X'(Z) \neq 0$. Ceci équivaut à montrer que N est fermé. Or, pour toute $h \in H$, soit $h'' \in X'$ la forme linéaire continue qui lui est associée, alors $\mathrm{Ker}\, h''$ est fermé, et $N = \bigcap_{h \in H} \mathrm{Ker}\, h''$ l'est aussi.

PROPOSITION 3.3.2. — *Soient* E *et* F *deux espaces de Banach sur* K, *soient* $(e_i)_{i\in I}$ *une base normale de* E *et* g_i *la forme linéaire i-ème coordonnée,* $g_i(x) = x_i$ *si* $x = \Sigma x_i e_i$, *et soit* h'_i *l'unique application linéaire continue de* G *dans* F *telle que* $h'_i(x \otimes y) = g_i(x)\, y$.

(i) *L'application linéaire* h' *de* $E \otimes F$ *dans* F^I *définie par* $h'(z) = (h'_i(z))_{i\in I}$ *est un isomorphisme isométrique de* $G = E \otimes F$ *sur un sous-espace dense de* $c_{\mathbb{F}}(I)$.

(ii) *Soit* $E \hat{\otimes} F = \hat{G}$ *le complété de* G, *tout* $z \in \hat{G}$ *admet une unique représentation :*

$$z = \sum_{i\in I} e_i \otimes y_i, \quad \text{où} \quad y_i \in F, \quad y_i \to 0 \quad \text{et} \quad |z| = \mathrm{Max}\,|y_i|.$$

Soit $z = \Sigma' x_j \otimes y_j$ une représentation de z, pour chaque j, $g_i(x_j) \to 0$, donc $h'_i(z) = \Sigma' g_i(x_j)\, y_j \to 0$, et $h'(z) \in c_{\mathbb{F}}(I)$. Nous avons remarqué plus haut que, si $z \neq 0$, il existe une forme linéaire continue sur G telle que $h(z) \neq 0$: on en déduit aisément que h' est injective. De plus $|h'(z)| = \mathrm{Sup}\,|h'_i(z)| \leqslant |z|\,\mathrm{Sup}\,|h'_i| = |z|$. Donc h' admet un unique prolongement linéaire continu au complété $\hat{G}$ de G. Soit v l'application de $c_{\mathbb{F}}(I)$ dans $\hat{G}$ qui à (f_i) associe $\Sigma e_i \otimes f_i = v((f_i)_{i\in I})$: v est une application linéaire continue, et $|v| \leqslant 1$. Pour $z \in G$, $v(h'(z)) = z$. On en déduit que h' est un isomorphisme isométrique

de $\hat{G}$ sur $c_{\mathbb{F}}(I)$, d'où l'assertion (i). Le (ii) se déduit trivialement de (i).

COROLLAIRE 3.3.3. — *Soient* E *un espace de Banach sur* K, L *un corps valué complet contenant* K, $F = E \hat{\otimes} L$, F *a une structure naturelle de* L*-espace de Banach; alors, si* $(e_i)_{i\in I}$ *est une base normale de* E, *c'est aussi une base normale du* L*-espace vectoriel* F.

La structure naturelle de L-espace vectoriel sur $E \otimes L$, définie par $l(x \otimes l') = x \otimes ll'$, se prolonge par continuité à F. L'isomorphisme h' de F sur $c_L(I)$ est L-linéaire, et $h'^{-1}(\varepsilon_i) = e_i \otimes 1 = e_i$, (e_i) est une base normale du L-espace de Banach F.

3.4. EXEMPLES DE PRODUITS TENSORIELS COMPLÉTÉS

Les deux sortes d'exemples que nous considérerons concernent des espaces fonctionnels.

3.4.1. *Extension du corps des scalaires*

Soient X un espace topologique, K un corps valué complet, L une extension complète de K, $E = C(X, K)$ et $F = C(X, L)$. *Si* X *est compact,* $F \simeq E \hat{\otimes} L$. Plus précisément, soit a l'application K-linéaire de $E \otimes L$ dans F qui à $x \otimes l$ associe $a(x \otimes l) = lx$, a est une application linéaire continue de norme 1. Montrons que si X est compact, $a(E \otimes L)$ est dense dans F : il en résulte que a est un isomorphisme d'espaces de Banach de $E \hat{\otimes} L$ sur F. Soient $f \in F$ et $\varepsilon > 0$, il existe une fonction g localement constante sur X telle que $|f - g| \leqslant \varepsilon$. Le compact X est ainsi recouvert par une famille finie (U_i) de parties ouvertes et fermées, telles que la restriction de g à U_i soit une constante b_i. Soit h_i la fonction caractéristique de U_i, h_i est continue et $g = \Sigma' b_i h_i$, mais $h_i \in E$, et :

$$g = a(\Sigma' h_i \otimes b_i) \quad \text{donc} \quad g \in a(E \otimes L),$$

ce qui prouve que a est un isomorphisme.

On en déduit par exemple que les bases normales de $C(\mathbf{Z}_p, \mathbf{Q}_p)$ construites au § 3.2 sont aussi des bases normales du K-espace vectoriel $C(\mathbf{Z}_p, K)$ dès que K est un corps complet contenant $\mathbf{Q}_p$, que la valuation de K soit ou non discrète.

EXERCICE. — Soit K[X] l'espace des polynômes à coefficients dans K, montrer à l'aide des résultats du § 3.3 que le complété de K[X] pour la norme $|\sum a_i X^i| = \text{Sup}\,|a_i|$ admet la famille $(X^i)_{i\geqslant 0}$ pour base normale (on suppose ici K complet, donner un énoncé analogue si K n'est plus supposé complet).

3.4.2. *Fonctions continues de plusieurs variables*

Soient X et Y deux espaces compacts, $E = C(X, K)$, $F = C(Y, K)$ et $G = C(X \times Y, K)$, où K est un corps valué complet. Les espaces E, F et G munis de la norme de la convergence uniforme sur X, Y et $X \times Y$ respectivement sont des espaces de Banach. L'application bilinéaire b de $E \times F$ dans G définie par $b(e,f) = ef$ est de norme 1. Il existe donc une unique application linéaire continue b' de $E \otimes F$ dans G telle que $b'(e \otimes f) = ef$, et $|b'| = 1$. Notons encore b' le prolongement continu de b' à $E \hat{\otimes} F$, alors b' *est un isomorphisme d'espaces de Banach.* Comme dans l'exemple précédent la seule vérification non triviale concerne la densité de $b'(E \otimes F)$ dans G. Soient donc $g \in G$ et $\varepsilon > 0$: il existe une fonction h localement constante sur $X \times Y$ telle que $|g - h| \leqslant \varepsilon$. Les ouverts de la forme $U \times V$, où U est un ouvert de X et V un ouvert de Y, forment une base de la topologie de $X \times Y$. Il existe donc deux familles finies U_i et V_i d'ouverts de X et Y respectivement tels que $(U_i \times V_i)$ forme un recouvrement de $X \times Y$ et que la restriction de h à $U_i \times V_i$ soit constante. Pour un tel recouvrement fini U_i et V_i sont à la fois ouverts et fermés (s'ils sont deux à deux disjoints, ce que l'on peut supposer). Soit e_i (resp. f_i) la fonction caractéristique de U_i (resp. V_i), alors $e_i \in E$, $f_i \in F$ et $h = b'(\sum b_i e_i \otimes f_i)$, donc $h \in b'(E \otimes F)$.

Par exemple, si K est un sur-corps complet de $\mathbf{Q}_p$, les polynômes de deux variables $Q_{n,m}(x,y) = \binom{x}{n}\binom{y}{m}$, où $(n, m) \in \mathbf{N}^2$, constituent une base normale de $C(\mathbf{Z}_p^2, K)$. Peut-on par ce moyen trouver des bases normales de $C(\mathbf{Z}_p \times \mathbf{Z}_q, K)$ si p et q sont des nombres premiers et $p \neq q$?

3.5. ALGÈBRES DE BANACH

Parmi les espaces fonctionnels que nous étudierons au chapitre 4, la plupart sont aussi des algèbres.

DÉFINITION 3.5.1. — *Une algèbre* A *sur le corps valué* K, *munie d'une norme ultramétrique, est une* ALGÈBRE NORMÉE *(ultramétrique) si, pour tous x et y dans* A, $|xy| \leqslant |x|\,|y|$. *C'est une* ALGÈBRE DE BANACH, *si c'est un espace complet. On dit que la norme est* MULTIPLICATIVE *si, pour tous x et y,* $|xy| = |x|\,|y|$.

Remarquons qu'une algèbre de Banach à norme multiplicative est intègre. Son corps de fractions est un corps valué. Le sous-corps K.1 est isomorphe à K, et la norme de A induit sur K la valeur absolue de K : le corps des fractions de A est donc un sur-corps valué de K dont la valeur absolue prolonge celle de K. Sauf mention contraire, les algèbres considérées ici sont unitaires.

EXEMPLES. — 1. Les algèbres C(X, K), B(X, K), $C_0(X, K)$ sont des algèbres de Banach (cf. 3.1). De même, si A est une algèbre de Banach, B(X, A), C(X, A), $C_0(X, A)$ sont des algèbres de Banach. A quelle condition, sur l'espace localement compact X, l'algèbre $C_0(X, A)$ est-elle unitaire ? Si la norme de l'une de ces algèbres est multiplicative, X est réduit à un point.

2. Soit A une algèbre normée sur K. Il existe sur l'espace de Banach A' complété de A une unique structure d'algèbre normée prolongeant celle de A (xy est défini

par continuité). Si la norme de A est multiplicative, il en est de même sur A'.

3. L'anneau K[X] muni de la norme :

$$|\Sigma a_i X^i| = \mathrm{Sup}\,|a_i|$$

est une algèbre normée, à norme multiplicative : la norme du complété K[X] est donc aussi multiplicative.

4. Soient A une algèbre sur K et w une application de A dans $\mathbf{R} \cup \{\infty\}$, satisfaisant, pour tous x et y dans A et tout $b \in K$:

$$\begin{aligned} w(bx) &= v(b) + w(x) \\ w(xy) &\geqslant w(x) + w(y) \\ w(x+y) &\geqslant \mathrm{Inf}\,(w(x), w(y)). \end{aligned}$$

Soit r le réel positif tel que, pour $b \in K$, $|b| = r^{v(b)}$; alors $|x| = r^{w(x)}$ munit A d'une structure d'algèbre normée. Si de plus $w(xy) = w(x) + w(y)$, la norme est multiplicative. Réciproquement, si $|x|$ est une norme d'algèbre sur A, $w(x) = a\,\mathrm{Log}\,|x|$, où a est choisi de telle sorte que $v(b) = a\,\mathrm{Log}\,|b|$ pour $b \in K$, a les propriétés indiquées ci-dessus, w est une valuation si et seulement si la norme est multiplicative.

Exercice. — Dans une algèbre normée A, on dit que le produit $\prod_{i\in I} u_i$ est convergent s'il existe un élément non nul $u \in A$ tel que, pour tout $\varepsilon > 0$, il existe une partie finie J de I ayant la propriété suivante : pour toute partie finie J' de I contenant J :

$$|u - \prod_{i\in J'} u_i| \leqslant \varepsilon.$$

Si A est une algèbre de Banach ultramétrique à norme multiplicative, pour que le produit $\prod_{i\in I} u_i$ soit convergent, il faut et il suffit que :

(i) $u_i \neq 0$ pour tout i, et
(ii) $|u_i - 1| \to 0$ suivant le filtre des complémentaires des parties finies de I.

Proposition 3.5.2. — *Soient* A *et* B *deux algèbres normées sur* K, f *un homomorphisme continu de* A *dans* B. *Si la norme de* B *est multiplicative,* $|f| \leqslant 1$.

En effet, f est une application linéaire continue, soit $M = |f| = \mathrm{Sup}_{x\neq 0}\,(|f(x)|/|x|)$, alors, pour $n \geqslant 1$:

$$|f(x^n)| \leqslant M\,|x^n| \leqslant M\,|x|^n.$$

La norme de B étant multiplicative :

$$|f(x^n)| = |(f(x))^n| = |f(x)|^n,$$

d'où, pour $n \geqslant 1$, $|f(x)| \leqslant M^{1/n}\,|x|$, et $|f(x)| \leqslant |x|$.

Corollaire 3.5.3. — *Soient* A *et* B *deux algèbres à norme multiplicative sur le corps* K, K *non discret, et soit* f *un isomorphisme algébrique de* A *sur* B. *Si* f *est continue, c'est un isomorphisme d'algèbres normées* (*i.e.* une isométrie).

Soient en effet K et L les corps de fractions de A et B respectivement, K_0 et L_0 leurs boules unité. Soient x et $y \in A$, n et m deux entiers, alors :

$$|x|^n \leqslant |y|^m \Rightarrow x^n \in y^m K_0 \Rightarrow f(x)^n \in f(y)^m L_0 \Rightarrow |f(x)|^n \leqslant |f(y)|^m.$$

On en déduit qu'il existe un réel $a > 0$ tel que, pour tout $x \in A$, $|f(x)| = |x|^a$. Alors, pour $b \in K$:

$$|f(bx)| = |b|\,|f(x)| = |b|^a\,|x|^a$$

s'il existe $b \in K^*$ tel que $|b| \neq 1$, $a = 1$; or K est non discret, donc il existe un tel b, et f est une isométrie.

3.5.4. *Exemples d'algèbres de séries de Laurent*

Soit K un corps valué; notons A l'algèbre des « pseudo-polynômes », c'est-à-dire des séries formelles $f = \sum_{n\in\mathbf{Z}} a_n X^n$ telles que les a_n soient presque tous nuls, muni de sa structure naturelle d'anneau (l'unique structure d'anneau pour laquelle K[X] est un sous-anneau). Soit $m \in \mathbf{R}$, on pose, pour $f \in A$, $f \neq 0$:

$$v(f, m) = \mathrm{Inf}_n\,(v(a_n) + nm),$$

et $v(0) = +\infty$. On vérifie très facilement que, pour m fixé, $f \to v(f, m)$ est une valuation sur A, qui prolonge celle de K. Elle munit donc A d'une structure *d'algèbre normée à norme multiplicative*. La norme $|f|_m$ de f étant d'ailleurs :

$$|f|_m = \operatorname*{Max}_{n \in \mathbf{Z}} |a_n| r^n,$$

où, pour $b \in \mathrm{K}$:

$$(\operatorname{Log} r)/m = \operatorname{Log} |b|/v(b), \quad r = 1 \quad \text{si} \quad m = 0.$$

Notons A_m le complété de A pour la norme $|f|_m$: on sait que c'est une algèbre de Banach à norme multiplicative.

PROPOSITION 3.5.4. — *L'algèbre* A_m *complétée de* A *pour la norme* $|f|_m$ *est l'algèbre des séries de Laurent* $f = \sum_{n \in \mathbf{Z}} a_n \mathrm{X}^n$ *telles que* $v(a_n) + nm \to +\infty$ *quand* $n \to \pm\infty$.

Il est clair que l'ensemble B_m des séries de Laurent f telles que $v(a_n) + nm \to +\infty$ est un espace vectoriel contenant A, et que la norme $|\ |_m$ définie sur B_m par $v(f, m) = \operatorname{Inf}(v(a_n) + nm)$ et $|f|_m = r^{v(f,m)}$ prolonge la norme $|f|_m$ de A. Il suffit donc de montrer que A est dense dans B_m et que B_m est complet pour que la proposition en résulte. La structure d'algèbre de B_m, qui n'a été précisée à aucun moment, est définie par le fait que A est dense dans B_m. Pour montrer cette dernière assertion, il suffit de remarquer que si $f \in \mathrm{B}_m$, soit $\varepsilon > 0$, il existe N tel que, pour $n > \mathrm{N}$, $|a_n| r^n \leqslant \varepsilon$. Soit :

$$g = \sum_{|n| < \mathrm{N}} a_n \mathrm{X}^n,$$

alors $g \in \mathrm{B}_m$, $|f - g| \leqslant \varepsilon$, et $f - g \in \mathrm{A}$, donc A est dense.

On peut donner des formules « explicites » définissant le produit fg de deux éléments f et g de $\mathrm{A}_m = \mathrm{B}_m$. Soient $f = \sum_{n \in \mathbf{Z}} a_n \mathrm{X}^n$ et $g = \sum_{m \in \mathbf{Z}} b_m \mathrm{X}^m$, alors, pour tout $k \in \mathbf{Z}$, la famille $(a_n b_{k-n})_{n \in \mathbf{Z}}$ est sommable, soient $c_k = \sum_{n \in \mathbf{Z}} a_n b_{k-n}$

et $h = \sum_{k \in \mathbf{Z}} c_k \mathrm{X}^k$, alors $h \in \mathrm{B}_m$ et $fg = h$. On sait que l'espace $c_{\mathrm{K}}(\mathbf{Z})$ des familles sommables indexées dans $\mathbf{Z}$ est complet. Soient f et $g \in \mathrm{A}$, alors le produit $h = fg$ est bien donné par les formules précédentes, en particulier, la famille $(a_n b_{k-n})$ est sommable : il en est donc de même pour f et $g \in \mathrm{B}_m$. Pour $k \in \mathbf{Z}$, la forme linéaire :

$$f \to p_k(f) = a_k$$

est continue. Donc les coefficients (c_k) ci-dessus définis sont les valeurs $p_k(fg)$ pour tous f et g de B_m. Nous montrerons ci-dessous que B_m est complet, il en résulte alors que $fg \in \mathrm{B}_m$.

Soit f_k une suite de Cauchy dans B_m, $f_k = \sum_{n \in \mathbf{Z}} a_{nk} \mathrm{X}^n$.

Pour chaque $n \in \mathbf{Z}$, la suite $p_n(f_k)$ converge vers un élément a_n de K. Soit $\mathrm{M} \in \mathbf{R}$, il existe K(M) tel que, pour $k \geqslant \mathrm{K}(\mathrm{M})$, $\operatorname{Inf}_n((v(a_n - a_{nk})) \geqslant \mathrm{M}$. Fixons un tel k, il existe N(M) tel que, pour $|n| \geqslant \mathrm{N}(\mathrm{M})$, $v(a_{nk}) + nm \geqslant \mathrm{M}$. Alors, pour $|n| \geqslant \mathrm{N}(\mathrm{M})$, $v(a_n) + nm \geqslant \mathrm{M}$, donc :

$$f = \sum_{n \in \mathbf{Z}} a_n \mathrm{X}^n \in \mathrm{B}_m,$$

B_m est complet, et la proposition est démontrée.

Dans les algèbres de Banach sur $\mathbf{C}$, on définit un homomorphisme continu du groupe additif de A dans le groupe multiplicatif des éléments inversibles de A au moyen de la série exponentielle. Dans le cas ultramétrique, la série exponentielle ne converge plus sur A tout entier, mais seulement sur une boule de A.

Nous supposerons désormais que K est de caractéristique 0, p est le nombre premier tel que $|p| < 1$. Nous supposerons également que la valeur absolue de K et sa valuation prolongent celles de $\mathbf{Q}_p$.

PROPOSITION 3.5.5. — *Soit* A *une algèbre de Banach sur le corps* $\mathrm{K} \supseteq \mathbf{Q}_p$.

(i) *La série de terme général* $a^n/n!$ *converge dans* A *pour tout* $a \in \mathrm{A}$ *tel que* $|a| < p^{-1/p-1}$.

(ii) *La somme de cette série, notée exp (a), définit un homomorphisme continu du sous-groupe additif :*

$$G = \{a \in A \mid |a| < p^{-1/p-1}\}$$

sur un sous-groupe multiplicatif M *de l'ensemble des éléments inversibles de* A.

(iii) *La série de terme général* $(-1)^{n-1}(a-1)^n/n$ *converge lorsque* $|a-1| < 1$. *Sa somme, notée Log a, définit un homomorphisme continu du sous-groupe multiplicatif :*

$$L = \{a \in A \mid |a-1| < 1\}$$

sur un sous-groupe additif de A *contenant* G.

(iv) *Pour* $x \in G$ *et* $y \in M$, $y \in L$ *et* $exp\,(Log\,y)) = y$, $Log\,(exp\,x) = x$.

(v) *Si la norme de* A *est multiplicative, les séries exp et Log convergent au point a si et seulement si* $a \in G$ *(resp.* $a \in L$).

PREUVE. — Montrons d'abord (v) : (i) et la convergence de la série Log sur L en résultent dans le cas général, car alors $|a^n| \leqslant |a|^n$.

LEMME 3.5.6. — *Soient :*

$$n > 0, \quad n = n_0 + n_1 p + \ldots + n_h p^h$$

son développement en numération à base p, et :

$$Schiff_p\,(n) = n_0 + \ldots + n_h$$

la somme des chiffres de ce développement, alors :

$$v_p(n!) = (n - Schiff_p\,n)/p - 1.$$

Notons $[x]$ la partie entière du réel x, c'est-à-dire l'entier défini par $[x] \leqslant x < 1 + [x]$. Parmi les entiers $i = 1, \ldots, n$ il y en a $[n/p^k]$ qui sont divisibles par p^k. Il y en a donc $[n/p^k] - [n/p^{k+1}]$ dont la valuation p - adique est égale à k. Alors :

$$v_p(n!) = \sum_{1 \leqslant i \leqslant n} v_p(i) = \sum_{k \geqslant 1} k([n/p^k] - [n/p^{k+1}]) = \sum_{k \geqslant 1} [n/p^k].$$

Or :

$$[n/p^k] = \sum_{i \geqslant k} n_i p^{i-k},$$

d'où le lemme.

La série de terme général $a^n/n!$ converge si et seulement si son terme général tend vers 0, c'est-à-dire si et seulement si $w(a^n/n!) \to +\infty$, où $w(x) = -\mathrm{Log}\,|x|/\mathrm{Log}\,p$, or :

$$w(a^n/n!) = nw(a) - v(n!)$$

et : $\quad Schiff_p\,n \leqslant (p-1)\,(1 + [\mathrm{Log}\,n/\mathrm{Log}\,p]),$

donc $w(a^n/n!) \to +\infty$ lorsque $w(a) > 1/p - 1$. De plus, pour $n = p^h$, $v_p(n!) = \dfrac{n-1}{p-1}$, donc pour que :

$$w(a^n/n!) \to +\infty$$

il faut que $w(a) > 1/p - 1$, ce qui prouve la partie de (v) concernant l'exponentielle. De même, pour que :

$$w((-1)^{n-1}a^n/n) = w(a^n/n) = nw(a) - v(n) \to +\infty,$$

il faut et il suffit que $w(a) > 0$, car $v(n) \leqslant \mathrm{Log}\,n/\mathrm{Log}\,p$, et, pour $n = p^h$, $v(n) = \mathrm{Log}\,n/\mathrm{Log}\,p$.

Pour prouver (ii), il suffit d'observer que l'identité formelle $\exp(X+Y) = \exp X \exp Y$ (où $\exp X = \sum_{n \geqslant 0} X^n/n!$) entraîne que l'application $a \to \exp a$ définie par cette série dans son domaine de convergence est un homomorphisme de la structure additive de A dans sa structure multiplicative. Comme G est un sous-groupe, il suffit de montrer la continuité de exp à l'origine pour prouver que c'est un homomorphisme continu de G sur un sous-groupe multiplicatif M de A; M est alors nécessairement contenu dans l'ensemble des éléments inversibles. Or :

$$v(n!) \leqslant n/p - 1,$$

donc : $\quad w(a^n/n!) \geqslant n(w(a) - 1/p - 1),$

donc : $w(\exp a - 1) \geqslant \inf_{n \geqslant 1} w(a^n/n!) = w(a) - 1/p - 1.$

Ceci prouve la continuité à l'origine, et aussi que $M \subset L$.

Pour prouver (iii), montrons d'abord que L est un sous-groupe multiplicatif. Si $a \in L$ et $b \in L$:

$$ab = 1 + (a - 1) + (b - 1) + (a - 1)(b - 1),$$

donc : $ab \in L.$

De même, pour $a \in L$, la série de terme général $(1 - a)^n$ converge vers un élément b tel que $b \in L$ et $ab = 1$: L est donc un sous groupe. Nous avons vu que la série Log converge sur L : l'identité formelle :

$$\text{Log}(X + Y) = \text{Log } X + \text{Log } Y$$

montre que cela définit un homomorphisme de L dans le groupe additif de A. La continuité au point $a = 1$ résulte de ce que, pour $w(a - 1) > 1/p - 1$:

$$\inf_{n \geqslant 1} w((a - 1)^n/n) \geqslant w(a).$$

L'image de L par cet homomorphisme contient G d'après (iv). Et (iv) résulte des identités formelles classiques.

Exercices 3.5.6. — On conserve les notations de la proposition 3.5.5.

1. Soit $a \in A$, l'application $n \to a^n$ de N dans A se prolonge en une application continue f_a de Z_p dans A lorsque $|a - 1| < 1$. L'application $a \to f_a$ de L dans $C(Z_p, A)$ est un homomorphisme continu et injectif de L sur un sous-groupe multiplicatif de $C(Z_p, A)$.

2. Soit $HC(Z_p, A^*)$ le groupe des homomorphismes continus de Z_p dans le groupe des éléments inversibles de A, muni de la topologie induite par $E = C(Z_p, A)$. Si la norme de A est multiplicative, $a \to f_a$ est un isomorphisme de groupes topologiques de L sur $HC(Z_p, A^*)$.

3. On choisit $A = C_p$, on note alors $Z_p^* = HC(Z_p, C_p^*)$ (dual p - adique de Z_p). Montrer que le groupe de torsion T de Z_p^* est réunion d'une famille croissante T_n de sous-groupes cycliques finis, où T_n est d'ordre p^n. Le sous-espace vectoriel de E engendré par T est dense dans E.

4. Soient E' le dual de E, Q_n le n-ième polynôme binomial, $Q_n(x) = \binom{x}{n}$. Si $\mu \in E'$, on note $\mu_n = \mu(Q_n)$. Soit $a \in C_p$ tel que $|a - 1| < 1$, calculer $\mu(f_a)$. Soient $x \in Z_p$, et $\delta_x \in E'$ définie par $\delta_x(f) = f(x)$ si $f \in E$. Montrer que $X \to \delta_x(X)$ est, pour x fixé, un homomorphisme continu de Z_p^* dans L. Pour $x = 1$ c'est l'inverse de l'application $a \to f_a$ étudiée en 2.

5. Soit g un homomorphisme continu de Z_p^* dans L (c'est en particulier un élément de E'); il existe une suite a_n d'entiers positifs tels que, pour $t \in T_n$, $g(t) = t(1)^{a_n}$. Une telle suite a_n est une suite de Cauchy dans Z_p, soit x sa limite. Alors, pour tout $X \in Z_p^*$, $g(X) = X(1)^x = X(x)$ et $g = \delta_x$.

6. A une famille $(c_x)_{x \in Z_p} = c$ appartenant à $c_{0_p}(Z_p)$ on associe l'élément $d(c) = \sum_{x \in Z_p} c_x \delta_x$. On note D l'image de $c_{0_p}(Z_p)$ par d : on appelle distributions à support discret les éléments de D. Alors d est une application linéaire continue, injective, de norme 1, et $(\delta_x)_{x \in Z_p}$ est une base normale du sous-espace fermé D de E'. Montrer que $D \neq E'$.

7. Soit $b_0 = \exp p, b_1, \ldots, b_n, \ldots$ une suite d'éléments de C_p tels que $b_n^p = b_{n-1}$. Pour tout $n \geqslant 1$, $b_n \in T$. On note $B_n = p^{1-n} Z_p$ la boule de centre 0 et de rayon p^{n-1} dans Q_p. Pour $x \in B_n$, on pose $e_n(x) = b_n^{p^{n-1}x}$, alors e_{n-1} est la restriction de e_n à B_{n-1} et on pose $e(x) = e_n(x)$ pour $n + v(x) > 0$. On définit ainsi un homomorphisme continu e du groupe additif de Q_p dans L, prolongeant l'exponentielle. Soient e' et e'' deux homomorphismes continus de Q_p dans L dont les restrictions à Z_p coïncident; alors, pour tout $n \geqslant 1$, $e'(p^{-n})/e''(p^{-n})$ est racine p^n-ième de 1. Soient $V = Z_p^*/T$ le quotient de Z_p^* par son sous-groupe de torsion et $Q'_p = HC(Q_p, C_p^*)$ le groupe des homomorphismes continus de Q_p dans C_p. Montrer que V et Q'_p sont des groupes topologiques canoniquement isomorphes.

CHAPITRE 4

Fonctions analytiques

Dans ce chapitre, K est un corps valué ultramétrique complet de caractéristique 0, A son anneau de valuation, M l'idéal de valuation, $\mathbf{f} = A/M$. Soit p la caractéristique de $\mathbf{f}$, on supposera parfois que $v(p) = 1$ et $|p| = p^{-1}$: on dira alors que valuation et valeur absolue sont normalisées.

4.1. SÉRIES ENTIÈRES ET FONCTIONS ANALYTIQUES

Soient $f(X) = \sum_{n \geqslant 0} a_n X^n$ une série entière à coefficients dans K et L une extension complète de K. Pour $x \in L$, la série numérique $\sum_{n \geqslant 0} a_n x^n$ converge si et seulement si $|a_n|\,|x^n| \to 0$. Par définition, le RAYON DE CONVERGENCE $R(f)$ de f est :

$$R(f) = \mathrm{Sup}\{r \in \mathbf{R} \mid |a_n|\, r^n \to 0\},$$

alors : $$R(f)^{-1} = \overline{\lim}\,(|a_n|^{1/n}).$$

Il est clair que si $x \in K$, $\sum_{n \geqslant 0} a_n x^n$ converge pour $|x| < R(f)$ et diverge pour $|x| > R(f)$: si K est à valuation discrète cette propriété ne suffit pas à caractériser $R(f)$, c'est pourquoi nous avons donné la définition ci-dessus (si K est à valuation dense $R(f)$ est caractérisé par cette propriété). De plus, soit $R = R(f)$, il sera utile

de distinguer suivant que $|a_n|\,R^n \to 0$ ou non, ce que l'on ne peut pas faire à l'aide de l'ensemble des $x \in K$ tels que $a_n x^n \to 0$, lorsque $R \notin |K^*| = \{|x| \mid x \in K^*\}$. Nous noterons $R(f) \geqslant R^+$ si $a_n R^n \to 0$.

De même, si $a \in K$ et $r > 0$, ces données définissent deux boules $B(a, r)$ et $B'(a, r)$, qui peuvent coïncider (si $r \notin |K^*|$). Par définition le DISQUE OUVERT (resp. FERMÉ) de centre a et de rayon r, noté $D(a, r)$ (resp. $D'(a, r)$), est un objet abstrait. Pour toute extension L de K, $D(a, r)$ et $D'(a, r)$ définissent deux boules de L :

$$B(a, r) = \{x \in L \mid |x - a| < r\}$$

et : $$B'(a, r) = \{x \in L \mid |x - a| \leqslant r\}.$$

Par exemple $D(a, r)$ peut être considéré comme la collection des boules $B(a, r)$ de toutes les extensions L de K. Alors, par définition, le DISQUE DE CONVERGENCE de la série entière f est $D'(0, R(f))$ ou $D(0, R(f))$ suivant que $R(f) \geqslant R^+(f)$ ou non.

DÉFINITION 4.1.1. — *Soient $a \in K$ et $r > 0$ et soit f une fonction définie sur la boule fermée $B'(a, r) = B'$ de K. La fonction f est dite strictement analytique sur B' s'il existe une série entière $f_a \in K[[X]]$, dont le disque de convergence contient $D'(0, r)$, et telle que, pour $x \in B'$, $f(x) = \sum_{n \geqslant 0} a_n (x - a)^n$, où $f_a(X) = \sum_{n \geqslant 0} a_n X^n$.*

On montre très facilement les propriétés suivantes :

(i) L'ensemble des fonctions strictement analytiques sur B' est un espace vectoriel, que nous noterons $A(B')$.

(ii) Si $f \in A(B')$, f est continue et dérivable sur B', sa dérivée f' est, pour $x \in B'$:

$$f'(x) = \sum_{n \geqslant 0} n a_n (x - a)^{n-1}, \quad \text{et} \quad f' \in A(B').$$

(iii) Pour tout $k \geqslant 1$, f a une dérivée k-ième $f^{(k)}$, et pour $x \in B'$:

$$f^{(k)}(x) = k! \sum_{n \geqslant k} \binom{n}{k} a_n (x - a)^{n-k}, \quad f^{(k)} \in A(B').$$

En particulier $k!\, a_k = f^{(k)}(a)$.

(iv) Soit f une fonction définie au voisinage de b et indéfiniment dérivable au point b, rappelons que la *série de Taylor* de f au point b est, par définition, la série formelle :

$$f_b(X) = \sum_{k \geqslant 0} f^{(k)}(b)/k!\, X^k.$$

Nous noterons T_b l'application $f \to T_b(f) = f_b$.

PROPOSITION 4.1.2. — *Soit* $f \in A(B')$, *pour tout* $b \in B'$ *la série de Taylor* f_b *de* f *au point* b *a un disque de convergence* $D(f_b) \supseteq D'(0, r)$, *et, pour* $x \in B'$:

$$f(x) = \sum_{n \geqslant 0} f^{(k)}(b)/k!\, (x - b)^k.$$

La preuve de cette proposition repose sur le

LEMME 4.1.3. — *Soient :*

$$f \in A(B'(a, r)), \qquad T_a(f) = f_a = \sum_{n \geqslant 0} a_n X^n,$$

et :

$$M(f, r) = \operatorname*{Sup}_{n \geqslant 0} |a_n|\, r^n,$$

alors :

(i) $f \to M(f, r)$ *est une norme ultramétrique sur* $A(B')$;
(ii) *pour* $x \in B'$, $|f(x)| \leqslant M(f, r)$.

Pour prouver (i) il suffit d'observer que si $f \in A(B')$ la série f_a figurant dans la définition 4.1.1 est nécessairement égale à $T_a(f)$, compte tenu de la remarque (iii), et que T_a est linéaire. Alors (ii) est immédiate, car, pour $x \in B'$, $|f(x)| \leqslant \operatorname{Sup} |a_n|\, |(x - a)|^n$.

La proposition 4.1.2 s'en déduit. En effet, pour $k \geqslant 0$:

$$|f^{(k)}(b)/k!| = \Big| \sum_{n \geqslant k} \binom{n}{k} a_n (b - a)^{n-k} \Big|$$

$$\leqslant \operatorname*{Sup}_{n \geqslant k} \left| \binom{n}{k} a_n \right| r^{n-k} \leqslant r^{-k} \operatorname*{Sup}_{n \geqslant k} |a_n|\, r^n.$$

On en déduit que $R(f_b) \geqslant r^+$, et aussi que la famille $c_{nk} = \binom{n}{k} a_n (b - a)^{n-k} (x - b)^k$ est sommable ($(n, k) \in \mathbf{N}^2$) pour tout $x \in B'$. Alors :

$$\sum_{n \geqslant 0} a_n (x - a)^n = \sum_{n,k} c_{n,k} = \sum_{k \geqslant 0} f^{(k)}(b)/k!\, (x - b)^k = f(x).$$

COROLLAIRE 4.1.4. — *Soit* $f \in A(B')$, *le disque de convergence* $D(f_b)$ *de la série de Taylor de* f *au point* b *est indépendant de* $b \in B'$.

En effet, si $R(f_b) \geqslant R^+$, f est prolongeable en une fonction $\tilde{f} \in A(B'(b, R))$. Pour tout $c \in B'(a, r)$:

$$T_c(\tilde{f}) = T_c(f), \quad \text{donc} \quad R(f_c) \geqslant R^+.$$

Or le disque de convergence de f_b est entièrement défini par l'ensemble des réels R tels que $R(f_b) \geqslant R^+$.

Dans le plan complexe une méthode habituelle de prolongement analytique consiste, étant donné un disque D et une série entière dont le disque de convergence est D, à prolonger la somme f de cette série à l'aide des séries de Taylor de f aux points $b \in D$: cette série f_b converge au moins dans le plus grand disque centré en b contenu dans D, mais lorsqu'elle converge dans un disque qui rencontre le complémentaire de D, sa somme fournit un prolongement de f hors de D. Le corollaire 4.1.4 montre que dans le cas ultramétrique cette méthode est inefficace puisque, pour toute extension L de K, la boule de L définie par le disque de convergence de f_b sera indépendante de b. On est donc amené à définir autrement le prolongement analytique.

DÉFINITION 4.1.5. — *Soient* D *une partie infinie bornée de* K, R(D) *le sous-anneau du corps* K(X) *des fractions rationnelles à coefficients dans* K *constitué des fractions rationnelles sans pôle dans* D. *On identifie* R(D) *à son image naturelle dans* K^D. *On munit* R(D) *de la structure uniforme de la convergence uniforme sur* D. *L'espace* H(D) *complété de* R(D) *pour cette structure*

uniforme est appelé espace des ÉLÉMENTS ANALYTIQUES *sur* D.

Remarquons que, pour tout point $x \in D$ et toute suite $r_k \in R(D)$ convergeant vers $r \in H(D)$, la suite $r_k(x)$ converge vers une valeur $r(x)$ qui ne dépend pas du choix de r_k, mais seulement de r. Les éléments analytiques sont donc aussi des fonctions sur D; nous considérerons toujours que H(D) est un sous-espace de K^D.

D'autre part, dans la plupart des exemples que nous rencontrerons, la topologie de H(D) sera tout simplement définie par la norme de la convergence uniforme sur D. Le lecteur peu familier avec les structures uniformes peut donc se restreindre aux domaines D tels que, pour $r \in R(D)$, $\operatorname{Sup}_{x \in D} |r(x)| = |r|_D$ est fini.

Nous étudierons plus loin (§ 4.7) cette notion d'élément analytique; montrons dès maintenant que c'est une généralisation bien naturelle de la notion de fonction strictement analytique sur une boule.

THÉORÈME 4.1.6. — *Soient* K *algébriquement clos,* $B' = B'(a, r)$ *une boule fermée de* K, $r > 0$; *les espaces* H(B') *(muni de la norme de la convergence uniforme sur* B') *et* A(B') *(muni de la norme* $M(f, r)$*) coïncident.*

Pour simplifier les notations nous supposerons que $a = 0$, on se ramène à ce cas par translation.

LEMME 4.1.7. — *Soient* $f \in A(B')$, $\sum_{n \geqslant 0} a_n X^n$ *sa série de Taylor au point* O, *et* $M(f, r) = Sup\, |a_n|\, r^n$. *Si* $\tilde{k}$ *est infini et* $v(K^*)$ *dense,* $\operatorname{Sup}_{x \in B'} |f(x)| = M(f, r)$.

Supposons d'abord que $r \in |K^*|$, et soit $b \in K$ tel que $|b| = r$; posons $g(X) = \sum_{n \geqslant 0} a_n (bX)^n$, alors $R(g) \geqslant 1^+$, et, pour $|x| \leqslant 1$, $g(x) = f(xb)$: tout revient dans ce cas à prouver le lemme pour $r = 1$. Quitte à multiplier par un scalaire, on peut encore supposer que :

$$M(f, 1) = \operatorname{Sup} |a_n| = 1.$$

Il existe un indice n_0 tel que $|a_{n_0}| = 1$ et, pour $n \geqslant n_0$, $|a_n| < 1$. Soit alors :

$$P(X) = \sum_{0 \leqslant k \leqslant n_0} a_k X^k,$$

on a $M(f - P, 1) < 1$ et $M(P, 1) = 1$. L'image $\overline{P}$ de P dans $\tilde{k}[X]$ n'est pas nulle, donc il existe $\overline{x} \in \tilde{k}$ tel que $\overline{P}(\overline{x}) \neq 0$ (on a supposé $\tilde{k}$ infini). Soient $x \in K$, $x \in \overline{x}$, alors $|P(x)| = 1$. Pour un tel x :

$$f(x) = P(x) + (f(x) - P(x)) \quad \text{avec} \quad |P(x)| = 1$$

et $|f(x) - P(x)| \leqslant M(f - P, 1) < 1$, donc $|f(x)| = 1$.

Ceci prouve le lemme pour $r = 1$, donc aussi pour tout $r \in K^*$.

On a supposé que $v(K^*)$ est dense, donc, pour tout $r > 0$, il existe une suite croissante $r_k \to r$ telle que $r_k \in |K^*|$. Pour tout k, il existe $x_k \in K$ tel que $|x_k| = r_k$ et $|f(x_k)| = M(f, r_k)$. Donc :

$$\lim |f(x_k)| = \lim M(f, r_k) = M(f, r),$$

ce qui prouve le lemme.

REMARQUE. — Le lemme 4.1.7 reste vrai si on suppose seulement $v(K^*)$ dense, que $\tilde{k}$ soit infini ou non, comme nous le verrons à la fin du § 4.2.

Rappelons que nous avons montré que, étant donné un réel m, l'espace B_m des séries de Laurent $f = \sum_{n \in Z} a_n X^n$ telles que $v(a_n) + nm \to +\infty$, muni de la norme :

$$|f| = \operatorname{Sup}_n |a_n|\, r^n \quad \text{où} \quad m \operatorname{Log} p = v(p) \operatorname{Log} r,$$

est complet, que le sous-espace des pseudo-polynômes f ($a_n = 0$ pour presque tout n) y est dense, et que le prolongement continu de la multiplication des pseudo-polynômes à B_m fait de B_m une algèbre de Banach à norme multiplicative (3.5.4). Soit $B_m^0 = B_m \cap K[[X]]$ le sous-espace des séries entières de B_m. Alors B_m^0 est une sous-

algèbre, et un sous-espace fermé de B_m ($B_m^0 = \bigcap_{n<0} p_n^{-1}(0)$, et p_n est continue, cf. 3.5.4). Avec ces notations :

LEMME 4.1.8. — *L'application* T_a *de* $A(B')$ *dans* $K[[X]]$ *qui à* $f \in A(B')$ *associe sa série de Taylor* $T_a(f)$ *au point* a *est un isomorphisme d'espaces vectoriels normés de* $A(B')$ *sur* B_m^0. *En particulier* $A(B')$ *est complet, c'est un sous-anneau de* $K^{B'}$, *et* T_a *est un isomorphisme d'algèbres de Banach.*

Autrement dit : une limite uniforme sur B' de fonctions analytiques est analytique et le produit de deux fonctions analytiques est analytique, la norme $M(f, r)$ est multiplicative.

Il est clair, par définition de $A(B')$, que, pour $f \in A(B')$, $T_a(f) \in B_m^0$. De plus T_a est linéaire, et, d'après la définition, $M(f, r) = |T_a(f)|$, donc T_a est une isométrie.

T_a est surjective : si $g \in B_m^0$, $g = \sum_{n \geqslant 0} a_n X^n$, la fonction f définie sur B' par $f(x) = \sum_{n \geqslant 0} a_n (x - a)^n$ est dans $A(B')$, et $T_a(f) = g$. Donc T_a est un isomorphisme d'espaces normés : il en résulte que $A(B')$ est complet. De plus, la structure d'algèbre sur $A(D')$, image par T_a^{-1} de la structure d'algèbre de B_m^0, définie par :

$$T_a^{-1}(f)\, T_a^{-1}(g) = T_a^{-1}(fg),$$

coïncide avec celle induite par $K^{B'}$ sur le sous-espace des fonctions polynomiales, et ce sous-espace est dense dans $A(B')$. Donc si f et $g \in A(D')$, et quel que soit $x \in B'$, $fg(x) = \lim f_n g_n(x)$, où f_n et g_n sont des suites de fonctions polynomiales convergeant vers f et g, donc :

$$fg(x) = \lim f_n(x)\, g_n(x) = f(x)\, g(x),$$

la structure d'anneau de $A(D')$ définie par T_a^{-1} est bien celle induite par $K^{B'}$.

LEMME 4.1.9. — $R(B') \subseteq A(B')$.

Soit en effet $b \in K$ tel que $|b - a| > r$, et soit $n \geqslant 1$, la formule (formelle) du binôme :

$$(X - b)^{-n} = \sum_{k \geqslant 0} \binom{-n}{k} (X - a/b - a)^k (a - b)^{-n}$$

montre que la série de Taylor en a de la fonction $(x - b)^{-n}$ a pour coefficients :

$$a_k = (a - b)^{-n} \binom{-n}{k} (b - a)^{-k},$$

donc : $\quad |a_k|\, r^k \leqslant |a - b|^{-n} (r/|b - a|)^k.$

La fonction $(x - b)^{-n}$ est donc dans $A(B')$ lorsque $|b - a| > r$. Or, si $R \in R(B')$, R est somme d'un polynôme et d'une combinaison linéaire finie de $(x - b)^{-n}$, où $|b - a| > r$, donc $R \in A(B')$.

PREUVE DU THÉORÈME. — D'après 4.1.9 :

$$R(B') \subseteq A(B'),$$

et, d'après 4.1.7, la norme de $A(B')$ induit sur $R(B')$ la norme de la convergence uniforme sur B' (K est algébriquement clos, donc son corps résiduel est infini et sa valuation dense). Comme $A(B')$ est complet, $H(B') \subseteq A(B')$, mais les polynômes constituent un sous-espace dense de $A(B')$, contenu dans $R(B')$, donc $H(B') = A(B')$.

COROLLAIRE 4.1.10. — *Sous les hypothèses du théorème* 4.1.6, *soient* D *un ouvert de* K, $a \in D$, $f \in H(D)$ *et* $B' = B(a, r)$ *une boule fermée contenue dans* D, *la restriction de* f *à* B' *est strictement analytique sur* B'. *En particulier,* f *est indéfiniment dérivable sur* D.

Soit en effet i l'injection naturelle de $R(D)$ dans $R(B')$ (restriction). Elle est continue, car :

$$|i(f)| = \operatorname{Sup}_{x \in B'} |f(x)| \leqslant \operatorname{Sup}_{x \in D} |f(x)|.$$

Elle se prolonge donc en une injection continue de $H(D)$ dans $H(B') = A(B')$.

COROLLAIRE 4.1.11. — *Soient* $D' = D'(a, r)$ *une boule fermée et* $f \in A(D')$, *si* K *est algébriquement clos, pour tout* $b \in K$ *tel que* $|b - a| \leqslant r$, *on a :*

$$\operatorname{Sup}_{k \geqslant 0} |f^{(k)}(b)/k!|\, r^k = |f|_{D'} = \operatorname{Sup}_{|x-a| \leqslant r} |f(x)|.$$

On appelle ces relations : INÉGALITÉS DE CAUCHY.

COROLLAIRE 4.1.12. — *Sous les hypothèses de* 4.1.11 *on suppose en outre que* $r \in |K^*|$, *alors :*

$$|f|_{D'} = \operatorname{Sup}_{|x-a| = r} |f(x)| \text{ (PRINCIPE DU MAXIMUM).}$$

On a en effet prouvé cette relation pour démontrer le lemme 4.1.7. On peut de même prouver un analogue du lemme de Schwarz.

On dit qu'une fonction f définie sur K y est une FONCTION ENTIÈRE si la restriction de f à toute boule fermée de K est strictement analytique sur cette boule.

COROLLAIRE 4.1.13. — *Si* K *est algébriquement clos, une fonction entière bornée sur* K *est constante* (théorème de Liouville).

Compte tenu des inégalités de Cauchy, la preuve est la même que pour les fonctions analytiques d'une variable complexe. Si, pour tout $x \in K$, $|f(x)| \leqslant M$, alors, pour tout $r > 0$ et tout $k \geqslant 0$, $|f^{(k)}(0)/k!| \leqslant Mr^{-k}$. On en déduit que, pour $k \geqslant 1$, $f^{(k)}(0) = 0$. Remarquons que, si le corps résiduel de k est fini et sa valuation discrète, il existe des fonctions entières bornées sur K (cf. exercice 4.6.2).

Nous indiquons ici deux propriétés qui nous seront utiles aux chapitres 4 et 5.

LEMME 4.1.14. — *Soient* $S_1, \ldots, S_k \in A[X]$, *unitaires, et dont les images dans* $\tilde{k}[X]$ *satisfont* $(\bar{S}_1, \ldots, \bar{S}_k) = 1$. *Soit*

q le degré du p.p.c.m. de $\bar{S}_1, \ldots, \bar{S}_k$, *alors, pour tout* $P \in K[X]$, *satisfaisant* $dg\, P < q$, *il existe une unique représentation :*

(i) $P = U_1 S_1 + \ldots + U_k S_k$ *avec* $dg\,(U_i) < q - dg\, S_i$;
(ii) *de plus* $M(P, 1) = \operatorname{Max}_i (M(U_i, 1))$.

Il est évident que $(S_1, \ldots, S_k) = 1$, d'où l'existence d'une représentation (i) avec :

$$dg\,(U_i) \leqslant dg\,(P) - dg\, S_i < q - dg\,(S_i).$$

Il est aussi évident que, pour une telle représentation, on a $M(P, 1) \leqslant \operatorname{Max}(M(U_i, 1))$, puisque $M(S_i, 1) = 1$. Supposons donc qu'il existe P pour lequel cette inégalité soit stricte : on en déduit qu'il existe des $U_i \in A[X]$ tels que les $\bar{U}_i$ ne soient pas tous nuls, $dg\, U_i < q - dg\, S_i$, et $\Sigma \bar{U}_i \bar{S}_i = 0$, or ceci est impossible, d'où le lemme.

COROLLAIRE 4.1.15. — *Soient* $a_1, \ldots, a_k \in A$, *dont les images* $\bar{a}_i$ *dans* $\tilde{k}$ *sont deux à deux distinctes, soient* $n_1, \ldots, n_k$ *des entiers positifs, et* $Q_1, \ldots, Q_k$ *des polynômes unitaires dans* A[X], *tels que* $\bar{Q}_i = (X - \bar{a}_i)^{n_i}$. *On note :*

$$A_i = \{x \in A \mid |Q_i(x)| = 1\} \quad \textit{et} \quad C = A_1 \cap A_2 \cap \ldots \cap A_k.$$

Pour toute famille (P_i) *de polynômes tels que* $dg\, P_i < n_i$, *on pose* $R_i = P_i/Q_i$ *et* $R = \Sigma R_i$. *Alors, si le corps résiduel* $\tilde{k}$ *est infini, on a :*

$$Sup\{|R(x)| \mid x \in C\} = \operatorname{Max}_i (Sup\{|R_i(x)| \mid x \in A_i\}).$$

Soient $Q = Q_1 \ldots Q_k$ et $S_i = Q/Q_i$, alors les S_i satisfont les hypothèses du lemme 4.1.14 et, de plus, $\bar{Q}$ est le p.p.c.m. des $\bar{S}_i$, donc $q = n_1 + \ldots + n_k$. Soient $R = P/Q$, $dg\, P < q$, et $R = \Sigma P_i/Q_i$, donc $P = \Sigma P_i S_i$. Comme $dg\, P_i < n_i = q - dg\, S_i$, on en déduit :

$$M(P, 1) = \operatorname{Max}(M(P_i, 1)).$$

On a supposé $\tilde{k}$ infini, donc :

$$M(P, 1) = \operatorname{Sup}\{|P(x)| \mid x \in A\};$$

de même :

$$M(P_i, 1) = \mathrm{Sup}\{|P_i(x)| \mid x \in A\}.$$

Or, par définition de C et A_i, $|Q(x)| = 1$ pour $x \in C$, et $|Q_i(x)| = 1$ pour $x \in A_i$. Il suffit donc que :

$$\mathrm{Sup}\{|P(x)| \mid x \in C\} = \mathrm{Sup}\{|P(x)| \mid x \in A\},$$

et : $$\mathrm{Sup}\{|P_i(x)| \mid x \in A_i\} = \mathrm{Sup}\{|P_i(x)| \mid x \in A\},$$

pour que le corollaire en résulte. Or l'image dans $\tilde{k}$ de l'ensemble des $x \in A$ tels que $|P(x)| < M(P, 1)$ est finie, et l'image de C est infinie, donc il existe $x \in C$ tel que $|P(x)| = M(P, 1)$. Les égalités relatives aux P_i se démontrent de la même façon, et le corollaire est démontré (compte tenu de la remarque, triviale, suivant laquelle, pour tout $x \in C$:

$$|R(x)| \leqslant \mathrm{Max}\,|R_i(x)| \leqslant \mathrm{Max}\,(\mathrm{Sup}\{|R_i(x)| \mid x \in A_i\}).$$

Exercices 4.1.16. — 1. Montrer que l'égalité des normes $M(f, r) = \sup_{x \in B'} |f(x)|$ est fausse si la condition « $v(K^*)$ dense » n'est pas satisfaite.

2. Montrer que le lemme 4.1.9 est faux si K n'est pas algébriquement clos.

3. On dit qu'une fonction $f \in C(\mathbf{Z}_p, K)$ est localement analytique sur $\mathbf{Z}_p$ si, pour tout $a \in \mathbf{Z}_p$, il existe une boule $B'(a, r)$ non réduite à $\{a\}$ telle que la restriction de f à $B'(a, r)$ y soit strictement analytique. On note $LA(\mathbf{Z}_p)$ l'espace des fonctions localement analytiques sur $\mathbf{Z}_p$.

a) Si $f \in LA(\mathbf{Z}_p)$, f est indéfiniment dérivable. On note f_x sa série de Taylor au point x, alors $R(f) = \mathrm{Inf}\,R(f_x)$, $x \in \mathbf{Z}_p$, est non nul.

b) Soient $h \geqslant 0$ et $A_h(\mathbf{Z}_p)$ le sous-espace des $f \in LA(\mathbf{Z}_p)$ telles que $R(f) \geqslant (p^{-h})^+$, $A_{h+1} \supseteq A_h$ et $LA(\mathbf{Z}_p) = \bigcup_{h \geqslant 0} A_h(\mathbf{Z}_p)$. Pour $0 \leqslant i < p^h$, on note $B_i = B'(i, p^{-h})$, alors $A_h(\mathbf{Z}_p) = \oplus A(B_i)$. On munit $A_h(\mathbf{Z}_p)$ de la norme $|f|_h$ définie par cette décomposition en somme directe. L'espace des polynômes est dense dans $A_h(\mathbf{Z}_p)$ et, si P est un polynôme, $|P|_h \geqslant |P|_{h+1}$.

c) Soit $Q_n(X) = \binom{X}{n}$ le n-ième polynôme binomial, on rappelle l'identité :

$$Q_n(X + Y) = \sum_{0 \leqslant k \leqslant n} Q_k(X)\, Q_{n-k}(Y).$$

Montrer que :

$$|Q_n|_h \leqslant |[n/p^h]!\,|^{-1}.$$

d) Soit $f = \sum_{n \geqslant 0} b_n Q_n$ une fonction continue sur $\mathbf{Z}_p$, si :

$$\overline{\lim}\,|b_n|^{1/n} < 1, \quad f \in LA(\mathbf{Z}_p).$$

4.2. SÉRIES DE LAURENT

L'étude faite au § 4.1 nous a montré que, pour étudier l'anneau A(B') des fonctions strictement analytiques sur B', on pouvait étudier plutôt l'anneau B_m^0 de leurs séries de Taylor en un point.

Nous noterons $\mathbf{R}''$ la droite achevée :

$$\mathbf{R} \cup \{+\infty\} \cup \{-\infty\},$$

munie de l'ordre, la topologie et l'addition naturels (en particulier $(+\infty) + (-\infty)$ n'est pas défini).

Soit $f(X) = \sum_{n \in \mathbf{Z}} a_n X^n$ une série formelle à coefficients dans K, on note Conv (f) la partie de $\mathbf{R}''$ définie par :

— $+\infty$ (resp. $-\infty$) $\in$ Conv (f) si et seulement si $a_n = 0$ pour $n < 0$ (resp. $n > 0$);

— si $m \in \mathbf{R}$, $m \in$ Conv (f) si et seulement si :

$$v(a_n) + nm \to +\infty \quad \text{quand} \quad |n| \to \infty.$$

On voit donc que $\mathbf{R} \cap$ Conv $(f) = \{m \in \mathbf{R} \mid f \in B_m\}$ (cf. 3.5.4).

Proposition 4.2.1. — *Pour toute série formelle f, Conv (f) est un intervalle de $\mathbf{R}''$ appelé intervalle de convergence de f, Conv $(f) = \mathbf{R}'' \Leftrightarrow f \in K$.*

Si $f = \sum_{n \in \mathbf{Z}} a_n X^n$, nous noterons $f^+ = \sum_{n \geqslant 0} a_n X^n$ et $f^- = \sum_{n < 0} a_n X^n$. Il est clair que :

$$\text{Conv}\,(f) = \text{Conv}\,(f^+) \cap \text{Conv}\,(f^-),$$

$$+\infty \in \text{Conv}\,(f^+) \quad \text{et} \quad -\infty \in \text{Conv}\,(f^-).$$

Or, si $m \in \mathrm{Conv}(f^+)$, pour tout $m' > m$, et tout $n \geqslant 0$, $v(a_n) + nm' \geqslant v(a_n) + nm$, donc $m' \in \mathrm{Conv}(f^+)$, ce qui montre que $\mathrm{Conv}(f^+)$ est une demi-droite $[m_1, +\infty]$ ou $]m_1, +\infty]$. De même $\mathrm{Conv}(f^-)$ est une demi-droite $[-\infty, m_2]$ ou $[-\infty, m_2[$, ce qui prouve la proposition (remarquons qu'il est fort possible que $\mathrm{Conv}(f) = \varnothing$).

DÉFINITIONS 4.2.2. — *Soit* I *un intervalle de* $\mathbf{R}''$, *on note* $\mathrm{L_K(I)}$ *l'ensemble des séries de Laurent* f *à coefficients dans* K *telles que* $\mathrm{Conv}(f) \supseteq \mathrm{I}$. *On pose :*

— *si* $+\infty \in \mathrm{I}$ *(resp.* $-\infty \in \mathrm{I}$*) :*

$$n(f, +\infty) = 0, \quad \mathrm{N}(f, +\infty) = Inf\{n \mid a_n \neq 0\}$$

et : $$v(f, +\infty) = v(a_0)$$

(resp. $n(f, -\infty) = Sup\{n \mid a_n \neq 0\}$, $\mathrm{N}(f, -\infty) = 0$ *et* $v(f, -\infty) = v(a_0)$*);*

— *si* $m \in \mathrm{I} \cap \mathbf{R}$ *:*

$$v(f, m) = \inf_{n \in \mathbf{Z}} (v(a_n) + nm),$$

$$n(f, m) = Inf\{n \in \mathbf{Z} \mid v(a_n) + nm = v(f, m)\},$$

et : $$\mathrm{N}(f, m) = Sup\{n \in \mathbf{Z} \mid v(a_n) + nm = v(f, m)\}.$$

Si $f \neq 0$, toutes les quantités $v(f, m)$, $n(f, m)$ et $\mathrm{N}(f, m)$ sont finies pour $m \in \mathrm{Conv}(f)$. De plus, si $m \in \mathrm{I} \cap \mathbf{R}$, $v(f, m)$ est la valuation de f dans l'anneau A_m.

PROPOSITION 4.2.3. — *Soient* I *un intervalle non vide de* $\mathbf{R}''$, $f = \Sigma a_n \mathrm{X}^n$ *et* $g = \Sigma b_n \mathrm{X}^n$ *deux éléments de* $\mathrm{L_K(I)}$, *alors :*

(i) *pour tout* $k \in \mathbf{Z}$, *la famille* $(a_n b_{k-n})_{n \in \mathbf{Z}}$ *est sommable, soient* c_k *sa somme et* $h = \Sigma c_k \mathrm{X}^k$*;*

(ii) $h \in \mathrm{L_K(I)}$, *et* $fg = h$ *munit* $\mathrm{L_K(I)}$ *d'une structure d'anneau commutatif;*

(iii) *si* $\mathrm{I} \cap \mathbf{R}$ *est non vide,* $\mathrm{L_K(I)}$ *est intègre et, pour* $m \in \mathrm{I} \cap \mathbf{R}$, $f \to v(f, m)$ *est une valuation sur* $\mathrm{L_K(I)}$*;*

(iv) *pour tous* f *et* g *dans* $\mathrm{L_K(I)}$ *et tout* $m \in \mathrm{I}$ *:*

$$n(fg, m) = n(f, m) + n(g, m)$$

et : $$\mathrm{N}(fg, m) = \mathrm{N}(f, m) + \mathrm{N}(g, m).$$

Si $\mathrm{I} = (\{+\infty\})$ ou $\mathrm{I} = (\{-\infty\})$, $\mathrm{L_K(I)}$ se réduit à $\mathrm{K[[X]]}$ ou $\mathrm{K[[1/X]]}$ et les vérifications sont triviales.

Soit donc $m \in \mathrm{I} \cap \mathbf{R}$, alors $\mathrm{L_K(I)}$ est contenu dans A_m, d'où (i), et $h = fg \in \mathrm{A}_m$ quel que soit $m \in \mathrm{I} \cap \mathbf{R}$. Si, par exemple, $+\infty \in \mathrm{I}$, $h \in \mathrm{K[[X]]}$, et finalement :

$$h = fg \in \mathrm{L_K(I)}.$$

Donc, pour tout $m \in \mathrm{I} \cap \mathbf{R}$, $\mathrm{L_K(I)}$ est un sous-anneau de A_m, d'où (ii) et (iii).

Vérifions les relations (iv) relatives, par exemple, à $n(f, m)$.

Pour $n < n(f, m)$:

$$v(a_n) + nm > v(f, m)$$

et pour $k < n(g, m)$:

$$v(b_k) + km > v(g, m).$$

De plus, comme :

$$v(a_n) + nm \to \infty \quad \text{et} \quad v(b_k) + km \to \infty$$

$$\inf_{n < n(f, m)} \{v(a_n) + nm\} = v(f, m) + a$$

et : $$\inf_{k < n(g, m)} \{v(b_k) + km\} = v(g, m) + b$$

où $a > 0$ et $b > 0$.

Alors, pour $k + n < n(f, m) + n(g, m)$:

$$v(a_n b_k) + (k + n)\, m \leqslant v(f, m) + v(g, m) + \mathrm{Inf}\,(a, b),$$

et donc, pour $\mathrm{N} < n(f, m) + n(g, m)$:

$$v(c_{\mathrm{N}}) < v(f, m) + v(g, m) = v(fg, m).$$

Ceci prouve que $n(fg, m) \geqslant n(f, m) + n(g, m)$. Posons $\mathrm{N}_0 = n(f, m) + n(g, m)$, si nous montrons que :

$$v(c_{\mathrm{N}_0}) + \mathrm{N}_0 m = v(fg, m),$$

nous aurons prouvé l'égalité $n(fg, m) = n(f, m) + n(g, m)$. Or, dans la preuve de la proposition 3.5.4, pour montrer que $v(fg, m) = v(f, m) + v(g, m)$ nous avons justement prouvé que $v(c_{N_0}) = v(f, m) + v(g, m) - N_0 m$, d'où la proposition.

REMARQUE 4.2.4. — Soit $x \in K$ tel que :

$$v(x) = m \in \mathrm{Conv}\,(f),$$

alors la famille $a_n x^n$ est sommable dans K et sa somme $f(x)$ satisfait $v(f(x)) \geqslant v(f, m)$. Si de plus m et f sont telles que $n(f, m) = N(f, m)$, c'est-à-dire que parmi la famille $a_n x^n$ un seul terme a la valuation $v(f, m)$, alors $v(f(x)) = v(f, m)$. En particulier, *soit* $m \in Conv\,(f) \cap \mathbf{R}$ *tel que :*

$$n(f, m) = N(f, m),$$

alors pour tout $x \in K$ *tel que* $v(x) = m$, $f(x) \neq 0$. On appelle PENTES EXCEPTIONNELLES *pour une série de Laurent* f *les réels* $m \in Conv\,(f)$ *tels que* $n(f, m) \neq N(f, m)$. On voit que les zéros de la somme de f sont nécessairement situés sur les « cercles » $v(x) = m$ où m est une pente exceptionnelle.

EXERCICES 4.2.5. — On choisit $K = C_p$ et on note :

$$f(X) = \sum_{n \geqslant 1} (-1)^{n-1} X^n/n$$

la série du logarithme, pour $x \in C_p$ et $v(x) > 0$, on note Log $(1 + x)$ la somme de cette série au point x.

1. Si $v(x) > 0$ et s'il existe m tel que $(1 + x)^m = 1$:

$$\mathrm{Log}\,(1 + x) = 0.$$

2. Les pentes exceptionnelles de f sont les nombres :

$$m_h = 1/p^{h-1}(p - 1), \quad h \geqslant 1.$$

3. Montrer, à l'aide des relations (iv) proposition 4.2.3, que le nombre des zéros du logarithme sur le cercle $v(x) = m_h$ est au plus égal à $p^{h-1}(p - 1)$.

4. Décrire l'ensemble des zéros du logarithme dans C_p.

Il est clair, d'après les définitions de $n(f, m)$ et $N(f, m)$, que, pour $m \in \mathrm{Conv}\,(f)$, $n(f, m) \leqslant N(f, m)$. De plus :

PROPOSITION 4.2.6. — *Soient* f *une série de Laurent non nulle et* $I = Conv\,(f)$.

(i) *Les fonctions* $n(f, m)$ *et* $N(f, m)$ *sont non croissantes sur* I.

(ii) *Soit* $m \in I$, *alors :*

— *pour* $m' \in I$, $m' < m$ *et* m' *assez voisin de* m *:*

$$n(f, m') = N(f, m') = N(f, m);$$

— *pour* $m' \in I$, $m' > m$ *et* m' *assez voisin de* m *:*

$$n(f, m') = N(f, m') = n(f, m).$$

(iii) $n(f, m)$ *et* $N(f, m)$ *sont continues respectivement à droite et à gauche sur* I.

Nous allons montrer par exemple que la première assertion (ii) est vraie s'il existe $m' < m$, $m' \in I$: la seconde se démontre de façon analogue, (i) et (iii) s'en déduisent trivialement. Nous distinguerons suivant que $m \in \mathbf{R}$ ou $m = +\infty$.

Posons $N_0 = N(f, m)$: quitte à multiplier f par X^{-N_0}, ce que l'on peut faire grâce aux relations 4.2.3 (iv), on peut supposer que $N_0 = 0$.

Si $m = +\infty$, $a_n = 0$ pour $n < 0$. Soient $m_1 \in I \cap \mathbf{R}$ et N_1 un entier tel que, pour $n > N_1$, $v(a_n) + nm_1 > v(a_0)$. Alors, pour $m' \geqslant m_1$ et $n > N_1$, $v(a_n) + nm' > v(a_0)$. D'autre part, pour $1 \leqslant n \leqslant N_1$, $v(a_n) + nm' \to +\infty$ quand $m' \to +\infty$. Donc, pour m' assez grand :

$$v(a_n) + nm' > v(a_0), \quad \text{pour} \quad n \geqslant 1.$$

Pour un tel m', $n(f, m') = N(f, m') = 0$.

Si $m \in \mathbf{R} \cap I$, soit encore $m_1 < m$, $m_1 \in I$ et soit N_1 un entier tel que, pour $n > N_1$, $v(a_n) + nm_1 > v(a_0)$. Alors, pour tout $m' > m_1$ et $n > N_1$, $v(a_n) + nm' > v(a_0)$. Pour $1 \leqslant n \leqslant N_1$:

$$v(a_n) + nm' \to v(a_n) + nm > v(a_0), \quad \text{lorsque} \quad m' \to m.$$

Donc, pour m' assez voisin de m et $m' > m_1$:

$$v(a_n) + nm' > v(a_0) \quad \text{pour tout} \quad n \geqslant 1.$$

Or, pour $n < 0$ et $m' > m$:

$$v(a_n) + nm' > v(a_n) + nm \geqslant v(a_0).$$

Donc, pour $m' < m$ et assez voisin de m :

$$n(f, m') = \mathrm{N}(f, m') = 0.$$

COROLLAIRE 4.2.7. — *Soit* J *un intervalle compact contenu dans Conv* (f), $f \neq 0$, *alors l'ensemble des pentes exceptionnelles pour* f *appartenant à* J *est fini.*

Soit en effet $m \in \mathrm{I}$, il résulte de 4.2.6 qu'il existe un intervalle ouvert contenant m, soit V, tel que, pour $m' \in \mathrm{V} \cap \mathrm{I}$, $m' \neq m$, m' ne soit pas exceptionnelle. On peut recouvrir J par de tels intervalles, en extraire un recouvrement fini de cardinal N, alors le nombre de pentes exceptionnelles appartenant à J est au plus N.

COROLLAIRE 4.2.8. — *La fonction* $v(f, m)$ *est continue et affine par intervalles sur Conv* (f).

En effet, si $m_1 < m_2$ sont deux pentes exceptionnelles consécutives, alors, pour $m \in [m_1, m_2]$:

$$n(f, m) = \mathrm{N}(f, m) = \mathrm{N}(f, m_2) = n(f, m_1);$$

soit n_0 cette valeur commune, pour $m \in [m_1, m_2]$, on a donc $v(f, m) = v(a_{n_0}) + n_0 m$.

EXERCICE. — Déduire du corollaire 4.2.8 que le lemme 4.1.7 reste vrai si on n'y suppose plus k infini.

DÉFINITION 4.2.9. — *Le* POLYGONE DE NEWTON *de la série de Laurent* f *est le graphe, dans* R''^2, *de la fonction*

$$t \to \mathrm{P}(f, t) = \operatorname*{Sup}_{m \in Conv(f)} (v(f, m) - mt).$$

La fonction $\mathrm{P}(f, t)$ est convexe, puisqu'elle est définie comme enveloppe supérieure de fonctions affines. Nous donnons au § 4.3 une description « géométrique » du polygone de Newton. Ce langage géométrique n'est pas nécessaire pour l'étude ultérieure des séries de Laurent. Il fournit cependant un support intuitif pour les fonctions $v(f, m)$, $n(f, m)$ et $\mathrm{N}(f, m)$ qui est fort utile dans les applications pratiques.

4.3. POLYGONE DE NEWTON

Soit $f = \Sigma a_n \mathrm{X}^n$ une série de Laurent à coefficients dans K, nous appellerons *ensemble représentatif de* f dans $(\mathbf{R}'')^2$, et noterons $\mathrm{P}(f)$, l'ensemble des points $(n, v(a_n))$. Etant donné une droite non verticale d'équation :

$$\mathrm{Y} = a\mathrm{X} + b,$$

on dit qu'un point (X, Y) est au-dessus (resp. au-dessous) de cette droite si $\mathrm{Y} \geqslant a\mathrm{X} + b$ (resp. $\mathrm{Y} \leqslant a\mathrm{X} + b$).

Soit m un réel, on dit que m est *admissible* pour f, si, pour toute droite D_m de pente $-m$, l'ensemble des points de $\mathrm{P}(f)$ situés au-dessous de D_m est fini. En d'autres termes, $m \in \mathbf{R}$ est admissible pour f si et seulement si, pour tout $\mathrm{M} \in \mathbf{R}$, $v(a_n) + nm \geqslant \mathrm{M}$ pour presque tout n, c'est-à-dire si $v(a_n) + nm \to +\infty$. L'ensemble des réels admissibles est donc $\mathrm{Conv}\,(f) \cap \mathbf{R}$.

De même $+\infty$ (resp. $-\infty$) est admissible si $\mathrm{P}(f)$ est situé dans le demi-plan $\mathrm{X} \geqslant 0$ (resp. $\mathrm{X} \leqslant 0$). L'ensemble des éléments admissibles de $\mathbf{R}''$ est donc $\mathrm{Conv}\,(f)$.

Soit m un réel admissible, on appelle m-tangente à $\mathrm{P}(f)$ la plus basse des droites de pente $-m$ qui rencontre $\mathrm{P}(f)$. Soit D_m cette droite, son équation est $\mathrm{Y} + m\mathrm{X} = v(f, m)$.

PROPOSITION 4.3.1. — *Le polygone de Newton de* f *est la frontière de l'enveloppe supérieure convexe de* $\mathrm{P}(f)$.

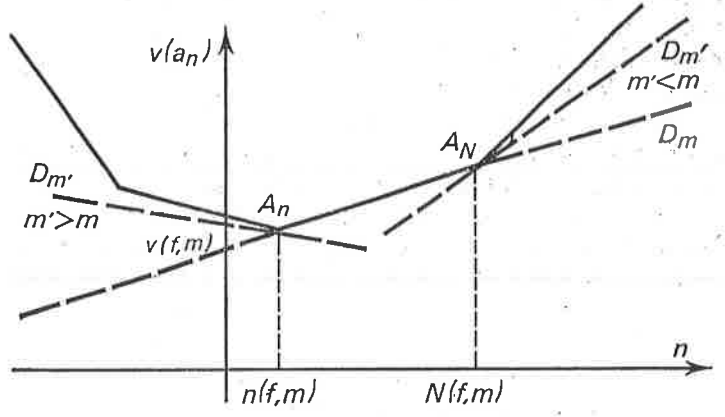
Rappelons que, si D est une droite non verticale, le demi-plan supérieur défini par D est l'ensemble des points situés au-dessus de D. L'enveloppe supérieure convexe d'une partie de $(\mathbf{R}'')^2$ est l'intersection des demi-plans supérieurs la contenant.

Soient m un réel, $\mathscr{D}_m$ l'ensemble des droites de pente $-m$, s'il existe un demi-plan supérieur défini par une droite $D \in \mathscr{D}_m$ qui contient $P(f)$ alors, ou bien m est admissible, ou bien m est extrémité de l'une des deux demi-droites Conv (f^+) ou Conv (f^-). Nous ne traiterons pas le cas où Conv (f) serait vide ou réduit à un point. Sinon, on voit aisément que $\widehat{P(f)}$, enveloppe supérieure convexe de $P(f)$, est encore intersection des demi-plans supérieurs le contenant et définis par une droite $D \in \mathscr{D}_m$ où $m \in$ Conv (f) (autrement dit, on peut négliger les pentes $-m$ où m est extrémité de l'intervalle Conv (f)). Notons S(D) le demi-plan supérieur défini par D; alors, pour $m \in$ Conv (f), $\bigcap S(D)$ pour $D \in \mathscr{D}_m$ et $S(D) \supseteq P(f)$ est $S(D_m)$. Donc :

$(X, Y) \in \widehat{P(f)} \Leftrightarrow$ (pour $m \in$ Conv (f), $Y + mX \geqslant v(f, m)$),

et : $$\widehat{P(f)} = \{(X, Y) \mid Y \geqslant P(f, X)\},$$

d'où la proposition.



Soit m une pente exceptionnelle pour f, alors la m-tangente D_m rencontre $P(f)$ en deux points d'abscisses $n(f, m)$ et $N(f, m)$. Soient A_n et A_N ces deux points. Comme

$\widehat{P(f)}$ contient $P(f)$, le segment $A_n A_N$ est contenu dans $\widehat{P(f)}$, mais comme $\widehat{P(f)}$ est contenu dans le demi-plan $S(D_m)$, le segment $A_n A_N$ est contenu dans le polygone de Newton de f. En d'autres termes :

PROPOSITION 4.3.2. — *Soit m une pente exceptionnelle pour f, alors, pour $n(f, m) \leqslant t \leqslant N(f, m)$, on a :*

$$P(f, t) = v(f, m) - mt.$$

Donnons une démonstration non géométrique de cette proposition. Soient $n = n(f, m)$ et $N = N(f, m)$. Pour tout $m' \in$ Conv (f) :

$$v(f, m') \leqslant v(a_n) + nm' \quad \text{et} \quad v(f, m') \leqslant v(a_N) + Nm'.$$

Alors :

— pour $m' \geqslant m$ et $t \leqslant N$:

$$v(f, m') - m't \leqslant v(a_N) + Nm - mt = v(f, m) - mt;$$

— et pour $m' \leqslant m$ et $t \geqslant n$:

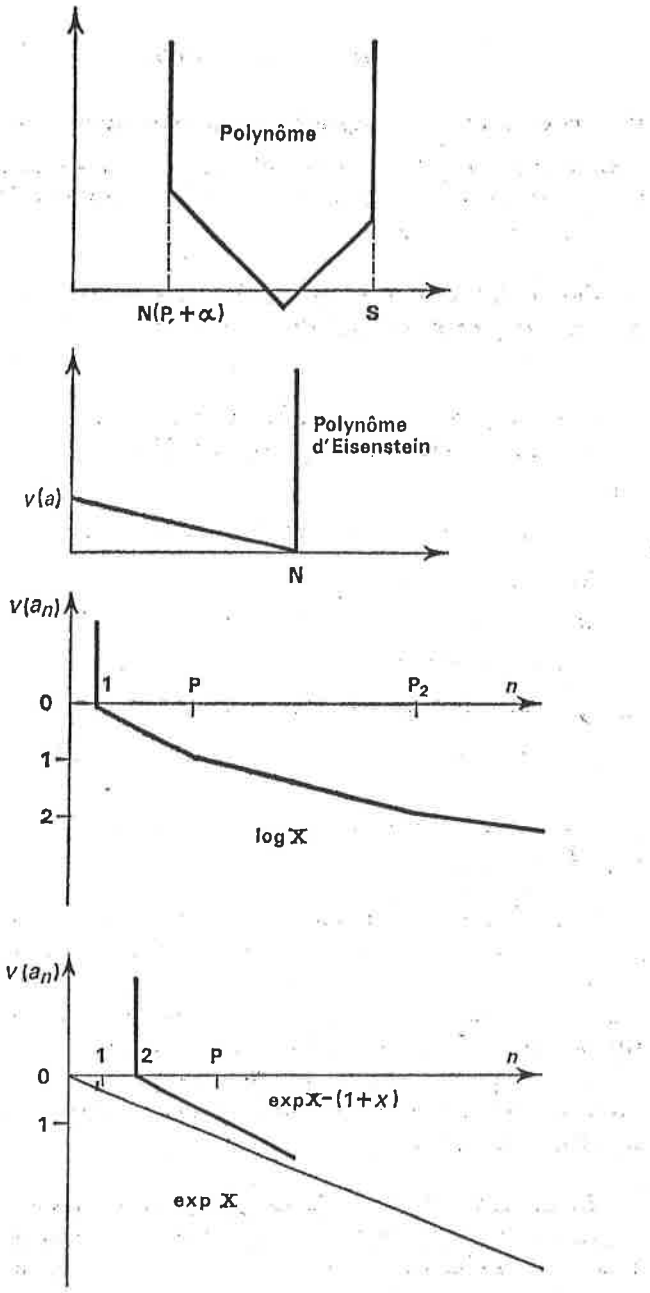
$$v(f, m') - m't \leqslant v(a_n) + nm - mt = v(f, m) - mt.$$

COROLLAIRE 4.3.3. — *La fonction $P(f, t)$ est affine par intervalles.*

Trivial.

On voit donc que le polygone de Newton est un « polygone » en ce sens que son intersection avec toute bande verticale $a \leqslant X \leqslant b$ est une ligne polygonale convexe. Les pentes exceptionnelles pour f sont les pentes des côtés du polygone de Newton. On appellera souvent longueur du côté de pente $-m$ la quantité $N(f, m) - n(f, m)$. Le croquis ci-dessus montre l'interprétation géométrique de la proposition 4.2.6.

EXEMPLES 4.3.4. — 1. Le polygone de Newton d'un polynôme P de degré s comporte : deux demi-droites verticales d'abscisses $N(P, +\infty)$ et s, et, entre ces abscisses,



un nombre fini, au plus égal à s, de segments finis. Si P est un polynôme d'Eisenstein de degré N, il n'y a qu'un seul segment de longueur N et de pente $-v(a)/N$, où a est une uniformisante.

2. Le polygone de Newton de la série du logarithme est constitué d'une demi-droite d'abscisse 1 et d'une suite de segments finis de pente a_h, $h \geqslant 1$, $a_h = -1/p^{h-1}(p-1)$, entre les abscisses $n(f, a_h) = p^{h-1}$ et $N(f, a_h) = p^h$ (cf. exercice 4.2.5).

3. Soit $g(X)$ la série exponentielle, son polygone de Newton est constitué de deux demi-droites, l'une d'abscisse 0, l'autre de pente $-1/p-1$.

4. Le polygone de Newton de $g(X) - (1+X)$ est formé d'une infinité de segments dont le premier a une pente $-1/p-2$. L'équation $\exp x = a$ n'a aucune solution dans $\mathbf{C}_p$ si $v(a-1) \leqslant 0$. Majorer le nombre de solutions suivant les valeurs de $v(a-1)$.

4.4. LEMME DE HENSEL

Nous avons remarqué en 4.2.4 que les zéros de la somme d'une série de Laurent f ont nécessairement pour valuation la pente d'un segment du polygone de Newton de f (pente exceptionnelle). Le lemme de Hensel que nous prouvons ci-dessous nous permettra de donner une description précise de l'ensemble des zéros de f, et de traiter, dans certains cas, les problèmes de divisibilité.

Rappelons que B_m désigne l'anneau $L_K(\{m\})$ des séries de Laurent f telles que $\mathrm{Conv}(f) \ni m$.

DÉFINITION 4.4.1. — *Soit m un réel, un polynôme* P *de degré s est dit* m-DOMINANT *si* $N(P, m) = s$. *Il est dit* m-EXTRÉMAL *s'il est m-dominant et que de plus* $n(P, m) = 0$.

On voit qu'un polynôme P de degré s est m-extrémal s'il est m-dominant et que son polynôme réciproque $P^* = X^s P(1/X)$ est $(-m)$-dominant. Remarquons aussi que si P est m-dominant, il est aussi m'-dominant pour $m' \leqslant m$. Enfin P est m-dominant (resp. m-extrémal) si et seulement si ses zéros dans une clôture algébrique de K sont dans la boule $v(x) \geqslant m$ (resp. sur la circonférence $v(x) = m$).

LEMME 4.4.2 (DIVISION EUCLIDIENNE). — *Soient* P *un polynôme m-dominant de degré s et f une série entière, $f \in B_m$. Il existe un unique couple (g, R) où g est une série entière, $g \in B_m$ et* R *un polynôme de degré $dg\, R < s$, tels que :*

(i) $f = Pg + R$, *de plus,* R *et g satisfont :*

(ii) $v(R, m) \geqslant v(f, m)$ *et* $v(g, m) \geqslant v(f, m) - v(P, m)$.

Supposons d'abord qu'il existe deux couples (g, R) et (g', R') tels que $f = Pg + R = Pg' + R'$, alors :

$$P(g' - g) = R - R',$$

et si $R \neq R'$:

$$N(R - R', m) = N(P, m) + N(g' - g, m)$$
$$= s + N(g' - g, m).$$

Or $N(g' - g, m) \geqslant 0$ et $N(R' - R, m) \leqslant dg\,(R' - R)$, on aurait donc $dg\,(R' - R) \geqslant s$, ce qui est impossible, d'où l'unicité.

On sait que le sous-anneau B_m^0 des séries entières appartenant à B_m est le complété de l'anneau des polynômes K[X] pour la valuation $Q \to v(Q, m)$. Supposons le lemme démontré lorsque f est un polynôme. Alors les relations (ii) montrent que le reste $R(f)$ et le quotient $g(f)$ dépendent continûment de f, et que les applications $f \to R(f)$ et $f \to g(f)$ sont des applications linéaires continues de K[X] (muni de $v(f, m)$) dans l'espace des polynômes de degré $\leqslant s$ et B_m^0 respectivement. Ces deux derniers espaces sont complets, donc les applications R et g se prolongent continûment à B_m^0, il est alors immédiat que leur prolongement satisfait (i) et (ii). Reste donc à prouver le lemme lorsque f est un polynôme.

Si f est un polynôme, on sait qu'il existe un unique couple (g, R) de polynômes tels que :

$$dg\, R < s \quad \text{et} \quad f = Pg + R.$$

Supposons d'abord que $m = 0$, alors quitte à le multiplier par une constante on peut supposer P unitaire et à coefficients dans A : dans ce cas les relations (ii) résultent du lemme 2.5.5. Supposons maintenant que $m \in v(K^*)$ et soit $a \in K$ tel que $v(a) = m$, soient $P_a = P(aX)$, $f_a = f(aX)$, alors P_a est 0-dominant, $v(P_a, 0) = v(P, m)$, $v(f_a, 0) = v(f, m)$ et si g_a, R_a sont le quotient et le reste dans la division de f_a par P_a, $g = g_a(X/a)$ et $R = R_a(X/a)$ satisfont visiblement (i) et (ii). Enfin, si $m \notin v(K^*)$, m est limite d'une suite croissante de valeurs $m' \in v(K^*)$. Pour tout $m' < m$, P est m'-dominant et $B_m^0 \subseteq B_{m'}^0$, donc le quotient $g(f)$ obtenu par division dans B_m^0 est encore celui obtenu dans $B_{m'}^0$, on a, pour tout $m' < m$, $m' \in v(K^*)$, $v(R, m') \geqslant v(f, m')$ et $v(g, m') \geqslant v(f, m') - v(P, m')$, et les relations (ii) se déduisent de la continuité des fonctions $m \to v(f, m)$.

COROLLAIRE 4.4.3. — *Soient $m \in \mathbf{R}$, $f \in B_m$ et* P *un polynôme m-extrémal de degré s, il existe un unique couple* (g, R) *où g est une série de Laurent telle que $g \in B_m$ et* R *un polynôme de degré s tel que :*

(i) $f = Pg + R$, *de plus :*

(ii) $v(R, m) \geqslant v(f, m)$, $v(g, m) \geqslant v(f, m) - v(P, m)$ *et* $Conv\,(g) \supseteq Conv\,(f)$.

Montrons d'abord l'unicité : si (g, R) et (g', R') satisfont $f = gP + R = g'P + R'$, où R et R' sont des poly-

nômes de degré $< s$ et g et g' des éléments de B_m, et si $R \neq R'$, on a :

$$N(R' - R, m) = N(P, m) + N(g - g', m) = s + N(g - g', m)$$

et : $\quad n(R' - R, m) = n(P, m) + n(g' - g', m)$,

or $n(P, m) = 0$ et $N(g - g', m) \geqslant n(g - g', m)$, d'où $N(R' - R, m) - n(R' - R, m) \geqslant s$, ce qui est impossible. L'existence et les conditions (ii) se déduisent du lemme 4.4.2.

Soit $f = f^+ + f^- = \sum_{n \geqslant 0} a_n X^n + \sum_{n<0} a_n X^n$ la décomposition canonique de f. Si $m' \leqslant m$ et $m' \in \mathrm{Conv}(f)$, alors $m' \in \mathrm{Conv}(f^+)$ et P est m'-dominant : si $f^+ = Pg^+ + R^+$ où R^+ est un polynôme de degré $\leqslant s$, $m' \in \mathrm{Conv}(g^+)$, donc $\mathrm{Conv}(g^+) \supseteq [m', +\infty]$. Soit $f_1 = X^{s-1} f^-(1/X)$, alors f_1 est une série entière, et, pour tout $m'' \geqslant m$, $m'' \in \mathrm{Conv}(f)$, $-m'' \in \mathrm{Conv}(f_1)$ et le polynôme :

$$P^* = X^s P(1/X)$$

est $-m''$-dominant. Alors $f_1 = P^* g_1 + R_1$ où $\mathrm{dg}\, R_1 < s$ et $-m'' \in \mathrm{Conv}(g_1)$. Soit $g_1 = X^{s-1} g_1(1/X) = g_1^+ + g_1^-$, alors $\mathrm{Conv}(g_1^-) \supseteq [-\infty, m'']$, et g_1^+ est un polynôme de degré $\leqslant s - 1$. En posant :

$$g = g^+ + g_1^- \quad \text{et} \quad R = R^+ + R_1^* + g_1^+,$$

on vérifie que $f = gP + R$, R est un polynôme de degré $< s$, et $\mathrm{Conv}(g) \supseteq [m', m'']$. On en déduit que $\mathrm{Conv}(g) \supseteq \mathrm{Conv}(f)$, et on vérifie facilement les inégalités (ii).

THÉORÈME 4.4.4 *(Lemme de Hensel).* — *Soient f une série de Laurent, m un réel tel que $m \in \mathrm{Conv}(f)$. Supposons que m soit une pente exceptionnelle pour f et soit $s = N(f, m) - n(f, m)$, alors il existe un unique couple (P, g) constitué d'un polynôme m-extrémal P de degré s, tel que $P(0) = 1$ et d'une série de Laurent $g \in B_m$ satisfaisant $f = Pg$. De plus :*

$\mathrm{Conv}(g) \supseteq \mathrm{Conv}(f)$ et $n(g, m) = N(g, m)$.

La démonstration est analogue à celle du théorème 2.5.3 : on construit par récurrence sur n une triple suite (P_n, g_n, R_n) telle que $f = P_n g_n + R_n$, que $R_n \to 0$, et que P_n et g_n tendent respectivement vers P et g satisfaisant le théorème.

Quitte à multiplier f par un scalaire, on peut supposer que $v(f, m) = 0$. De même, en multipliant f par une puissance convenable de X, on se ramène au cas où $n(f, m) = 0$. Soit donc $f = \sum_{n \in \mathbb{Z}} a_n X^n$ telle que :

$$0 = v(a_0) = v(a_s) + sm = v(f, m)$$

et : $\quad v(a_n) + nm > v(a_0)$ si $n > s$ ou $n < 0$.

Posons $P_1(X) = a_0 + a_1 X + \ldots + a_s X^s$. Alors P_1 est m-extrémal et :

$$v(f - P_1, m) > 0$$

(car $v(a_n) + nm \to +\infty$). On pose $h = v(f - P_1, m)$. Soient g_1 et R_1 le quotient et le reste de la division euclidienne de f par P_1, on a :

$$f = P_1 g_1 + R_1, \quad f - P_1 = (g_1 - 1) P_1 + R_1,$$
$$\mathrm{dg}\, R_1 < s, \quad \mathrm{Conv}(g_1) \supseteq \mathrm{Conv}(f)$$
$$v(g_1, m) \geqslant v(f, m) - v(P, m) = 0,$$
$$v(g_1 - 1, m) \geqslant v(f - P_1, m) - v(P_1, m) = h,$$

et : $\quad v(R_1, m) \geqslant h.$

Supposons que nous ayons construit $P_1, \ldots, P_n$; $g_1, \ldots, g_n$; $R_1, \ldots, R_n$ de telle sorte que, pour $1 \leqslant i \leqslant n$:

a) P_i est un polynôme m-extrémal de degré s, et :

$$v(P_i, m) = 0;$$

b) $g_i \in B_m$, et $\mathrm{Conv}(g_i) \supseteq \mathrm{Conv}(f)$, R_i est un polynôme de degré s, et $f = P_i g_i + R_i$;

c) $v(R_i, m) \geqslant ih$; $v(P_i - P_{i-1}, m) \geqslant (i-1)h$ et :

$$v(g_i - g_{i-1}, m) \geqslant ih.$$

Remarquons que ces conditions sont satisfaites pour $n = 1$. Posons $P_{n+1} = P_n + R_n$ et soient g_{n+1} et R_{n+1} le quotient et le reste de la division de f par P_{n+1}, alors pour $i = n + 1$ *a)* est satisfaite, car :

$$\mathrm{dg}\, R_n < s \quad \text{et} \quad v(R_n, m) > v(P'_n, m) = 0;$$

$g_{n+1} \in B_m$ et $\mathrm{Conv}(g_{n+1}) \supseteq \mathrm{Conv}(f)$, grâce à 4.4.3 et *b)* est satisfaite, de même $v(P_{n+1} - P_n, m) \geqslant nh$. De plus $P_n g_n + R_n = (P_n + R_n) g_{n+1} + R_{n+1}$, donc :

$$-R_n g_{n+1} = P_n(g_{n+1} - g_n) + R_{n+1} - R_n.$$

Cette dernière relation montre que $g_{n+1} - g_n$ et $R_{n+1} - R_n$ sont le quotient et le reste dans la division euclidienne de $-R_n g_{n+1}$ par P_n, on en déduit :

$$v(g_{n+1} - g_n, m) \geqslant v(R_n, m) + v(g_{n+1}, m) > v(g_{n+1}, m),$$

donc : $\quad v(g_{n+1}, m) = v(g_1, m) = 0$

et : $\quad v(g_{n+1} - g_n, m) \geqslant nh, \quad v(R_{n+1} - R_n) \geqslant nh.$

Mais alors $v(g_{n+1} - 1, m) \geqslant v(g_1 - 1, m) \geqslant h$ et de la relation de division euclidienne :

$$R_n(1 - g_{n+1}) = P_n(g_{n+1} - g_n) + R_{n+1}$$

on déduit :

$$v(g_{n+1} - g_n, m) \geqslant (n + 1)\, h \quad \text{et} \quad v(R_{n+1}, m) \geqslant (n + 1)\, h.$$

Les relations *a)*, *b)*, *c)* et *d)* sont satisfaites pour $i = n + 1$. Les suites P_n, g_n, R_n ainsi construites sont des suites de Cauchy dans B_m, soient P, g et R respectivement leurs limites, alors $f = Pg + R$, mais $R = 0$, et P est m-extrémal de degré s (tous les P_n le sont, et l'ensemble des polynômes Q m-extrémaux de degré s tels que $v(Q, m) = 0$ est fermé dans B_m). Donc g est le quotient dans la division euclidienne de f par P, $\mathrm{Conv}(g) \supseteq \mathrm{Conv}(f)$ et $v(g, m) = 0$.

Il nous reste à prouver l'unicité d'un couple (P, g) satisfaisant les conditions de l'énoncé. Il est clair que, si

$f = Pg$ où P est m-extrémal de degré $N(f, m) - n(f, m)$, alors $N(g, m) = n(g, m)$.

LEMME 4.4.5. — *Un élément f de B_m tel que :*

$$N(f, m) = n(f, m)$$

y est inversible.

En effet, quitte à multiplier f par un monôme convenable (les monômes non nuls sont visiblement inversibles) on peut supposer que $n(f, m) = N(f, m) = 0$ et $a_0 = 1$. Alors $v(f - 1, m) > 0$, or B_m est une algèbre de Banach, donc f y est inversible (cf. 3.5.5).

LEMME 4.4.6. — *Un polynôme m-extrémal non constant n'est pas inversible dans B_m.*

On sait en effet que B_m est isomorphe à l'anneau des fonctions analytiques strictes sur la boule :

$$B'_K = \{x \in K \mid v(x) \geqslant m\}$$

de K. Quel que soit L $\supseteq$ K, $A(B'_K)$ s'injecte dans $A(B'_L)$, et si L est une extension de K où le polynôme m-extrémal P a un zéro a, P ne peut être inversible dans $A(B'_L)$ car son inverse g devrait satisfaire $g(a)\, P(a) = g(a).0 = 1$. *A fortiori* P n'est pas inversible dans $A(B'_K)$ ni dans B_m.

LEMME 4.4.7. — *Les éléments inversibles de B_m sont les f telles que $n(f, m) = N(f, m)$.*

Nous savons déjà que ces éléments sont inversibles, soit $f \in B_m$, si $n(f, m) \neq N(f, m)$, il existe un polynôme m-extrémal non constant qui divise f dans B_m, et f n'est pas inversible.

LEMME 4.4.8. — *Soit* $I = (\mathbf{R} \cup \{+\infty\})$, *les éléments inversibles de $L_K(I)$ sont les constantes non nulles.*

Comme $I \ni +\infty$, les éléments de $L_K(I)$ sont des séries entières. Si $f = \sum_{n \geqslant 0} a_n X^n \in L_K(I)$ et y est inver-

sible, $a_0 \neq 0$, car f est formellement inversible, donc $N(f, +\infty) = 0$. Pour $m \in \mathbf{R}$ et assez grand :

$$n(f, m) = N(f, m) = 0.$$

Mais pour tout $m \in \mathbf{R}$, f est inversible dans B_m, donc les fonctions $n(f, m)$ et $N(f, m)$ coïncident sur $\mathbf{R}$, elles sont continues à droite et à gauche, donc continues, et à valeurs entières, donc constantes, et, pour tout $m \in \mathbf{R}$:

$$n(f, m) = N(f, m) = 0.$$

Soit $n \in \mathbf{Z}$, $n \neq 0$, et supposons que $a_n \neq 0$, alors pour m assez grand (resp. assez petit) $v(a_n) + nm < v(a_0)$, donc $a_n = 0$ pour $n \neq 0$, f est constante.

FIN DE LA PREUVE DU THÉORÈME. — Si $f = Pg = P'g'$ où P et P' sont m-extrémaux de degré s, g et g' sont inversibles dans B_m, donc $P = hP'$ et $P' = h'P$ où $hh' = 1$, h et $h' \in B_m$. Mais alors h (resp. h') est le quotient dans la division euclidienne de P par P' (resp. de P' par P), et $\mathrm{Conv}(h) \geq \mathrm{Conv}(P)$, $\mathrm{Conv}(h') \geq \mathrm{Conv}(P')$. Donc h et $h' \in L_K(\mathbf{R} \cup \{+\infty\})$ et y sont inversibles, puisque leur produit dans B_m, donc leur produit formel, est 1. Donc h et h' sont des constantes. Si on impose de plus $P(0) = P'(0) = 1$, on a donc $P = P'$ et $g = g'$.

COROLLAIRE 4.4.9. — *Soient* I *un intervalle fermé de* $\mathbf{R} \cup +\infty$ *et* $L = L_K(I)$, *soit* $f \in L$:

(i) *f est inversible dans* L *à la condition nécessaire et suffisante que* $n(f, m_1) = N(f, m_2)$ *où* $I = [m_1, m_2]$;

(ii) *si* $f \neq 0$, *il existe un unique polynôme de degré :*

$$N(f, m_2) - n(f, m_1),$$

soit P, *tel que* $P(0) = 1$, *que* P *divise f dans* L, *et* $f = Pf'$ *où f' est inversible dans* L.

D'abord, si f est inversible dans L, il l'est dans tout B_m, $m \in I$, donc pour tout $m \in I$:

$$n(f, m) = N(f, m) = N(f, m_1) = n(f, m_2).$$

Réciproquement, si $N(f, m_1) = n(f, m_2)$, pour tout $m \in I$, $N(f, m_1) \geq N(f, m) \geq n(f, m) \geq n(f, m_2)$, donc toutes ces valeurs coïncident. On peut, comme en 4.4.5, supposer que cette valeur commune est 0 et que $a_0 = 1$. Alors la série de terme général $(1 - f)^n$ dont la somme est une série de Laurent appartenant à tous les B_m, $m \in I$, définit un élément de L, qui est inverse de f.

Si $s = N(f, m_1) - n(f, m_2) \neq 0$, soient $p_1 \geq m_1$ la plus petite pente exceptionnelle de f, s_1 la longueur $N(f, p_1) - n(f, p_1)$ du côté correspondant du polygone de Newton, et P_1 l'unique polynôme P_1-extrémal de degré s_1 tel que $P_1(0) = 1$ et qui divise f. Alors $f = P_1 f_1$ et $N(f_1, m_1) - n(f_1, m_2) = s - s_1 < s$; par induction sur s on peut donc supposer que $f_1 = P_2 f'$ où $\deg P_2 = s - s_1$, $P_2(0) = 1$ et f' est inversible dans L. Soit $P = P_1 P_2$, alors P et f' satisfont les conditions annoncées. Supposons que $f = Qg'$, g' inversible dans L et :

$$\deg Q = N(f, m_1) - n(f, m_2) = \deg P, \qquad Q(0) = 1.$$

Alors P_1 divise Q dans L, soit $Q = P_1 g_1$, et $g_1 g' = f_1$: on peut, par induction sur s, supposer que la décomposition $f_1 = P_2 f'$ de f_1 est unique, d'où on déduit $P = Q$ et $f' = g'$.

COROLLAIRE 4.4.10. — *Soit* I *un intervalle fermé de* $\mathbf{R} \cup \{+\infty\}$, $I \neq \{+\infty\}$, *alors l'anneau* $L_K(I)$ *est principal, ses idéaux sont engendrés par des polynômes.*

Soient $B = L_K(I)$, M un idéal de B et $N = M \cap K[X]$, N est un idéal de K[X], il est principal, et il existe $Q \in K[X]$ tel que $N = QK[X]$. Alors d'une part $Q \in M$, donc $M \supseteq QB$, d'autre part, si $f \in M$, soit $f = Pf'$ la décomposition de f décrite en 4.4.9, alors $P = (f')^{-1} f \in M$, donc $P \in N$ et il existe un polynôme P_1 tel que $P = P_1 Q$, $f = Q(P_1 f')$ et $f \in QB$, donc $M = QB$.

En particulier, sous les hypothèses de 4.4.10, les idéaux de $L_K(I)$ sont fermés et de codimension finie. Si

K est algébriquement clos, les idéaux maximaux sont de codimension 1. On voit que si I est un intervalle fermé de $\mathbf{R} \cup \{+\infty\}$ et si K est algébriquement clos le spectre maximal de $L_K(I)$ s'identifie à la couronne $\{x \in K \mid v(x) \in I\}$, et les éléments de $L_K(I)$ sont des fonctions à valeurs dans K définies sur cette couronne.

Si I est un intervalle non fermé (*i.e.* ouvert ou semi-ouvert) de $\mathbf{R} \cup \{+\infty\}$, la structure des idéaux de $L_K(I)$ est plus compliquée, et nous ne l'étudierons pas ici : on trouvera un exposé complet des résultats généraux dans [19].

4.5. FONCTIONS ANALYTIQUES SUR UNE COURONNE

Soient I un intervalle de $\mathbf{R} \cup \{+\infty\}$ et $a \in K$, pour tout corps valué $L \supseteq K$, on note $C_L(a, I)$ l'ensemble des $x \in L$ tels que $v(x-a) \in I$. La COURONNE de centre a définie par I est la collection des $C_L(a, I)$ où L parcourt l'ensemble des extensions de K. Si $C = C(a, I)$ est une couronne, $C_L = C_L(a, I)$ est appelé ensemble des points de C dans L. Par exemple, si $I = [m, +\infty]$, $C(a, I)$ est un disque fermé de centre a (cf. 4.1). On dit que la couronne C est FERMÉE si I est un intervalle fermé. Si $I \neq \mathbf{R}$, C_L est une partie ouverte et fermée de L.

DÉFINITION 4.5.1. — *Soient* $C = C(a, I)$ *une couronne et f une fonction définie sur* C_K *et à valeurs dans* K. *On dit que f est strictement analytique sur* C *s'il existe* $f_a \in L_K(I)$, $f_a(X) = \sum_{n \in \mathbf{Z}} a_n X^n$ *telle que :*

$$\text{pour } x \in C_K, \quad f(x) = \sum_{n \in \mathbf{Z}} a_n (x-a)^n \qquad (1)$$

On démontre aisément les propriétés suivantes :

(i) L'ensemble des fonctions strictement analytiques sur C et à valeurs dans K est un K-espace vectoriel, qu'on notera $A_K(C)$ ou $A(C)$.

(ii) Si C est un disque fermé, cette définition coïncide avec celle de 4.1.1.

(iii) Si $f \in A(C)$, f est continue et dérivable sur C_K et, pour $x \in C_K$, sa dérivée est :

$$f'(x) = \sum_{n \in \mathbf{Z}} n a_n (x-a)^{n-1};$$

de même, pour $k \geqslant 1$, f a une dérivée k-ième $f^{(k)}$, $f^{(k)} \in A(C)$ et, pour $x \in C_K$:

$$f^{(k)}(x) = \sum_{n \in \mathbf{Z}} \binom{n}{k} a_n (x-a)^{n-k}.$$

(iv) Pour $x \in C_K$, $v(f(x)) \geqslant v(f_a, v(x-a))$ et, si $v(x-a)$ n'est pas une pente exceptionnelle pour f_a, $v(f(x)) = v(f_a, v(x-a))$.

Soit r' un réel, tel que $-\operatorname{Log} r' \in I \cap v(K^*)$, on pose :

$$|f|_{a, r'} = \sup_{|x-a| = r'} |f(x)|$$

et
$$|f|_{C_K} = \sup_{x \in C_K} |f(x)| = \sup (|f|_{a, r'})$$

pour :
$$-\operatorname{Log} r' \in I \cap v(K^*)$$

(on a supposé ici que dans $K^* v(x) = -\operatorname{Log}|x|$). On voit que $|f|_{a, r'} = e^{-v(f_a, -\operatorname{Log} r')}$, on vérifie que $f \to |f|_{a, r'}$ est une semi-norme sur $A(C)$. Si C est une couronne fermée $|f|_{C_K}$ est fini, car $v(f_a, m)$ a une borne inférieure finie sur I, on munit $A(C)$ de la norme $|f|_{C_K}$. Si C n'est pas fermée, on munit $A(C)$ de la topologie définie par la famille des semi-normes $|f|_{a, r'}$.

D'autre part, si I est fermé, $v(g, I) = \inf_{m \in I} v(g, m)$ est finie pour toute $g \in L_K(I)$ et définit sur $L_K(I)$ une norme $|g|_1 = e^{-v(g, I)}$, pour laquelle $L_K(I)$ est une algèbre de Banach. Si I n'est pas fermé, on munit $L_K(I)$ de la topologie définie par la famille des normes $|f|_m = e^{-v(f, m)}$ lorsque $m \in I$. On vérifie que, si $J \subseteq I$, l'injection canonique de $L_K(I)$ dans $L_K(J)$ est continue.

PROPOSITION 4.5.2. — *Soit* $C = C(a, I)$ *une couronne telle que* $I \cap v(K^*) \neq \varnothing, \{+\infty\}$.

(i) *L'application* S_a *de* $L_K(I)$ *dans* $A(C)$ *qui à* $f_a \in L_K(I)$ *associe la fonction* $f = S_a(f_a)$ *définie par* (1) *est une application linéaire continue.*

(ii) *Si le corps résiduel* $\tilde{k}$ *de* K *est infini,* S_a *est injective.*

(iii) *Si de plus la valuation* $v(K^*)$ *est dense,* S_a *est bicontinue, en particulier si* I *est fermé,* S_a *est une isométrie.*

(iv) $A(C)$ *est une sous-algèbre de* K^{C_K}, *et si* $\tilde{k}$ *est infini,* S_a *est un isomorphisme d'algèbres.*

PREUVE. — L'assertion (i) résulte de ce que, pour $-\operatorname{Log} r \in I \cap v(K^*)$, et $f_a \in L_K(I)$, on a, d'après la remarque (iv) ci-dessus :

$$|S_a(f_a)|_{a,r} \leqslant |f_a|_{-\operatorname{Log} r}.$$

Si $\tilde{k}$ est infini, la restriction de S_a à l'espace des pseudo-polynômes est injective, car, si $Q(X) = \sum_{N \leqslant n \leqslant N'} a_n X^n$ est un pseudo-polynôme non nul tel que $a_N \neq 0$:

$$S_a(Q)(x) = a_N (x-a)^N S_a(Q_1)(x)$$

où : $\quad Q_1(X) = 1 + b_1 + \ldots + b_{N'-N} X^{N'-N}.$

Soient r tel que $-\operatorname{Log} r \in I$ et $b \in K^*$ tel que $|b| = r$, alors $Q_1(bX)$ est à coefficients dans l'anneau de valuation de K, et non nul. Il existe $t \in K$, $|t| = 1$ tel que $|Q_1(bt)| = 1$, alors, pour $x = a + bt$, :

$$S_a(Q_1)(x) = Q_1(bt) \neq 0.$$

Or S_a est continue, donc son noyau est fermé, son intersection avec le sous-espace des pseudo-polynômes, qui est dense dans $L_K(I)$, est $\{0\}$, donc S_a est injective. Nous avons d'ailleurs montré de plus que, si Q est un pseudo-polynôme et si $-\operatorname{Log} r \in I \cap v(K^*)$:

$$|S_a(Q)|_{a,r} = |Q|_{-\operatorname{Log} r}$$

par densité, ceci est encore vrai pour toute $f \in L_K(I)$. Nous avons ainsi prouvé (ii) et (iii) en résulte car si $v(K^*)$ est dense, $v(K^*) \cap I$ est dense dans I et, pour tout intervalle fermé $J \subset I$, $|S_a(f_a)|_{C(a,J)} = |f_a|_J$. Donc, si I est fermé, S_a est une isométrie, sinon S_a est une isométrie pour chaque semi-norme de la famille définissant la topologie de $L_K(I)$ et la semi-norme correspondante sur $A(C)$: elle est encore bicontinue.

Enfin, pour prouver (iv), il suffit de remarquer que la structure d'algèbre définie sur $A(C)$ comme image par S_a de celle de $L_K(I)$ est, pour les pseudo-polynômes, celle induite sur $A(C)$ par K^{C_K}, et on conclut par densité.

COROLLAIRE 4.5.3. — *Soient* C *et* K *satisfaisant les hypothèses de* 4.5.2; *si* $\tilde{k}$ *est infini, pour toute* $f \in A(C)$ *il existe une unique* $f_a \in L_K(I)$ *satisfaisant* (1), *on l'appelle* SÉRIE DE LAURENT *de* f *relative au point* a.

Reformulation immédiate de l'assertion (ii) ci-dessus.

COROLLAIRE 4.5.4. — *Soit* $f \in A(C)$, $f \neq 0$, *et soit* $b \in C_K$, *il existe un unique entier* $q \geqslant 0$ *tel que :*

$$f(x) = (x-b)^q g(x) \quad \text{où} \quad g \in A(C) \quad \text{et} \quad g(b) \neq 0.$$

On appelle q LA MULTIPLICITÉ *du zéro* b *pour* f.

Montrons d'abord l'unicité : si :

$$f(x) = (x-b)^q g(x) = (x-b)^{q'} g(x) \quad \text{et si} \quad q \geqslant q',$$

alors $g'(x) = (x-b)^{q'-q} g(x)$ pour $x \neq b$, mais aussi pour $x = b$, par continuité. Si $q > q'$ $g'(b) = 0$, d'où l'unicité. Soit $m = v(b-a)$, il existe un unique couple P_m, h_m où P_m est m-extrémal de degré $N(f_a, m) - n(f_a, m)$, $P_m(0) = 1$ et $h_m \in L_K(I)$ (si m n'est pas une pente exceptionnelle, $P_m = 1$), satisfaisant $f_a = P_m h_m$. Alors $S_a(h_m)(b) \neq 0$, car m n'est pas pente exceptionnelle pour h_m, et il existe $q \geqslant 0$ tel que :

$$P_m(X) = (1 - X/b - a)^q Q(X), \quad \text{avec} \quad Q(b-a) \neq 0,$$

et cet entier q convient.

COROLLAIRE 4.5.5. — *Soient* $C = C(a, I)$ *une couronne fermée où* $I = [m_1, m_2] \neq \{+\infty\}$, *et* $f \in A(C)$, $f \neq 0$.

(i) *L'ensemble* $Z(f)$ *des zéros de* f *dans* C_K, *c'est-à-dire des* $b \in C_K$ *tels que* $f(b) = 0$, *est fini. Si* $b \in Z(f)$, *soit* $q(b)$ *sa multiplicité :*

$$\sum_{b \in Z(f)} q(b) \leqslant N(f, m_1) - n(f, m_2).$$

(ii) *Si de plus* K *est algébriquement clos :*

$$\sum_{b \in Z(f)} q(b) = N(f, m_1) - n(f, m_2).$$

Soit en effet $f_a = Pf'$ où $\operatorname{dg} P = N(f, m_1) - n(f, m_2)$ et f' est inversible dans $L_K(I)$. Alors $Z(f) = a + Z(P)$ et, pour $b \in Z(f)$, $q(b)$ est la multiplicité de la racine $b - a$ de P, d'où le (i), (ii) résulte de ce que, comme :

$$\operatorname{dg}(P) = N(P, m_1) - n(P, m_2),$$

toute racine c de P satisfait nécessairement $v(c) \in I$, car sinon $(X - c)$ est inversible dans $L_K(I)$ et on aurait $N(P, m_1) - n(P, m_2) < \operatorname{dg} P$.

COROLLAIRE 4.5.6. — *L'application* S_a *définie en* 4.5.2 *est injective, que* $\mathfrak{k}$ *soit ou non fini.*

En effet, comme K est de caractéristique 0, K est infini et, pour tout $m \in v(K^*)$, $\{x \in K \mid v(x - a) = m\}$ est infini, donc s'il existe $m \in \mathbf{R} \cap I \cap v(K^*)$ et si $f \in A(C)$, soit f_a telle que $f = S_a(f)$. Soient $\widetilde{K}$ la clôture algébrique de K et $\widetilde{f} = S_a(f_a) \in A_{\widetilde{K}}(C)$, on sait par 4.5.5 que f n'a qu'un nombre fini de zéros dans $\widetilde{K}$ tels que $v(x - a) = m$, si $f_a \neq 0$, car $\mathfrak{k}$ est infini. Donc si $f_a \neq 0$, $\widetilde{f}$ ne peut être nulle sur la couronne $C_K(a, \{m\})$ qui est une partie infinie de K, et sur cette couronne, $f(x) = \widetilde{f}(x)$.

De même 4.5.3 reste vrai, que $\mathfrak{k}$ soit fini ou non.

THÉORÈME 4.5.7. — *Soit* C *une couronne fermée telle que* $C_K \neq \{a\}$, *si* K *est algébriquement clos, l'espace* $H(C_K)$ *des éléments analytiques sur* C_K *coïncide avec* $A(C)$.

Rappelons que $H(C_K)$ et $A(C)$ sont des sous-espaces de K^{C_K}, d'où le sens coïncide, de plus ils sont l'un et l'autre munis d'une topologie, et c'est la même.

Par définition $H(C_K)$ est le complété, pour la topologie de la convergence uniforme sur C_K, de l'espace $R(C_K)$ des fractions rationnelles sans pôles dans C_K. Il suffit donc, comme en 4.1.6, de montrer que $R(C_K)$ est contenu dans $A(C)$, puisque la norme de $A(C)$ est, d'après sa définition, la norme de la convergence uniforme sur C_K, et que les pseudo-polynômes définissent par S_a un sous-espace dense de $A(C)$, qui est contenu dans $R(C_K)$. Soient $b \in K$ et $n \in \mathbf{Z}$. Si $v(b - a) < m_1$, où $C = C(a, I)$, $I = [m_1, m_2]$, on sait que $(x - b)^n$ est analytique stricte sur $C_1 = C(a, I_1)$, $I_1 = [m_1, +\infty)$. On montre de même que la formule du binôme :

$$(X + a - b)^{-p} = \sum_{n \geqslant 0} \binom{-p}{n} X^{-(n+p)}(a - b)^n = g(X)$$

fournit, pour $v(b - a) > m_2$, une série de Laurent g telle que $\operatorname{Conv}(g) \supseteq [-\infty, m_2]$, et donc telle que :

$$S_a(g) \in A(C).$$

Si $R \in R(C_K)$, sa décomposition en éléments simples est aussi une représentation de R comme combinaison linéaire d'éléments de $A(C)$, d'où le théorème.

COROLLAIRE 4.5.8. — *Soit* $C = C(a, I)$ *une couronne telle que* $C_K \neq \{a\}$, *soient* $b \in C_K$ *et* $m \in \mathbf{R}$ *tels que le disque fermé* $D' = C(b, [m, +\infty])$ *soit contenu dans* C (i.e. $D'_L \subseteq C_L$, $\forall L \supseteq K$), *alors, pour toute* $f \in A(C)$, *la restriction* $f_{D'}$, *de* f *à* D'_K *est dans* $A(D')$, *et* $f \to f_{D'}$ *est continue, si* $m \neq +\infty$, *c'est une injection.*

Supposons d'abord K algébriquement clos : alors le corollaire résulte de 4.1.10 et 4.5.7. Sinon $A_K(C)$ est plongé dans $A_{\widetilde{K}}(C)$, si $D'' = D'_{\widetilde{K}}$, la restriction de f à D'' est dans $A_{\widetilde{K}}(D')$ et à valeurs dans K, pour $x \in D'_K$, et le corollaire en résulte.

4.6. EXEMPLES

4.6.1. *Exponentielle et logarithme*

L'étude faite en 3.5.5 montre que les séries :

$$E(X) = \sum_{n \geqslant 0} X^n/n! \quad \text{et} \quad L(X) = \sum_{n \geqslant 1} (-1)^{n-1} X^n/n$$

définissent des fonctions strictement analytiques sur $C(0,]1/p - 1, +\infty])$ et $C(0,]0, +\infty])$ respectivement, si p est la caractéristique du corps résiduel $\tilde{k}$. On vérifie que l'exponentielle n'a aucun zéro. On sait que les pentes exceptionnelles pour L sont $a_h = 1/p^{h-1}(p-1)$ et que $n(L, a_h) = p^{h-1}$, $N(L, a_h) = p^h$. Notons :

$$\mathrm{Log}\,(1 + x) = S_0(L)\,(x)$$

la somme de la série L au point x. On sait aussi que, s'il existe $m \in \mathbf{N}$ tel que $(1+x)^m = 1$, $\mathrm{Log}\,(1+x) = 0$. En particulier si $(1+x)^{p^h} = 1$, alors $v(x) \geqslant a_h$, donc les p^h racines distinctes de l'équation $(1+x)^{p^h} = 1$ sont des zéros de $\mathrm{Log}\,(1+x)$; comme d'autre part $\mathrm{Log}\,y$ a au plus $N(L, a_h) - n(L, +\infty) = p^h$ zéros dans le disque $v(y-1) \geqslant a_h$, on a une détermination complète des zéros du logarithme. Posons :

$$P_h(X) = ((1+X)^{p^h} - 1)/p((1+X)^{p^{h-1}} - 1),$$

alors $P_h(0) = 1$ et les racines de $P_h(Y-1)$ sont les racines primitives p^h-ièmes de 1, donc les zéros de P_h sont les zéros de $\mathrm{Log}\,(1+x)$ situés sur le cercle $v(x) = a_h$. On en déduit, par récurrence sur h, qu'il existe :

$$g_h \in L_K(]0, +\infty])$$

telle que :

$$L(X) = XP_1 \ldots P_h g_h \quad \text{et} \quad N(g_h, a_h) = n(g_h, a_h) = 0;$$

on vérifie aussi que $g_h(0) = 1$.

LEMME 4.6.1. — *Le produit :*

$$XP_1 \ldots P_h = ((1+X)^{p^h} - 1)/p^h$$

converge vers $L(X)$ *dans* $L_K(]0, +\infty)$, *autrement dit, pour tout* $x \in K$ *tel que* $v(x) > 0$ *:*

$$\mathit{Log}\,(1+x) = \mathit{lim}\,((1+x)^{p^h} - 1)/p^h),$$

et cette convergence est uniforme dans tout disque $v(x) \geqslant m > 0$.

Il suffit de montrer que, pour tout $m > 0$:

$$v(g_h - 1, m) \to +\infty \quad \text{quand} \quad h \to \infty,$$

ou, ce qui revient au même, que $v(P_h - 1, m) \to +\infty$. Posons $Y_h = (1+X)^{p^h} - 1$, alors $P_h(X) = P_1(Y_{h-1})$, et $v(P_h - 1, m) \geqslant \mathrm{Inf}\,(v(Y_{h-1}, m), (p-1)\,v(Y_{h-1}, m) - 1)$, car $P_1(X) = 1 + \sum_{2 \leqslant i \leqslant p-1} \binom{p-1}{i-1} X^{i-1}/i$. Il suffit donc de montrer que $v(Y_h, m) \to +\infty$. Or $L(X) = p^{-h} Y_h g_h$, et $v(g_h, m) = 0$ pour $m \geqslant a_h$, pour un tel m :

$$v(Y_h, m) = h + v(L, m),$$

d'où le lemme.

4.6.2. *Fonctions entières*

Par définition, une fonction f définie sur K est une FONCTION ENTIÈRE si elle est strictement analytique sur tout disque de K. L'ensemble E des fonctions entières est un sous-anneau de K^K, on le munit de la topologie définie par la famille des semi-normes $|f|_{D'}$, où D' parcourt la famille des disques bornés. On voit aisément que, si $a \in K$, l'application T_a de E dans $K[[X]]$ qui à f associe sa série de Taylor $f_a = T_a(f)$ au point a est un isomorphisme d'algèbres de E sur $L_K(\mathbf{R} \cup \{+\infty\})$, et que, si K est algébriquement clos, T_a est bicontinue. Rappelons que nous avons montré que les seuls éléments inversibles de $L_K(\mathbf{R} \cup \{+\infty\})$, donc aussi de E, sont les constantes. Soit $f \in E$, les pentes exceptionnelles de sa série de Taylor f_0 au point 0 peuvent être indexées en une suite décrois-

sante $+\infty \geqslant m_1, m_2 \ldots m_k$, où $m_k \to -\infty$ (cf. 4.2.7). Pour $m_k \neq +\infty$, notons P_k l'unique polynôme m_k-extrémal de degré $N(f_0, m_k) - n(f_0, m_k) = s_k$ qui satisfait $P_k(0) = 1$ et tel que P_k divise f_0 dans $L_K(m_k)$. Si :

$$m_1 = +\infty,$$

on pose $P_1 = X^{N(f_0, +\infty)}$, et soit $a = a_{N(f_0, +\infty)}$; nous allons montrer que le produit $aP_1 \ldots P_k$ converge vers f dans E. En effet, il existe $g_k \in E$ telle que $f = aP_1 \ldots P_k g_k$, et $N(g_k, m_k) = n(g_k, +\infty) = 0$, $g_k(0) = 1$. Soit :

$$g_{k0}(X) = 1 + \sum_{n \geqslant 1} b_{nk} X^n$$

la série de Taylor de g au point 0, on a donc :

$$v(b_{nk}) + nm_k > 0 \quad \text{pour} \quad n \geqslant 1,$$

donc $v(g_k - 1, m) = \inf_{n \geqslant 1} (v(b_{nk}) + nm) \geqslant m - m_k$. Ceci montre que, pour tout $m \in \mathbf{R}$, $v(g_k - 1, m) \to \infty$ quand $k \to \infty$, et donc que le produit $aP_1 \ldots P_k$ converge vers f dans E.

On voit que la famille $Z(f)$ des zéros de f dans K est un ensemble dont l'intersection avec toute boule de K est finie, et $Z(f)$ est fini si et seulement si f est un polynôme. Réciproquement, si Z est une partie de K dont l'intersection avec toute boule est finie, soit $q(z)$ une famille d'entiers positifs indexés dans Z (multiplicités), on peut ranger les valuations $v(z)$ des éléments de Z en une suite décroissante $m_1, \ldots, m_k, \ldots$ tendant vers $-\infty$, et si $P_k(X) = \Pi(1 - X/z)^{q(z)}$, où le produit est étendu aux $z \in Z$ tels que $v(z) = m_k$, on montre aisément que le produit $P_1 \ldots P_k \ldots$ est convergent (cf. 3.5.1, exercice) et définit une fonction entière f dont les zéros sont les points $z \in Z$, avec les multiplicités $q(z)$. Donc la donnée d'une famille Z, avec multiplicités, détermine une fonction entière ayant cette famille de zéros, unique à une constante multiplicative près.

PROPOSITION 4.6.2. — *Toute fonction entière f non nulle est limite dans* E *d'un unique produit convergent :*

$$f = aX^N P_1 \ldots P_k \ldots, \quad \text{où} \quad a \in K,$$

P_k est un polynôme m_k-extrémal tel que $P_k(0) = 1$ et $m_k \to -\infty$, et où l'on convient que $P_k = 1$ à partir d'un certain rang si f est un polynôme.

Ce résultat, analogue au théorème de Weierstrass pour les fonctions entières sur **C**, en diffère cependant à plusieurs titres; d'une part, il n'y a que des polynômes dans le produit convergent, d'autre part, il y a unicité à une constante près de la fonction entière associée à une famille donnée de zéros. On déduit aisément de cette étude que l'ensemble des idéaux maximaux de E s'identifie à l'ensemble des polynômes irréductibles et unitaires de K[X], en particulier si K est algébriquement clos, il s'identifie à K.

EXERCICES. — 1. Soient D un ouvert de K et $a \in D$, soit f une fonction définie sur $D^* = D - \{a\}$, on dit que f a au point a un pôle d'ordre p si la fonction $(x-a)^p f$ coïncide sur D^* avec un élément analytique g sur D tel que $g(a) \neq 0$.

a) Si $f \in H(D^*)$, et si f a un pôle d'ordre p en a, $p = 0$ (montrer que f est bornée au voisinage de a).

b) Soit C une couronne fermée, on suppose K algébriquement clos. On dit qu'une fonction f est méromorphe sur C s'il existe une famille finie $a_1, \ldots, a_n$ de points de C_K tels que f soit définie sur $C^* = C_K - \{a_1, \ldots, a_n\}$ et ait en chaque a_i un pôle d'ordre p_i. Montrer que tout élément du corps des fractions de A(C) définit une fonction méromorphe sur C, et que l'ensemble des fonctions méromorphes sur C s'identifie à ce corps.

c) On dit qu'une fonction f est méromorphe sur K si sa restriction à toute boule fermée de K est méromorphe sur cette boule. L'ensemble des fonctions méromorphes sur K est le corps des fractions de E (K algébriquement clos).

2. On se propose de construire une fonction entière sur $\mathbf{Q}_p$, bornée.

a) Soit $P(X) = 1 - X^{p-1}$; déterminer :

$$\inf\{v(P(x)) \mid x \in \mathbf{Q}_p \text{ et } v(x) = k\}, \quad k \in \mathbf{Z}.$$

b) Déterminer une suite d'entiers $h(k)$ tels que si :

$$P_k(X) = P(X)\,(P(pX))^{h(1)} \ldots P(p^k X)^{h(k)}$$

on ait :

$$\sup\{|P_k(x)| \mid x \in \mathbf{Q}_p,\ v(x) \geqslant -k\} = 1.$$

c) En déduire un exemple de fonction entière f bornée sur $\mathbf{Q}_p$. Montrer que l'on peut aussi choisir les entiers $h(k)$ de sorte que $\lim |f(x)| = 0$ quand $|x| \to \infty$ et $x \in \mathbf{Q}_p$.

4.7. PROLONGEMENT ANALYTIQUE

Dans tout ce paragraphe on suppose K algébriquement clos.

Nous avons défini en 4.1 l'espace H(D) des éléments analytiques sur une partie infinie bornée de K; pour donner une définition raisonnable pour les parties non bornées, il est commode de se placer sur la *droite projective* de K. Rappelons que la droite projective $\mathbf{P}_1(K)$ est l'ensemble des droites de K^2, c'est-à-dire le quotient de $K^2 - \{0\}$ par la relation $(x, y) \simeq (x', y') \Leftrightarrow xy' = x'y$, muni de la topologie quotient. Si $x \neq 0$, on identifie la classe de (x, y) dans $\mathbf{P}_1(K)$ au point $t = y/x$ de K, et on note ∞ la classe de $(0, 1)$. Ceci permet d'identifier $\mathbf{P}_1(K)$ avec $K' = K \cup \{\infty\}$, où les voisinages de ∞ dans K' sont les complémentaires dans K' des parties bornées de K. De plus, si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K)$ est une matrice inversible, elle définit par passage au quotient un homéomorphisme φ de K', où $\varphi(z) = az + b/cz + d$ si $z \in K$, si $c \neq 0$, $\varphi(\infty) = a/c$ et $\varphi(-d/c) = \infty$, et, si $c = 0$, $\varphi(\infty) = \infty$. Les homéomorphismes de K' ainsi associés aux automorphismes de K^2 s'appellent les transformations homographiques.

Soient D une partie infinie bornée de K et φ une transformation homographique telle que $\varphi(D)$ soit borné. Si f est une fonction définie sur D on vérifie que :

$$f \in H(D) \Leftrightarrow f \circ \varphi^{-1} \in H(\varphi(D)) \qquad (1)$$

Soient D une partie infinie de K' et φ une transformation homographique telle que $\varphi(D)$ soit une partie bornée de K (une telle φ existe si $\overline{D} \neq K'$), alors, par définition, les fonctions f définies sur D qui y sont des éléments analytiques sont celles qui satisfont :

$$f \circ \varphi^{-1} \in H(\varphi(D)).$$

On vérifie que grâce à (1) cette définition de H(D) ne dépend que de D et pas du choix de φ. On convient que si $\overline{D} = K'$, H(D) est réduit aux constantes.

Par exemple, soient :

$$a \in K, \quad r > 0, \quad \text{et} \quad D = \{x \in K' \mid |x - a| \geqslant r\},$$

alors H(D) est l'espace des fonctions f définies sur D telles que $f(1/y + a)$ soit élément analytique sur le disque $|y| \leqslant 1/r$. On voit ainsi que toute $f \in H(D)$ admet un unique développement $f(x) = \sum_{n \geqslant 0} a_n (x-a)^{-n}$, convergeant uniformément sur D, et que $||f||_D = \operatorname{Max} |a_n| r^{-n}$.

Lorsque D est un voisinage du point à l'infini de K', on note $H_0(D)$ le sous-espace de H(D) constitué des f telles que $\lim_{|x| \to \infty} f(x) = 0$: le sous-espace $R_0(D)$, intersection de R(D) et $H_0(D)$, est alors l'espace des fractions rationnelles sans pôle dans D et dont le degré du dénominateur est strictement supérieur à celui du numérateur.

Dans l'exemple ci-dessus, où $D = \{x \mid |x - a| \geqslant r\}$, le sous-espace $H_0(D)$ est simplement caractérisé par $a_0 = 0$.

On voit, par ces définitions, qu'on peut toujours ramener l'étude d'un espace H(D) au cas où le domaine D est borné.

Soit D une partie bornée de K, on note $\boldsymbol{D}$, et on appelle ENVELOPPE de D, l'intersection des disques fermés contenant D : c'est un disque fermé.

Si D est fermé, soit $D'' = \boldsymbol{D} - D$: D'' est un ouvert, D'' est réunion des disques ouverts qu'il contient. Un disque ouvert T contenu dans D'' est appelé un TROU de D s'il est maximal (pour l'inclusion) parmi les disques ouverts contenus dans D''. On note $\mathscr{T}(D)$ la famille des trous de D, alors $\boldsymbol{D} = D \cup \bigcup_{T \in \mathscr{T}(D)} T$.

Notons B′ le complémentaire dans K′ d'une partie B de K′, alors si D est un fermé borné de K, on a :

$$D = \boldsymbol{D} \cap \Big(\bigcap_{T \in \mathcal{E}'(D)} T'\Big).$$

Cette décomposition « ensembliste » du fermé D permet une représentation commode de l'espace H(D), lorsque D appartient à une classe de parties que nous allons définir.

DÉFINITION 4.7.1 (INFRACONNEXES). — *Soit* D *une partie bornée de* K, $a \in K$, *on note* $v_a(x) = v(x-a)$. *On dit que* D *est* INFRACONNEXE *si, pour tout* $a \in K$, *l'image* $v_a(D)$ *de* D *par* v_a *a pour adhérence un intervalle de* $\mathbf{R}''$.

On vérifie qu'un disque ou une couronne sont des infraconnexes (si la valuation de K est dense : nous avons ici supposé K algébriquement clos, on remarquera que si la valuation de K n'est pas dense, il y a fort peu d'infraconnexes !). De même, si D est un disque, et si $T_1, \ldots, T_n$ sont des disques disjoints strictement contenus dans D, alors $D \cap T_1' \cap T_2' \cap \ldots \cap T_n'$, est un infraconnexe.

EXERCICE. — Soient D un disque, $(T_n)_{n \geqslant 1}$ une famille de disques deux à deux disjoints strictement contenus dans D. Donner des conditions suffisantes sur la famille T_n pour que :

$$D \cap T_1' \cap T_2' \cap \ldots \cap T_n' \cap \ldots$$

soit infraconnexe, et d'autres pour qu'il ne le soit pas.

La propriété essentielle des infraconnexes est la suivante : soient $a \in K$, $I = \overline{v_a(D)}$, et $f \in H(D)$, on peut définir sur I une fonction $v_a(f, m)$ tout à fait analogue à la fonction $v(f, m)$ qui a été un outil essentiel dans l'étude des fonctions analytiques sur une couronne. Plus précisément :

DÉFINITION 4.7.2. — *Soient* $R = P/Q$ *une fraction rationnelle,* $b \in K$, $P_b(X) = P(b+X)$ *et* $Q_b(X) = Q(b+X)$; *on pose* $v_b(R, m) = v(P_b, m) - v(Q_b, m)$. *La fonction ainsi définie ne dépend pas du choix de la représentation* $R = P/Q$.

On sait que $v(P_b, m) = \mathrm{Inf}\{v(P(x)) \mid v(x-b) = m\}$, si $m \in v(K^*)$, et que, si P n'a aucun zéro z satisfaisant $v(z-b) = m$, on a, pour $v(x-b) = m$:

$$v(P(x)) = v(P_b, m).$$

On en déduit :

LEMME 4.7.3. — *Soient* $R \in K(X)$, $b \in K$, $x \in K$ *et* $m = v(x-b)$.

(i) *Si* R *n'a aucun pôle tel que* $v(z-b) = m$:

$$v(R(x)) \geqslant v_b(R, m)$$

et : $v_b(R, m) = \mathit{Inf}\,(v(R(y)) \mid v(y-b) = m)$.

(ii) *Si* R *n'a aucun zéro tel que* $v(z-b) = m$:

$$v(R(x)) \leqslant v_b(R, m)$$

et : $v_b(R, m) = \mathit{Sup}\,(v(R(y)) \mid v(y-b) = m)$.

(iii) *Si* R *n'a ni zéro ni pôle tel que* $v(z-b) = m$, $v(R(x)) = v_b(R, m)$.

Il est d'autre part immédiat que $v_b(R, m)$ est continue sur $\mathbf{R}''$.

COROLLAIRE 4.7.4. — *Soient* D *un infraconnexe,* T *un trou de* D, R *une fraction rationnelle* $R \in H_0(T')$, *alors* $\|R\|_D = \|R\|_{T'}$.

Rappelons que $H_0(T')$ désigne l'espace des fractions rationnelles nulles à l'infini et dont tous les pôles sont dans T. Soit $b \in T$, $T = \{x \mid v(x-b) > m\}$. Alors ou bien $v_b(D) = \{m\}$, ou bien il existe une suite $x_n \in D$ telle que $v(x_n - b) = m_n < m$ et $m_n \to m$. Dans ce dernier cas, pour n assez grand, R n'a aucun zéro tel que $v(z-b) = m_n$ et on a $v(R(x_n)) = v_b(R, m_n)$, alors :

$$\lim v(R(x_n)) = v_b(R, m).$$

Soit $R(x) = \sum_{k \geqslant 1} a_k/(x-b)^k$ la série représentant R dans $H_0(T')$, alors $v_b(R, m') = \mathrm{Inf}\{v(a_k) - km'\}$, donc

$v_b(R, m) = \mathrm{Inf}\,(m' < m \mid v_b(R, m'))$. Nous avons donc montré que, si :

$$v_b(D) \neq \{m\},\ \mathrm{Sup}\{|R(x)| \mid x \in D\} = \mathrm{Sup}\{|R(x)| \mid x \in T'\},$$

comme $D \subseteq T'$, le corollaire est prouvé dans ce cas.

Supposons maintenant que $v_b(D) = \{m\}$, et soit $a \in D$ tel que $v(a - b) = m$. Alors $v_a(D)$ est dense dans $[m, +\infty]$, en effet, $v_a(D) \ni +\infty$, et si $I = \overline{v_a(D)} \not\ni [m, +\infty]$, T est contenu dans D. Soit $R = P/Q$ où les zéros de Q sont dans T, il existe une suite $x_n \in D$ telle que :

$$v(x_n - a) = m_n > m \quad \text{et} \quad v(x_n - a) \to m.$$

Pour un tel x_n, $v(Q(x_n)) = v_a(Q, m_n)) = v_b(Q, m)$, pour n assez grand $v(P(x_n)) = v_a(P, m_n)$, alors :

$$\lim v(R(x_n)) = v_a(R, m) = v_b(R, m),$$

et la démonstration s'achève comme dans le cas précédent.

PROPOSITION 4.7.5. — *Soit* D *un infraconnexe non réduit à un point,* $R \in R(D)$, *on note, pour* $a \in K$:

$$w_a(R) = \mathit{Inf}\{v_a(R, m) \mid m \in v_a(D)\},$$

et : $$w_D(R) = \mathit{Inf}\{w_a(R) \mid a \in D\},$$

alors : $$w_D(R) = \mathit{Inf}\{v(R(x)) \mid x \in D\}.$$

Remarquons d'abord que, D n'étant pas réduit à un point, il existe $m \in \mathbf{R}$ tel que, pour tout $a \in D$:

$$\overline{v_a(D)} = [m, +\infty] = I.$$

En effet, si $\boldsymbol{D} = \{x \mid v(x - b) \geqslant m\}$, alors, pour tout $a \in D$, $\boldsymbol{D} = \{x \mid v(x - a) \geqslant m\}$: on en déduit que :

$$m \in \overline{v_a(D)};$$

comme de plus $+\infty \in v_a(D)$ et $v_a(D) \subseteq [m, +\infty]$, il est clair que $\overline{v_a(D)} = [m, +\infty]$.

Notons provisoirement $v_D(R) = \mathrm{Inf}\{v(R(x)) \mid x \in D\}$. Pour $a \in D$, soit J_a l'ensemble des $m' \in I$ tels que R n'ait ni zéro ni pôle satisfaisant $v(z - a) = m'$: J_a ne diffère de I que par un ensemble fini, et :

$$w_a(R) = \mathrm{Inf}\{v_a(R, m') \mid m' \in J_a\}.$$

Or, pour $x \in D$ et $v(x - a) \in J_a$, on a :

$$v(R(x)) = v_a(R, v(x - a)),$$

et l'ensemble $v_a(D) \cap J_a$ est dense dans J_a, d'où :

$$w_a(R) \geqslant v_D(R).$$

D'autre part, soient $\varepsilon > 0$ et $a \in D$ tel que :

$$v(R(a)) \leqslant v_D(R)\,(1 + \varepsilon),$$

pour un tel a :

$$w_a(R) \leqslant v_a(R, +\infty) = v(R(a)) \leqslant v_D(R)\,(1 + \varepsilon),$$

d'où la proposition.

Remarquons que toutes les fonctions $v_a(R, m)$, $w_a(R)$ et $w_D(R)$ sont à valeurs dans $\mathbf{R}''$: $\mathbf{R}''$ est homéomorphe, par une application exponentielle à base inférieure à 1, à $[0, +\infty]$. Nous munirons $\mathbf{R} \cup \{+\infty\}$ de la structure uniforme déduite de celle de $[0, +\infty[$ par cet homéomorphisme; avec cette convention, nous pouvons maintenant préciser la fonction $v_a(f, m)$ d'un élément analytique f : elle est à valeurs dans $\mathbf{R} \cup \{+\infty\}$.

COROLLAIRE 4.7.6. — *Soit* $f \in H(D)$, *pour toute suite* $R_n \in R(D)$ *qui converge vers f uniformément sur* D, *et pour tout* $a \in D$, *la suite de fonctions* $v_a(R_n, m)$ *converge uniformément sur* $I = \overline{v_a(D)}$ *vers une fonction continue* $v_a(f, m)$, *à valeurs dans* $\mathbf{R} \cup \{+\infty\}$, *indépendante de la suite* R_n *choisie. Cette fonction a, en particulier, les propriétés suivantes :*

(i) *Soient :*

$$w_a(f) = \mathit{Inf}\{v_a(f, m) \mid m \in I\}$$

et : $$w_D(f) = \mathit{Inf}\{w_a(f) \mid a \in D\},$$

alors : $$w_D(f) = \mathit{Inf}\{v(f(x)) \mid x \in D\}.$$

(ii) *Si* J *est un intervalle contenu dans* I *où la restriction de* $v_a(f, m)$ *ne prend que des valeurs finies, la fonction* $v_a(f, m)$ *est affine par intervalles sur* J.

La preuve est à peu près immédiate si on remarque que, compte tenu de 4.7.5, une suite R_n converge uniformément sur D à la condition nécessaire et suffisante que $w_D(R_{n+1} - R_n)$ tende vers l'infini. Le (ii) résulte de ce que, si $v_a(f, m)$ est fini, pour n assez grand (uniformément sur tout intervalle fermé où $v_a(f, m)$ est majoré) :

$$v_a(f, m) = v_a(R_n, m).$$

THÉORÈME 4.7.7 (THÉORÈME DE MITTAG-LŒFFLER). — *Soient* D *un infraconnexe fermé borné,* $\boldsymbol{D}$ *son enveloppe,* $\mathscr{C}(D)$ *la famille de ses trous. Pour toute* $f \in H(D)$, *soit* $T \in \mathscr{C}(D)$, *alors :*

(i) *il existe une unique* $f_T \in H_0(T')$ *telle que :*

$$f - f_T \in H(D \cup T),$$

de plus $||f_T||_{T'} \leqslant ||f||_D$;

(ii) *la famille* f_T *ainsi associée à* f *est sommable dans* H(D), *et il existe une unique* $f_0 \in A(\boldsymbol{D})$ *telle que* $f = f_0 + \Sigma f_T$, *de plus :*

$$||f||_D = \mathrm{Max}\,(||f_0||_{\boldsymbol{D}}, \mathrm{Max}\,||f_T||_{T'}).$$

En d'autres termes, soit $E = A(\boldsymbol{D}) \oplus (\hat{\oplus} H_0(T'))$ muni de sa norme canonique (cf. 3.2.3). Soit φ l'application naturelle de E dans H(D) : à un élément de E est associée la fonction définie sur D par $f(x) = f_0(x) + \Sigma f_T(x)$, on vérifie que cette série est uniformément convergente sur D et que $f \in H(D)$. Le théorème de Mittag-Lœffler est alors équivalent à : φ est bijective et isométrique, *i.e.* φ est un isomorphisme d'espaces de Banach.

Pour démontrer ce théorème, remarquons tout d'abord que, si $R \in R(D)$, R admet une décomposition canonique $R = P + \Sigma R_i$, où, (a_i) désignant la famille (finie) des pôles de R, R_i est la partie principale de R relative au

pôle a_i, *i.e.* l'unique fraction rationnelle $R_i = P_i/(x - a_i)^{q_i}$ telle que $\mathrm{dg}\,P_i < q_i$ et $R - R_i$ n'a pas de pôle en a_i, et où P est un polynôme (la partie entière de R). Si $T \in \mathscr{C}(D)$ nous noterons R_T la somme des R_i où a_i parcourt l'ensemble des pôles de R qui appartiennent à T, de même R_0 désignera la somme des R_i où a_i parcourt l'ensemble des pôles de R n'appartenant pas à $\boldsymbol{D}$. Avec ces notations, on a $R = P + R_0 + \Sigma R_T$, où les R_T sont presque tous nuls.

LEMME 4.7.8. — *Soient* D *un infraconnexe,* R_T *une famille de fractions rationnelles presque toutes nulles,* $R_T \in R_0(T')$, *et soit* $R = \Sigma R_T$, *alors :*

$$||R||_D = \mathrm{Max}\,||R_T||_{T'}.$$

PREUVE DU THÉORÈME 4.7.7. — Comme $\varphi(E)$ contient R(D) qui est dense dans H(D), il suffit de montrer que φ est une isométrie pour qu'il en résulte à la fois qu'elle est injective, bicontinue, que son image est fermée, et que donc φ est surjective. Donc il suffit de montrer que, si $(f_T) \in \hat{\oplus} H_0(T')$ et $f_0 \in A(\boldsymbol{D})$, $f = f_0 + \Sigma f_T$ satisfait :

$$||f||_D = \mathrm{Max}\,(||f_0||_{\boldsymbol{D}}, \mathrm{Max}\,(||f_T||_{T'})) \qquad (M)$$

Notons M le membre de droite de cette égalité, il est évident que $||f||_D \leqslant M$. De plus, si T est un trou de D tel que $||f_T||_{T'} < M$, soient $b \in T$ et i une inversion de centre b, alors $f \circ i^{-1} \in H(i(D))$, l'enveloppe $\boldsymbol{i(D)}$ de $i(D)$ est $i(T')$, $g = f \circ i^{-1}$ s'écrit comme somme de $g_0 = f_T \circ i^{-1} \in A(\boldsymbol{i(D)})$, de $g_1 = f_0 \circ i^{-1} \in H_0(\boldsymbol{i(D')})$ et des $f_S = f_S \circ i^{-1}$ relatifs aux trous $S \neq T$. Alors, si l'égalité (M) est vraie pour g et $i(D)$, elle l'est aussi pour f et D. On voit ainsi que pour montrer (M) il suffit de le montrer dans le cas où $||f_0||_{\boldsymbol{D}} < M$, ou, ce qui revient au même, compte tenu de l'inégalité ultramétrique, dans le cas où $f_0 = 0$. Or il existe une partie finie $\mathscr{C}_1$ de $\mathscr{C}(D)$ telle que, pour $T \notin \mathscr{C}_1$, $||f_T||_{T'} < M/2$. De même, pour

chaque $T \in \mathscr{E}_1$, soient $b \in T$, $f_T = \sum_{k \geqslant 1} a_k/(x-b)^k$, il existe N tel que $R_T = \sum_{1 \leqslant k \leqslant N} a_k/(x-b)^k$ satisfasse :

$$||f_T - R_T||_{T'} < M/2.$$

Alors, si $R = \sum_{T \in \mathscr{E}_1} R_T$, on a $||f - R||_D < M/2$. En appliquant à R le lemme 4.7.8, on a déduit :

$$||R||_D = M = ||f||_D.$$

Ceci prouve l'égalité (M), donc aussi le théorème.

PREUVE DU LEMME 4.7.8. — Soient :

$$M = \text{Max}\, ||R_T||_{T'}, \quad R' = \Sigma R_T$$

où T parcourt l'ensemble des T pour lesquels :

$$||R_T||_{T'} = M,$$

alors $||R - R'||_D < M$, et pour prouver le lemme on peut supposer que, pour $R_T \neq 0$, $||R_T||_{T'} = M$.

Soient $T_1, \ldots, T_n$ les trous de D pour lesquels $||R_T||_{T'} = M$, pour alléger l'écriture nous noterons $R_i = R_{T_i}$ et $||R_i||_i = ||R_{T_i}||_{T_i}$. On a donc :

$$R = R_1 + \ldots + R_n,$$

avec $||R_i||_i = M$ pour tout i. Choisissons $b_i \in T_i$, $T_i = \{x \mid v(x - b_i) > m_i\}$. On dira que les trous T_i et T_j sont CONTIGUS si $\boldsymbol{T}_i = \boldsymbol{T}_j$: ainsi T_i et T_j sont contigus si et seulement si $m_i = m_j = v(b_i - b_j)$.

LEMME 4.7.9. — *Soient $T_1, \ldots, T_n$ des trous contigus de l'infraconnexe D, $R_i \in R_0(T_i')$ des fractions rationnelles telles que, pour tout i, $||R_i||_i = M$, et $R = R_1 + \ldots + R_n$, alors, quels que soient $\varepsilon > 0$ et $m' < m$ (où m est la valeur commune des m_i), il existe $x \in D$ satisfaisant $v(x - b_1) \geqslant m'$ et $|R(x)| \geqslant M(1 - \varepsilon)$. De plus si $D \not\subset \boldsymbol{T}_1$, on peut choisir x de telle sorte que $v(x - b_1) < m$.*

D'abord, si $n = 1$, c'est le corollaire 4.7.4 ou du moins une forme à peine améliorée qui a en fait été démontrée dans la démonstration de 4.7.4. Si $n \neq 1$, alors $m \in v(K^*)$, car $m = v(b_1 - b_2)$, par exemple. Quitte à faire un changement de variable de la forme $x \to ax + b$, on peut supposer que l'enveloppe commune $\boldsymbol{T}_1$ des T_i est A, anneau de valuation de K, et que $b_1 = 0$. Alors les images $\bar{b}_i$ des b_i dans le corps résiduel $\mathfrak{k}$ sont deux à deux distinctes (les T_i sont disjoints). On peut appliquer à R le corollaire 4.1.15, et on obtient :

$$\text{Max}\,(|R(x)| \mid x \in A \cap T_1' \cap \ldots \cap T_n'\} = M.$$

Si l'intersection de D avec A est non vide, soit $b \in D \cap A$, alors $\overline{v_b(D)} \supseteq [0, +\infty]$, donc il existe une suite $x_n \in D$ telle que $v(x_n - b) = m_n > 0$, $v(x_n) = 0$ et $m_n \to 0$. Si $R = P/Q$ où Q est un polynôme unitaire ayant ses zéros dans la réunion des T_i, alors $M(P, 1) = M$, car, pour $x \in A \cap T_1' \cap \ldots \cap T_n'$, $v(Q(x)) = 0$. Alors $|P(x_n)| \to M$ et $|R(x_n)| \to M$.

Si de plus l'intersection de D avec le complémentaire de A est non vide (*i.e.* si $D \not\subset \boldsymbol{T}_1$), il existe une suite $x_n \in D$ telle que $v(x_n) < 0$ et $v(x_n) \to 0$, et, pour n assez grand, $|Q(x_n)|$ est voisin de 1 et $|P(x_n)| \geqslant M$, d'où le lemme.

Pour achever la preuve du lemme 4.7.8, il reste donc à prouver qu'on peut se ramener au cas d'une fraction rationnelle dont les parties principales sont relatives à des trous contigus. Revenons donc au cas général où :

$$R = R_1 + \ldots + R_n,$$

avec $||R_i||_i = M$ pour tout i. Soit $m = \text{Inf}\,(m_i)$, supposons par exemple que $m = m_1$, et soient $T_1, T_2, \ldots, T_s$ les trous T_i contigus à T_1, T_j n'étant pas contigu à T_1 pour $j > s$. Alors, pour $j > s$, ou bien $m_j > m$, ou bien $v(b_j - b_1) < m$.

Si $m_j > m$, choisissons n_j de telle sorte que :

$$m < n_j < m_j,$$

alors :

$$\mathrm{Max}\{|\mathrm{R}_j(x)| \mid v(x-b_j) \leqslant n_j\} = \mathrm{M}_j < \mathrm{M},$$

donc, pour ε assez petit, $v(x-b_1) \geqslant m_1 - \varepsilon$ entraîne $|\mathrm{R}_j(x)| \leqslant \mathrm{M}_j$.

De même, si $v(b_j - b_1) < m$, pour :

$$v(x-b_1) = m' > v(b_j - b_1), \qquad v(x-b_j) = v(b_1 - b_j),$$

alors, soit :

$$\mathrm{M}_j = \mathrm{Max}\{|\mathrm{R}_j(x)| \mid v(x-b_j) \leqslant v(b_1-b_j) < m_j\},$$

on a $\mathrm{M}_j < \mathrm{M}$ et, pour $v(x-b_1)$ assez voisin de m, $|\mathrm{R}_j(x)| \leqslant \mathrm{M}_j$. Finalement, soit M' la borne supérieure des M_j, $\mathrm{M}' < \mathrm{M}$. En appliquant le lemme 4.7.9 on voit qu'il existe $x \in \mathrm{D}$ tel que :

$$|\mathrm{R}_1(x) + \ldots + \mathrm{R}_s(x)| \geqslant \mathrm{M}(1-\varepsilon),$$

pour ε assez petit $\mathrm{M}(1-\varepsilon) > \mathrm{M}'$, et on peut choisir x de telle sorte que $|\mathrm{R}_{s+1}(x) + \ldots + \mathrm{R}_n(x)| \leqslant \mathrm{M}'$, pour un tel x on aura donc $|\mathrm{R}(x)| \geqslant \mathrm{M}(1-\varepsilon)$, ce qui achève la démonstration.

Corollaire 4.7.10. — *Soient* $\mathrm{T}_1, \ldots, \mathrm{T}_n$ *des disques ouverts disjoints dont les rayons appartiennent à* K, *et soit* $\mathrm{C} = (\boldsymbol{T}_1 \cup \ldots \cup \boldsymbol{T}_n) \cap (\mathrm{T}'_1 \cap \ldots \cap \mathrm{T}'_n)$, *soient :*

$$f_i \in \mathrm{H}_0(\mathrm{T}'_i), \qquad ||f_i||_{\mathrm{T}'_i} = ||f_i||_i,$$

et P *un polynôme, notons* $f = \mathrm{P} + f_1 + \ldots + f_n$, *alors :*

$$||f||_0 = \mathit{Max}\,(||\mathrm{P}||_0, \mathit{Max}\,||f_i||_i).$$

Si les disques T_i sont tels que C soit infraconnexe, c'est une simple application du théorème de Mittag-Lœffler, mais si par exemple $n = 2$ et $\boldsymbol{T}_1 \cap \boldsymbol{T}_2 = \varnothing$, alors C est réunion des deux couronnes $\boldsymbol{T}_i \cap \mathrm{T}'_i$, dont la distance mutuelle est supérieure au rayon de chacune d'entre elles, et on voit aisément qu'un tel C n'est pas infraconnexe.

On se ramène au cas où, pour tout i :

$$||f_i||_i = \mathrm{M} \geqslant ||\mathrm{P}||_0,$$

par l'inégalité ultramétrique. On se ramène de même au cas où $f_i = \mathrm{R}_i$ est une fraction rationnelle. Soit :

$$m = \mathrm{Inf}\,(m_i), \quad \text{où} \quad \mathrm{T}_i = \{x \mid v(x-b_i) > m_i\};$$

supposons par exemple que $m = m_1$, et que $\boldsymbol{T}_i \subseteq \boldsymbol{T}_1$, pour $i \leqslant s$, et $\boldsymbol{T}_j \cap \boldsymbol{T}_1 = \varnothing$ pour $j > s$. Alors, nous avons montré dans la preuve du lemme 4.7.8 que :

$$\mathrm{Sup}\{|\mathrm{R}_{s+1}(x) + \ldots + \mathrm{R}_n(x)| \mid x \in \boldsymbol{T}_1 \cap \mathrm{C}\} = \mathrm{M}' < \mathrm{M}.$$

Or $\mathrm{D} = \boldsymbol{T}_1 \cap \mathrm{C}$ est un infraconnexe, dont les trous sont $\mathrm{T}_1, \ldots, \mathrm{T}_s$, donc :

$$\mathrm{Sup}\{|\mathrm{P}(x) + \mathrm{R}_1(x) + \ldots + \mathrm{R}_s(x)| \ x \in \mathrm{D}\} = \mathrm{M},$$

et le corollaire est démontré.

Les algèbres d'éléments analytiques sur un infraconnexe fermé borné ne sont pas nécessairement intègres. On peut trouver des infraconnexes D et des éléments analytiques f sur D qui sont « localement nuls » sans être partout nuls (*i.e.* dont la restriction à un ouvert de D est nulle sans que f soit nulle partout). On peut caractériser les infraconnexes D pour lesquels H(D) est une algèbre nœthérienne, ou principale (nous avons vu que H(D) est principale lorsque D est une couronne). On trouvera une étude systématique de ces algèbres dans [23].

Pour poursuivre une théorie du prolongement analytique, une méthode consiste à choisir une classe $\mathscr{P}$ de parties de $\mathbf{P}_1(\mathrm{K})$, stable par les homographies. Rappelons qu'on dit qu'une famille $(\mathrm{P}_i)_{i\in\mathrm{I}}$ de parties d'un ensemble E est *enchaînée* si, pour tout couple (i,j), il existe une suite finie $i = i(0), \ldots, j = i(n)$, d'éléments de I, tels que $\mathrm{P}_{i(k)} \cap \mathrm{P}_{i(k+1)} \neq \varnothing$, pour $k = 0, \ldots, n-1$. Etant donné une partie C de $\mathbf{P}_1(\mathrm{K})$ et une fonction f définie sur C, on dit que f est *une fonction $\mathscr{P}$-analytique* s'il existe un recouvrement de C par une famille enchaînée $(\mathrm{P}_i)_{i\in\mathrm{I}}$ de parties

appartenant à la famille $\mathscr{P}$, telles que, pour tout i, la restriction de f à P_i y soit un élément analytique. Par exemple, si $\mathscr{P}$ est la classe des disques fermés, on voit que les seules parties C de $P_1(K)$ qui soient réunion enchaînée de disques fermés sont les disques (fermés ou non), et on vérifie que, si C est un disque fermé, les fonctions $\mathscr{P}$-analytiques sur C sont les éléments analytiques sur C, tandis que si C est un disque non fermé les fonctions $\mathscr{P}$-analytiques sont les fonctions analytiques sur C au sens de 4.1. On voit ainsi que la classe des disques fermés ne donne lieu qu'à une théorie fort restreinte du prolongement analytique (contrairement au cas complexe, où une réunion de disques fermés enchaînés peut être n'importe quel connexe). On montre également que si $\mathscr{P}$ est la famille des couronnes de $P_1(K)$ les fonctions $\mathscr{P}$-analytiques sont les fonctions analytiques sur une couronne au sens de 4.1. On trouvera une étude systématique des classes $\mathscr{P}$ pour lesquelles l'espace des fonctions $\mathscr{P}$-analytiques jouit de propriétés « raisonnables » dans [27].

Une autre méthode de prolongement analytique consiste, au lieu de se donner *a priori* des parties de $P_1(K)$, et de construire des espaces ou des anneaux de fonctions définies dans ces parties, à se donner *a priori* des anneaux, que l'on représente comme anneaux de fonctions. Plus précisément, notons $K\{X_1, \ldots, X_n\}$ l'algèbre de Banach complétée de $K[X_1, \ldots, X_n]$ pour la norme « sup des coefficients » (si $n = 1$, $K\{X\}$ est simplement $L_K[0, +\infty]$). Une algèbre de Banach B sur K est dite topologiquement de type fini si elle est quotient d'une algèbre $K\{X_1, \ldots, X_n\}$ par un idéal fermé. On montre que le spectre maximal d'une telle B se plonge de façon naturelle dans $P_n(K)$, et B se trouve ainsi représenté comme algèbre de fonctions sur une partie de $P_n(K)$. Les spectres maximaux des algèbres B jouant le rôle de « variétés analytiques locales », une théorie du recollement de ces variétés donne lieu à la notion de variété analytique rigide. Nous allons étudier en 4.8 une classe particulière d'infraconnexes qui sont des spectres d'algèbres topologiquement de type fini. On trouvera un exposé de la théorie des espaces analytiques rigides par exemple en [28], et une étude des algèbres d'éléments analytiques sur des infraconnexes, qui sont aussi topologiquement de type fini, dans [24].

4.8. LEMNISCATES

Soit P un polynôme unitaire non constant de degré q, $M > 0$, alors la LEMNISCATE définie par P et M est l'ensemble :

$$B = B(P, M) = \{x \in K \mid |(P(x)| \leqslant M\}.$$

Il est clair que B est fermé et borné.

PROPOSITION 4.8.1. — *Soit* $B = B(P, M)$ *une lemniscate,* $q = dg\, P$, *il existe* $h \leqslant dg\, P$ *et des disques fermés disjoints* $B_1, \ldots, B_h$ *tels que* $B = B_1 \cup \ldots \cup B_h$. *De plus, si* K *est algébriquement clos,* P *a au moins un zéro dans chaque* B_i.

Soit $b \in B$, alors il existe un disque fermé contenant b et contenu dans B (P est continue). Soit C_b la réunion de ces disques : c'est un disque contenant b et contenu dans B. Soit $\boldsymbol{C_b}$ son enveloppe, alors :

$$\mathrm{Sup}\{|P(x)| \mid x \in \boldsymbol{C_b}\} = \mathrm{Sup}\{|P(x)| \mid x \in C_b\} \leqslant M,$$

donc : $$\boldsymbol{C_b} \subseteq C_b,$$

et C_b est un disque fermé. On voit ainsi que B est réunion des disques fermés maximaux qu'il contient. Supposons K algébriquement clos, et soit C un disque fermé contenu dans B. Si P n'a aucun zéro dans C, alors, pour tout $c \in C$, $|P(c)| = ||P||_C \leqslant M$. Il existe un disque fermé C′ contenant strictement C et où P n'a pas de zéros, pour un tel C′, $||P||_{C'} = ||P||_C \leqslant M$, donc $C' \subseteq B$. Donc, si C est maximal dans B, P a un zéro dans C : le nombre de tels C (deux à deux disjoints) est majoré par q. Si K n'est pas algébriquement clos, soient $\tilde{K}$ sa clôture algébrique

et $\widetilde{B} = \{x \in \widetilde{K} \mid |P(x)| \leqslant M\}$, alors $\widetilde{B} = \widetilde{B}_1 \cup \ldots \cup \widetilde{B}_h$, $h \leqslant q$, où les $\widetilde{B}_i$ sont des boules fermées disjointes, et, si $B_i = \widetilde{B}_i \cap K$, $B = B_1 \cup \ldots \cup B_h$, où les B_i sont soit des disques fermés, soit vides, d'où le lemme.

Exemple. — Soient :

$$K = \mathbf{Q}_p, \quad P_n(X) = X(X-1)\ldots(X-n+1),$$
$$M_n = |n!|_p,$$

alors $B(P_n, M_n) = \mathbf{Z}_p$. En effet, si :

$$Q_n(X) = P_n(X)/n! = \binom{X}{n},$$

on sait que, pour $x \in \mathbf{Z}_p$, $|Q_n(x)| \leqslant 1$, d'où $\mathbf{Z}_p \subseteq B$. D'autre part, si $x \notin \mathbf{Z}_p$, alors :

$$|P_n(x)| = |x|^n > 1 \geqslant M_n, \quad \text{donc} \quad B = \mathbf{Z}_p.$$

Exercice. — On prend $K = \mathbf{C}_p$, P_n et M_n comme ci-dessus. Soit h l'unique entier tel que :

$$p^h \leqslant n < p^{h+1}, \quad \text{et} \quad B_{i,h} = \{x \in \mathbf{C}_p \mid v(x-i) \geqslant h\}.$$

Montrer que :

$$B(P_n, M_n) = \bigcup_{0 \leqslant i < p^h} B_{i,h}.$$

Montrer que $\bigcap B(P_n, M_n) = \mathbf{Z}_p$.

Corollaire 4.8.2. — *Soient* K *algébriquement clos et* $M \in |K^*|$*; alors les rayons des disques maximaux de la lemniscate* B(P, M) *appartiennent à* K.

Soit en effet $b \in K$ tel que $|b| = M$, alors :

$$B(P, M) = \{x \in K \mid |P(x) - b| \leqslant M\}.$$

Donc chaque disque B_i contient un zéro c_i de l'équation $P(x) = b$. Or si le rayon de B_i n'appartient pas à K, comme P a un zéro dans B_i, on a, pour tout $x \in B_i$, $|P(x)| < ||P||_{B_i} \leqslant M$, d'où le corollaire.

Etant donné un polynôme P unitaire de degré $q \geqslant 1$ et une constante $M > 0$, nous noterons :

$$B'(P, M) = \{x \in P_1(K) \mid |P(x)| \geqslant M\}$$

et : $$C(P, M) = B(P, M) \cap B'(P, M).$$

Il est clair que $B(P, M) \neq \varnothing$ si et seulement si $M \in |K^*|$.

Lemme 4.8.3. — *Soient* P *un polynôme unitaire de degré* $q \geqslant 1$, $f \in H_0(B'(P, M))$ *et* Q *un polynôme, alors, si* $C = C(P, M)$ *n'est pas vide et si* K *est algébriquement clos :*

$$||f + Q||_C = Max\,(||Q||_C, ||f||_{B'}).$$

Soit T(P, M) l'ensemble des $x \in K$ tels que :

$$|P(x)| < M$$

T(P, M) est contenu dans B, et, si $B_1, \ldots, B_h$ sont les disques maximaux disjoints de B, l'intersection de T avec B_i est la réunion des disques ouverts contenus dans B_i, de même rayon que B_i, et contenant un zéro de P. Notons $T_1, \ldots, T_n$ ces disques ouverts, $n \leqslant q$. Soit :

$$T_i = \{x \mid v(x - b_i) > m_i\}$$

alors $|P(x)| = M$ si et seulement s'il existe i pour lequel $v(x - b_i) = m_i$, et pour tout j, $v(x - b_j) \geqslant m_j$. Donc $C(P, M) = C = (T_1 \cup \ldots \cup T_n) \cap (T_1' \cap \ldots \cap T_n')$.

Le lemme est donc un cas particulier du corollaire 4.7.10.

Corollaire 4.8.4. — *Soit :*

$$Q \in K[X], \quad Q = Q_0 + Q_1 + \ldots + Q_s P^s,$$

l'unique représentation de Q *où les* Q_i *soient des polynômes de degré* $< q$*, alors* $||Q||_C = Max\,(||Q_i||_C M^i)$.

Soient :

$$n = \deg Q, \quad s = [n/q],$$
$$Q = Q_s P^s + R_s, \quad \deg R_s < sq,$$

l'identité de division euclidienne de Q par P^s : on voit, par récurrence sur s, que Q admet une représentation de la forme annoncée, l'unicité est évidente. De plus :

$$Q/P^s = Q_s + R_s/P^s \quad \text{et} \quad R_s/P^s \in H_0(B'),$$

donc :

$$||Q/P^s||_0 = \text{Max}\,(||Q_s||_0, ||R_s/P^s||_{B'}) \geqslant ||Q_s||_0.$$

Or, pour $x \in C$, $|P(x)| = M$, d'où :

$$||Q||_0 \geqslant ||Q_s||_0 M^s.$$

Par récurrence sur s, on en déduit que, pour tout i, $||Q||_0 \geqslant ||Q_i||_0 M^i$, mais d'autre part :

$$||Q||_0 \leqslant \text{Max}\,(||Q_i||_0 M^i),$$

d'où le corollaire.

PROPOSITION 4.8.5. — *Soit* $f \in H_0(B')$, *il existe une unique suite de polynômes* Q_i, $dg\, Q_i < q$, *tels que :*

$$||Q_i||_0/M^i \to 0,$$

et que :

(i) $f = \sum_{i \geqslant 1} Q_i/P^i$, *où cette série converge uniformément sur* B' ;

on a de plus :

(ii) $||f||_{B'} = Max\,(||Q_i||_0/M^i)$.

Il est clair que cet énoncé n'a un sens que si $C \neq \varnothing$, *i.e.* si $M \in |K^*|$.

Montrons d'abord que toute représentation du type (i) satisfait (ii) : l'unicité en résulte.

Soient $\Gamma = B$ et $D = \Gamma \cap B'$; D est infraconnexe puisque c'est un disque privé d'un nombre fini de trous $T_1, \ldots, T_k$.

Pour $n \geqslant 1$ et $f \in H_0(B')$, $P^n f \in H(D)$ et admet une unique décomposition $P^n f = S_n + R_n$, où $S_n \in H(\Gamma)$ et $R_n \in H_0(B')$; de plus, $||P^n f||_D = \text{Max}\,||S_n||_\Gamma, ||R_n||_{B'}$. Or, si f admet une représentation (i), posons :

$$S_n = P^n \sum_{1 \leqslant i \leqslant n} Q_i/P^i, \qquad R_n = P^n f - S_n;$$

alors S_n est un polynôme et $R_n \in H_0(B')$, donc il s'agit de la représentation cherchée de $P^n f$. Or, comme S_n est un polynôme, en appliquant le lemme 4.8.3 on a $||S_n||_0 \leqslant ||P^n f||_0 = M^n ||f||_0$. En appliquant d'autre part le lemme 4.8.4 au polynôme S_n, on en déduit, pour $i \leqslant n$, $||Q_i||_0/M^i \leqslant ||f||_0$, d'où la relation (ii).

Remarquons de plus que, si $f \in H_0(B')$, dans l'unique décomposition $P^n f = S_n + R_n$ telle que $S_n \in H(\Gamma)$ et $R_n \in H_0(B')$, S_n est nécessairement un polynôme de degré $< nq$ car S_n/P^n tend vers zéro lorsque $|x| \to +\infty$, de plus $S_{n+1} - PS_n$ est un polynôme de degré $< q$, et il suffit de prouver que $||f - S_n/P^n||_0 = ||R_n||_0/M^n \to 0$ pour que la suite S_n/P^n fournisse la série cherchée.

Or $f = \Sigma f_j$ où $f_j \in H_0(T'_j)$, et il suffit de montrer que chaque f_j a une représentation (i). Soit b_j un zéro de P dans T_j, alors, pour $x \in T'_j$, $f_j(x) = \sum_{n \geqslant 1} a_{n,j}/(x - b_j)^n$. Notons $f_{n,j} = \sum_{1 \leqslant k \leqslant n} a_{k,j}/(x - b_j)^k$, alors :

$$||f_j - f_{n,j}||_0 \to 0,$$

et de plus $P^n f_{n,j} = U_{n,j}$ est un polynôme, donc, si :

$$P^n f_j = S_{n,j} + R_{n,j},$$

où $S_{n,j}$ est un polynôme et $R_{n,j} \in H_0(B')$, alors :

$$P^n(f_j - f_{n,j}) = S_{n,j} - U_{n,j} + R_{n,j}$$

et, d'après le lemme 4.8.3, $||R_{n,j}||_0 \leqslant M^n ||f_j - f_{n,j}||_0$. On en déduit que $S_{n,j}/P^n$ converge vers f_j uniformément sur C, donc f_j admet une représentation (i), et f aussi, ce qui achève la démonstration.

COROLLAIRE 4.8.6. — *Soit* $L = K\{X, Y\}$ *l'anneau complété de* K[X, Y] *pour la norme « sup des coefficients »*, P, M, B, B' *et* C *comme ci-dessus, on suppose de plus que* $B \subseteq A$ *(anneau de valuation de* K*)* i.e. *que* $P \in A[X]$ *et* $M \leqslant 1$. *Soient* $b \in A$ *tel que* $|b| = M$, *et* $Q(X, Y) = b - P(X)\,Y$. *Notons* I *l'idéal engendré par* Q *dans* L, $L' = L/I$ *et* φ *l'application canonique de* L *sur* L'. *Soit* ψ *l'application de* K[X, Y] *dans* $R(B' \cap A)$ *qui à* $F(X, Y) \in K[X, Y]$ *associe :*

$$\psi(F)(X) = F(X, b/P(X)),$$

alors :

(i) *Ker* $\psi = I \cap K[X, Y]$, $\|\psi\| = 1$, *on note encore* ψ *l'unique prolongement continu (à valeurs dans* $H(B' \cap A)$*) de* ψ *à* L;

(ii) *soit* L_1 *le sous-espace de* L, *fermeture dans* L *de l'espace des polynômes de la forme :*

$$G(X, Y) = G_0(X) + \sum_{1 \leqslant i \leqslant k} G_i(X)\, Y^i,$$

où $dg\, G_i < q$ *pour* $i \geqslant 1$, *alors* $L = L_1 \oplus I$ *et la restriction* ψ_1 *de* ψ *à* L_1 *est un isomorphisme d'espaces de Banach;*

(iii) *soit* $\omega = \varphi \circ \psi_1^{-1}$, ω *est un isomorphisme d'algèbres de Banach de* $H(B' \cap A)$ *sur* L'.

La démonstration de ce corollaire ne présente aucune difficulté compte tenu des résultats précédents. Nous n'utiliserons pas ce résultat et en laissons la démonstration au lecteur. Il signifie que l'algèbre $H(B' \cap A)$ est topologiquement de type fini, ainsi que nous l'avions annoncé en 4.7.

Nous terminerons ce paragraphe par une remarque qui nous sera utile au chapitre 5. Soit $f = Q + g$ où Q est un polynôme et $g \in H_0(B')$, nous noterons $a_1(f)$ le « résidu de f à l'infini », c'est-à-dire la limite, pour $x \to +\infty$, de $xg(x)$; alors, si $D(B)$ désigne le diamètre de B, on a $|a_1(f)| \leqslant \|f\|_0\, D(B)$.

Supposons en effet que $B \ni 0$ (ce qu'on peut faire, car $a_1(f)$ est visiblement invariant par translation), alors, d'après 4.8.3, $|a_1(f)| \leqslant \|fx\|_0 \leqslant D(B)\|f\|_0$.

COROLLAIRE 4.8.7. — *Soit* $f \in H_0(B')$, *il existe une constante* $M(f)$ *telle que, pour tout polynôme* Q :

$$|a_1(Qf)| \leqslant M(f)\, \|Q\|_0.$$

En effet,

$$\|fQ\|_0 \leqslant \|f\|_0\, \|Q\|_0, \quad \text{et} \quad M(f) = \|f\|_0 D(B)$$

a la propriété annoncée.

CHAPITRE 5

Théorèmes de rationalité

5.1. INTRODUCTION

Soient K un corps de nombres et $f \in K[[X]]$ une série formelle à coefficients dans K. A chaque extension valuée C de K correspond un domaine de convergence de f dans C : si C est le corps des nombres complexes, la somme de f définit une fonction analytique sur un certain disque de C (éventuellement réduit à $\{0\}$); de même, si C est une extension d'un complété $\mathfrak{P}$ - adique de K, f définit une fonction analytique stricte dans un certain disque de cette extension. De plus les fonctions ainsi définies par f dans des disques de différents corps C peuvent être prolongeables hors de ces disques, soit au sens habituel dans C, soit comme éléments analytiques au sens de 4.1, sur un certain domaine de C, lorsque C est une extension de $\mathbf{Q}_p$.

Un des moyens de reconnaître, parmi les séries formelles à coefficients dans K, celles qui sont des fractions rationnelles, consiste à étudier les fonctions analytiques associées à f dans des extensions valuées de K : si les domaines où ces fonctions sont analytiques sont « assez grands », f est rationnelle. Les théorèmes de rationalité ci-dessous sont de ce type. Un exemple classique d'un tel critère est la :

PROPOSITION 5.1.1. — *Soit* $f(X) = \sum_{n \geqslant 0} a_n X^n$ *une série formelle à coefficients entiers définissant dans* C *une fonction méro-*

morphe dans un disque de rayon strictement supérieur à 1, alors f est une fraction rationnelle.

Cette proposition apparaîtra comme un corollaire des deux théorèmes de rationalité que nous prouverons ci-dessous.

Nous donnons d'abord, au § 2, deux critères purement algébriques (Hankel et Kronecker), au § 3, le théorème de Borel-Dwork qui n'utilise que les notions de fonction méromorphe sur un disque, sans faire appel à la théorie du prolongement analytique, et au § 4 le théorème de Polya-F. Bertrandias, qui généralise le précédent et utilise à la fois quelques notions sur le prolongement analytique et une notion de « grandeur » d'un domaine, plus fine que la notion de diamètre, à savoir le diamètre transfini.

Le théorème de Borel-Dwork est un cas particulier du théorème de Polya-F. Bertrandias, et la démonstration du second, que nous donnerons, n'utilise pas le premier : la preuve du théorème de Borel-Dwork aurait donc pu être omise. Elle a cependant été donnée car, étant apparemment d'un accès plus facile que celle du second théorème, elle peut en faciliter la compréhension.

5.2. CRITÈRES ALGÉBRIQUES, DÉTERMINANTS

Soit $a = (a_n)_{n \geqslant 0}$ une suite d'éléments d'un corps K, on appelle DÉTERMINANT DE HANKEL de rang n et d'ordre k, de la suite a, et on note $D_n^k(a)$ le déterminant $[\alpha_{ij}]$, $0 \leqslant i \leqslant k$, $0 \leqslant j \leqslant k$, où $\alpha_{ij} = a_{n+i+j}$. Le déterminant $D_0^n(a)$, aussi noté $D^n(a)$, est appelé le n-ième *déterminant de Kronecker* de la suite a.

PROPOSITION 5.2.1. — *Pour que la série formelle :*

$$f(X) = \sum_{n \geqslant 0} a_n X^n$$

soit une fraction rationnelle il faut et il suffit qu'il existe k tel que, pour n assez grand, $D_n^k(a) = 0$.

Supposons d'abord que f soit une fraction rationnelle; soient $Q(X) = q_0 + q_1 X + \ldots + q_k X^k$ un dénominateur de f, et $P = Qf$, alors, pour $n > \deg P$:

$$q_0 a_n + q_1 a_{n-1} + \ldots + q_k a_{n-k} = 0.$$

Donc, pour $n + k > \deg P$, $D_n^k(a) = 0$.

Pour montrer la réciproque, nous utiliserons une relation élémentaire sur les déterminants : la relation de *Sylvester*.

Soit $D = [a_{ij}]$, $0 \leqslant i \leqslant m$, $0 \leqslant j \leqslant m$, un déterminant d'ordre $m + 1$: c'est un polynôme homogène de degré $m + 1$ par rapport à l'ensemble des variables a_{ij}, de degré 1 par rapport à chacune d'entre elles. Notons A_{ij} le coefficient de a_{ij} dans D, et d le déterminant $d = [a_{ij}]$, $1 \leqslant i \leqslant m-1$, $1 \leqslant j \leqslant m-1$ (d est le déterminant extrait de D en supprimant les lignes et colonnes extrêmes), alors la relation de Sylvester s'énonce :

$$D\,d = A_{00} A_{mm} - A_{0m} A_{m0}.$$

Pour la démontrer, on peut considérer le déterminant $D' = [b_{ij}]$, où $b_{0j} = A_{0j}$, $b_{mj} = A_{mj}$, et, pour $i \neq 0, m$, $b_{ij} = \delta_{ij}$ (*i.e.* 1 pour $i = j$ et 0 sinon). On vérifie aisément que :

$$D\,D' = D^2 d = D(A_{00} A_{mm} - A_{0m} A_{m0}).$$

Comme le polynôme D n'est pas nul, la relation de Sylvester en résulte. Appliquée aux déterminants de Hankel d'une suite a, elle devient :

$$D_n^k D_{n+2}^{k-2} = D_{n+2}^{k-1} D_n^{k-1} - (D_{n+1}^{k-1})^2, \quad \text{pour } k \geqslant 2 \quad (S)$$

Nous supposerons la suite a non stationnaire : si elle l'est, f est rationnelle.

LEMME 5.2.2. — *Soit a une suite non stationnaire, s'il existe k et* n_0 *tels que, pour* $n \geqslant n_0$, $D_n^k(a) = 0$, *il existe h et* n_1 *tels que* $D_n^h(a) = 0$ *pour* $n \geqslant n_1$ *et* $D_n^{h-1}(a) \neq 0$ *pour* $n \geqslant n_1 + 1$.

Nous dirons que k est admissible pour a si $D_n^k = 0$ pour n assez grand. Remarquons que $D_n^0 = a_n$, donc 0 n'est pas admissible (a non stationnaire). Par hypothèse, il existe k admissible : soit h le plus petit entier admissible et soit n_1 le plus petit indice tel que $D_n^h = 0$ pour $n \geqslant n_1$. Si $h = 1$, on conviendra que $D_n^{-1} = 1$; on vérifie que la relation (S) est encore vraie pour $k \geqslant 1$ (elle s'écrit alors $D_n^1 = a_n a_{n+2} - (a_{n+1})^2$). Soit m un indice tel que $D_m^{h-1} = 0$; si $m \geqslant n_1 + 1$, la relation de Sylvester appliquée à $n = m - 1$:

$$D_{m-1}^h D_{m+1}^{h-1} = D_{m+1}^{h-1} D_{m-1}^{h-1} - (D_{m+1}^{h-1})^2,$$

montre, par récurrence, que $D_{m'}^{h-1} = 0$ pour $m' \geqslant m$. S'il en est ainsi, $h - 1$ est admissible, ce qui est contraire à l'hypothèse. Donc, pour $m \geqslant n_1 + 1$, $D_m^{h-1} \neq 0$, et le lemme est démontré.

FIN DE LA PREUVE DE LA PROPOSITION. — Supposons a non stationnaire, et satisfaisant l'hypothèse du lemme, choisissons h et n_1 comme dans le lemme, soit (E_n) l'équation linéaire par rapport aux inconnues $Y_0, \ldots, Y_h$:

$$Y_0 a_n + Y_1 a_{n-1} + \ldots + Y_h a_{n-h} = 0 \qquad (E_n)$$

Le système d'équations (E_n), $N + h \leqslant n \leqslant N + 2h$, a pour déterminant D_N^h. Pour $N \geqslant n_1$, il admet donc une solution, mais il est de rang $h - 1$, car D_{N+1}^{h-1} est un de ses mineurs d'ordre h et est non nul. Donc ce système admet une solution unique telle que $Y_h = 1$: on voit ainsi que l'unique solution du système correspondant à $N = n_1$, et satisfaisant $Y_h = 1$, est encore solution des systèmes d'indice $N \geqslant n_1$. Si :

$$Q(X) = X^h + Y_{h-1} X^{h-1} + \ldots + Y_0,$$

fQ est un polynôme, et f est rationnelle.

Remarquons que nous avons aussi montré que, si h est le plus petit entier admissible, f admet un dénominateur de degré h, et n'en admet pas de degré moindre.

COROLLAIRE 5.2.3. — *Pour que la série formelle :*

$$f(X) = \sum_{n \geqslant 0} a_n X^n$$

soit une fraction rationnelle, il faut et il suffit que, pour n assez grand, $D^n(a) = 0$.

Notons $A_n^k(a) = (a_n, a_{n+1}, \ldots, a_{n+k}) \in K^{k+1}$, alors :

$$D^n(a) = \mathrm{Det}\,(A_0^n(a), A_1^n(a), \ldots, A_n^n(a)).$$

Si f est une fraction rationnelle, soit :

$$Q(X) = q_0 + q_1 X + \ldots + q_k X^k$$

un dénominateur de f; alors, pour n assez grand :

$$q_0 A_n^n(a) + q_1 A_{n-1}^n(a) + \ldots + q_k A_{n-k}^n(a) = 0,$$

et : $$D^n(a) = 0.$$

Réciproquement, si, pour $n \geqslant n_0$, $D^n(a) = 0$, on voit, en appliquant la relation (S) :

$$D_0^{n+1} D_2^{n-1} = D_2^n D_0^n - (D_1^n)^2,$$

que $D_1^n = 0$ pour $n \geqslant n_0$. Supposons qu'on ait montré que, pour $n \geqslant n_0$, et pour $p \leqslant h$, $D_p^n = 0$, alors :

$$D_h^{n+1} D_{h+2}^{n-1} = D_{h+2}^n D_h^n - (D_{h+1}^n)^2,$$

donc $D_{h+1}^n = 0$ pour $n \geqslant n_0$. On voit ainsi que $D_m^n = 0$, pour tout m, et pour $n \geqslant n_0$: par la proposition 5.2.1, f est rationnelle.

5.3. LE THÉORÈME DE BOREL-DWORK

Soit K un corps de nombres, rappelons (cf. 1.8) que les places de K sont les classes de valeurs absolues équivalentes sur K. Les places finies de K sont en bijection avec les idéaux premiers de l'anneau des entiers de K, on notera P(K) l'ensemble de ces idéaux premiers. Si $\mathfrak{P} \in P(K)$, on notera $|x|_{\mathfrak{P}}$ la valeur absolue $\mathfrak{P}$ - adique normalisée associée à $\mathfrak{P}$. Soient p le nombre premier divisant $\mathfrak{P}$ et $\mathbf{C}_p$ le complété de la clôture algébrique de $\mathbf{Q}_p$, on notera $\mathbf{C}_{\mathfrak{P}}$ l'extension de K isomorphe à $\mathbf{C}_p$, munie

de l'unique valeur absolue $|x|_{\mathfrak{P}}$ prolongeant la valeur absolue $\mathfrak{P}$ - adique normalisée de K.

De même, à toute place infinie de K, est associée une valeur absolue $|x|_i$, $1 \leqslant i \leqslant r+s$, qui est la valeur absolue induite par le plongement correspondant de K dans $\mathbf{C}$ muni de la valeur absolue usuelle $|z|^2 = z\bar{z}$. Les valeurs absolues ainsi normalisées de K satisfont la *formule du produit* : cf. théorème 1.8.4.

Nous noterons désormais C un corps valué complet algébriquement clos, extension de K, et dont la valeur absolue induit sur K l'une des valeurs absolues normalisées ci-dessus : C est donc ou bien $\mathbf{C}$, ou bien $\mathbf{C}_{\mathfrak{P}}$.

DÉFINITION 5.3.1. — *Soient* $f(X) = \sum_{n \geqslant 0} a_n X^n$ *une série formelle à coefficients dans* C *et* $R > 0$; *nous dirons que* f *définit une fonction* MÉROMORPHE *dans le disque de centre* O *et de rayon* R, *si, quel que soit* $r < R$, *il existe un polynôme* Q_r *tel que la série* $Q_r f$ *converge pour* $|X| \leqslant r$.

On vérifie aisément que cette définition est équivalente aux définitions usuelles, tant dans le cas complexe que dans le cas p - adique.

THÉORÈME 5.3.2 *(Borel-Dwork)* [31]. — *Soient* K *un corps de nombres et* $f(X) = \sum_{n \geqslant 0} a_n X^n$ *une série formelle à coefficients dans* K. *S'il existe une partie finie* $P_1(K)$ *de* $P(K)$ *telle que :*

(i) *pour tout* $\mathfrak{P} \notin P_1(K)$ *et tout* $n \geqslant 0$, $|a_n|_{\mathfrak{P}} \leqslant 1$;

(ii) *pour chacune des* $r+s$ *places infinies de* K, f *définit dans* $\mathbf{C}$ *une fonction méromorphe dans un disque ouvert de centre* O *et de rayon* R_i, $i = 1, \ldots, r+s$;

(iii) *pour* $\mathfrak{P} \in P_1(K)$, f *définit dans* $\mathbf{C}_{\mathfrak{P}}$ *une fonction méromorphe dans un disque ouvert de centre* O *et de rayon* $R_{\mathfrak{P}}$;

(iv) *le produit* $R = \prod_{i=1}^{r+s} R_i^{N(i)} \times \prod_{\mathfrak{P} \in P_1(K)} R_{\mathfrak{P}}$ *satisfait* $R > 1$,

alors f *est une fraction rationnelle.*

Remarquons d'abord que la proposition 5.1.1 est un corollaire de ce théorème : si f satisfait les hypothèses de 5.1.1, en prenant $K = \mathbf{Q}$, la condition (i) est satisfaite par $P_1(\mathbf{Q}) = \varnothing$, la condition (ii) pour $R_1 = R$, la condition (iii) est vide, et (iv) est satisfaite puisque $R > 1$, donc f est rationnelle.

Le théorème initial de Borel est exactement la généralisation de 5.1.1 obtenue en y remplaçant « ayant dans $\mathbf{C}$ un rayon de convergence strictement supérieur à 1 » par « qui définit dans $\mathbf{C}$ une fonction méromorphe dans un disque de centre O et de rayon $R > 1$ ». C'est visiblement un cas particulier de 5.3.2. La généralisation par Dwork du théorème de Borel consiste donc à remplacer une condition « locale » (portant sur une seule place) par une condition « globale » plus faible (portant sur toutes les places).

LEMME 5.3.3. — *Avec les notations du théorème, et si la condition* (i) *est satisfaite, pour tout* $\mathfrak{P} \in P_1(K)$ *et pour tous* n *et* k, $|D_n^k(a)|_{\mathfrak{P}} \leqslant 1$.

En effet, le sous-anneau de K constitué des x tels que $|x|_{\mathfrak{P}} \leqslant 1$ contient les a_n, donc contient aussi la valeur au point $(a_n, a_{n+1}, \ldots, a_{n+2k})$ de tout polynôme à coefficients entiers, et en particulier $D_n^k(a)$.

Nous allons maintenant majorer la valeur absolue de D_n^k relative à une place pour laquelle f définit une fonction méromorphe dans un disque du corps C correspondant : la majoration obtenue, jointe à la condition (iv) et à la formule du produit, permettra de montrer que, sous les hypothèses du théorème, il existe k tel que pour n assez grand $D_n^k(a) = 0$, et de conclure, par le lemme 5.2.1.

LEMME 5.3.4. — *Soit* $f(X) = \sum_{n \geqslant 0} a_n X^n$ *une série entière à coefficients dans* C, *définissant une fonction méromorphe dans le disque ouvert de centre* O *et de rayon* R. *Soient* $r < R$ *et* Q

un polynôme de degré s tel que Qf converge pour $|X| \leqslant r$, et soit $k \geqslant s$, alors il existe M tel que, pour $n \geqslant 0$:

$$|D_n^k| \leqslant M b^{-ns} r^{-n(k-s)},$$

où b désigne la borne inférieure des $|z|$ lorsque z parcourt les zéros de Q.

PREUVE DU THÉORÈME 5.3.2. — En admettant le lemme ci-dessus, que nous prouverons ensuite, prouvons le théorème. Choisissons des réels r_i, pour $i = 1, \ldots, r+s$ et $r_{\mathfrak{P}}$, $\mathfrak{P} \in P_1(K)$, de telle sorte que $r_i < R_i$, $r_{\mathfrak{P}} < R_{\mathfrak{P}}$, et que le produit $r = \prod r_i^{N(i)} \prod r_{\mathfrak{P}} > 1$. Notons v un indice parcourant $V = \{1, \ldots, r+s\} \cup P_1(K)$. Pour $v \in V$, soit Q_v un polynôme de degré s_v satisfaisant « $Q_v(0) \neq 0$ et fQ_v converge dans C_v pour $|X| \leqslant r_v$ », et soit b_v la borne inférieure des z_v où z parcourt les zéros de Q_v. Notons s la borne supérieure des s_v, alors, pour $k \geqslant s$, il existe des constantes $M_{v,k}$ telles que :

$$\prod_{v \in V} |D_n^k|_v^{N(v)} \leqslant \prod_{v \in V} (M_{v,k} b_v^{-ns_v} r_v^{-n(k-s_v)})^{N(v)},$$

où : $\quad N(v) = 1 \quad$ si $\quad v = \mathfrak{P}$.

Posons $\Delta_v(k) = (b_v^{-s_v} r_v^{-(k-s_v)})^{N(v)}$, et $\Delta(k) = \prod_{v \in V} \Delta_v(k)$, alors $\lim_{k \to \infty} (\Delta(k))^{1/k} = 1/r$, donc on peut choisir k de telle sorte que $\Delta(k) < 1$. Fixons un tel k, et soit $\Delta = \Delta(k)$, alors, en posant $M = \prod_{v \in V} M_{v,k}^{N(v)}$, on a :

$$\prod_{v \in V} |D_n^k|_v^{N(v)} \leqslant \Delta^n M, \quad \text{avec} \quad \Delta < 1.$$

Compte tenu du lemme 5.3.3 et de la formule du produit, $D_n^k(a) \neq 0$ entraîne $M\Delta^n \geqslant 1$; donc, pour n assez grand, $D_n^k(a) = 0$, ce qui prouve le théorème.

PREUVE DU LEMME 5.3.4. — Nous utiliserons l'inégalité de HADAMARD. Soit $D = [a_{ij}]$ un déterminant d'ordre $m+1$, et soit $A_j = (a_{0j}, \ldots, a_{mj}) \in C^{m+1}$. On munit

C^{m+1} de la norme $||X||$, qui au vecteur $X = (X_i)$ associe :

$$||X|| = \operatorname{Max} |X_i| \quad \text{si} \quad C = C_{\mathfrak{P}}$$

et : $\quad ||X|| = (|X_0^2| + \ldots + |X_m^2|)^{1/2} \quad$ si $\quad C = \mathbf{C}$,

alors :

$$|D| \leqslant ||A_0|| \, ||A_1|| \ldots ||A_m|| \qquad (H)$$

Cette inégalité étant triviale lorsque l'un des A_j est nul, il suffit de la prouver pour $||A_j|| = 1$, $j = 0, \ldots, m$. Dans ce cas :

— si $C = C_{\mathfrak{P}}$, les a_{ij} sont tous dans l'anneau de valuation de $C_{\mathfrak{P}}$, donc D aussi, et $|D| \leqslant 1$;

— si $C = \mathbf{C}$ et $D \neq 0$, on vérifie que si $U_0, \ldots, U_m$ est une suite orthonormale construite à partir de A_j par le procédé de Schmidt :

$$D(U_0, \ldots, U_m) = 1 \geqslant D(A_0, \ldots, A_m) = D.$$

Reprenant les hypothèses du lemme, nous noterons $a_n(f)$ la suite des coefficients de f, et $g = Qf$, où :

$$Q(X) = q_0 + \ldots + q_s X^s;$$

nous noterons aussi $A_n^k(f) = (a_n(f), \ldots, a_{n+k}(f)) \in K^{k+1}$. Avec ces notations :

$$D_n^k(a(f)) = D_n^k = \operatorname{Det}(A_n^k(f), A_{n+1}^k(f), \ldots, A_{n+k}^k(f));$$

de plus, pour $k \geqslant s$ et $m \geqslant s$:

$$A_m^k(g) = q_0 A_m^k(f) + q_1 A_{m-1}^k(f) + \ldots + q_s A_{m-s}^k(f).$$

On a donc, pour $k \geqslant s$:

$$D_n^k = \operatorname{Det}(A_n^k(f), \ldots, A_{n+s-1}^k(f), A_{n+s}^k(g), \ldots, A_{n+k}^k(g)).$$

Or f (resp. g) définit une fonction analytique bornée dans le disque $|X| < b$ (resp. $|X| \leqslant r$), de C, et C est algébriquement clos, donc, d'après les inégalités de Cauchy, il existe deux constantes L et L′ telles que, pour $n \geqslant 0$, $|a_n(f)| \leqslant L b^{-n}$ (resp. $|a_n(g)| \leqslant L' r^{-n}$).

On en déduit, pour tous n et k :

$$\|A_n^k(f)\| \leqslant \begin{cases} Lb^{-n}\,\mathrm{Max}\,(1, b^{-k}) & \text{si } C = C_{\mathfrak{P}}, \\ Lb^{-n}(1 + b^{-2} + \ldots + b^{-2k})^{1/2} & \text{si } C = \mathbf{C}, \end{cases}$$

et des inégalités analogues pour $A_n^k(g)$, où b est remplacé par r.

Il existe donc deux constantes L_1 et L_1' telles que, pour tout $n \geqslant 0$ (k fixé) :

$$\|A_n^k(f)\| \leqslant L_1 b^{-n} \quad \text{et} \quad \|A_n^k(g)\| \leqslant L_1' r^{-n}.$$

En appliquant l'inégalité (H) de Hadamard, on en déduit, pour $k \geqslant s$ et $n \geqslant 0$:

$$|D_n^k| \leqslant M b^{-ns} r^{-n(k-s)},$$

avec :

$$M = L_1^s L_1'^{k-s+1} b^{-s(s-1)/2} r^{-(k-s+1)(k-s+2)/2},$$

ce qui prouve le lemme.

Ce théorème a été utilisé par B. Dwork pour montrer la rationalité de la fonction zéta d'une variété algébrique définie sur un corps fini (cf. par exemple [32]). Par diverses réductions, on ramène la démonstration de ce théorème au problème suivant : soit :

$$F(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$$

un polynôme « irréductible », où $k = \mathbf{F}_p$ est le corps à p éléments. Notons k_s l'unique extension de degré s de k, et $N(s)$ le nombre des solutions de l'équation $F = 0$ dans k_s^n, pour lesquelles aucun des X_i n'est nul. On considère la série formelle (à coefficients rationnels) :

$$\zeta_F(T) = \exp\{\sum_{s \geqslant 1} N(s)\, T^s/s\}.$$

Comme $N(s) \leqslant p^{ns}$, on montre aisément que cette série définit dans $\mathbf{C}$ une fonction holomorphe pour $|z| < 1/p^n$. On montre également qu'elle est à coefficients entiers, puis qu'elle définit dans $\mathbf{C}_p$ une fonction méromorphe dans tout disque de $\mathbf{C}_p$. Elle satisfait donc les hypothèses du théorème 5.3.4 avec :

$$K = \mathbf{Q}, \quad P_1(\mathbf{Q}) = P(\mathbf{Q}) - p, \quad R_1 = 1/p^n$$

et R_p arbitrairement choisi de telle sorte que $R_p > p^n$, d'où sa rationalité. La démonstration originale du théorème 5.3.4 se trouve dans [31].

5.4. LE THÉORÈME DE POLYA-F. BERTRANDIAS

Avant de pouvoir énoncer ce théorème, nous devons indiquer quelques propriétés du diamètre transfini.

5.4.1. *Diamètre transfini*

Soient E *un espace métrique,* B *une partie de* E, *pour* $n \geqslant 2$, *on pose :*

$$D_n(B) = Sup\{\prod_{i \neq j} d(x_i, x_j) \mid x = (x_1, \ldots, x_n) \in B^n\},$$

et :

$$d_n(B) = (D_n(B))^{1/n(n-1)}.$$

Alors, $\lim_{n \to \infty} d_n(B)$ *existe, on note* $d(B)$ *cette limite et on l'appelle le* DIAMÈTRE TRANSFINI *de* B.

Remarquons que, si B n'est pas borné, $D_n(B) = +\infty$, on convient dans ce cas que $d(B)$ est infini, mais on s'intéressera désormais à des parties bornées de E.

Si B est borné, soit D(B) son diamètre :

$$D(B) = \mathrm{Sup}\{d(x, y) \mid (x, y) \in B^2\},$$

alors $D_2(B) = D(B)^2$, et il est immédiat que, pour $n \geqslant 2$, $d_n(B) \leqslant D(B)^{2n}$, on a donc $d(B) \leqslant D(B)$.

On remarque d'autre part que si on remplace la distance d par une distance d' proportionnelle :

$$d'(x, y) = r\, d(x, y), \quad r > 0,$$

la quantité $d'_n(B)$ correspondant à d' est $rd_n(B)$: on peut donc, quitte à faire une homothétie sur les distances, supposer que $D(B) \leqslant 1$. Posons :

$$g_n(x_1, \ldots, x_n) = \prod_{i \neq j} d(x_i, x_j) = g_n(x),$$

$$x = (x_1, \ldots, x_n) \in B^n,$$

alors : $g_{n+1}(x_1, \ldots, x_{n+1})^n = h_1 \ldots h_{n+1}$,

où : $h_j = g_n(x^j)$, $x^j = (x_1, \ldots, \check{x}_j, \ldots, x_{n+1}) \in B^n$.

Donc :

$$(D_{n+1}(B))^n \leqslant D_n(B)^{n+1},$$

$$d_{n+1}(B) \leqslant (d_n(B))^{1+1/n} \leqslant d_n(B)\,(D(B))^{1/n}.$$

Si $D(B) < 1$, la suite $d_n(B)$ est décroissante et minorée, donc convergente.

On vérifiera, à titre d'exercice, que, si B est un disque de **C** ou d'un corps valué non archimédien dont le corps résiduel est infini, $d(B)$ est le rayon de B.

Les propriétés ci-dessous sont immédiates :

(i) si $A \subseteq B$, $d(A) \leqslant d(B)$;
(ii) si $A \subseteq B$ et A dense dans B, $d(A) = d(B)$;
(iii) si B est un ensemble fini, $d(B) = 0$;
(iv) si B est un ensemble fini et A borné, $d(A \cup B) = d(A)$.

Dans le cas où l'espace métrique E est un corps valué K, le diamètre transfini admet une définition équivalente à la précédente, et que nous utiliserons.

LEMME 5.4.2. — *Soit* B *une partie bornée du corps valué* K, *on note* $\mathscr{P}_n$ *l'ensemble des polynômes unitaires de degré n à coefficients dans* K, *et :*

$$S_n(B) = Inf\{\underset{a \in B}{Sup}\,(|P(x)|) \mid P \in \mathscr{P}_n\}, \qquad s_n(B) = (S_n(B))^{1/n},$$

alors $s_n(B) \to d(B)$, $n \to \infty$.

Si f est une fonction définie sur B et à valeurs dans K ou **R**, nous noterons $\|f\|_B = \mathrm{Sup}\{|f(x)| \mid x \in B\}$. Donc $S_n(B) = \mathrm{Inf}\{\|P\|_B \mid P \in \mathscr{P}_n\}$. Choisissons :

$$y = (y_1, \ldots, y_n) \in B^n,$$

et soit $P_y(x) = (x - y_1) \ldots (x - y_n)$, alors :

$$g_{n+1}(x, y_1, y_2, \ldots, y_n) = P_y(x)^2\, g_n(y_1, \ldots, y_n).$$

Etant donné $\varepsilon > 0$, on peut choisir y de telle sorte que $g_n(y) \geqslant D_n(B)\,(1 - \varepsilon)$, pour un tel choix de y on a :

$$D_n(B)\,(1 - \varepsilon)\,\|P_y\|_B^2 \leqslant D_{n+1}(B).$$

A tout $\varepsilon > 0$ on peut associer $P_y \in \mathscr{P}_n$ et satisfaisant cette inégalité, d'où $S_n(B) \leqslant (D_{n+1}(B)/D_n(B))^{1/2}$. Or, quand $n \to \infty$, $(D_{n+1}(B)/D_n(B))^{1/n}$ tend vers $d(B)^2$. On a donc $\underline{\lim}\, s_n(B) \leqslant d(B)$.

D'autre part, on remarque que :

$$g_n(x_1, \ldots, x_n) = |V(x_1, \ldots, x_n)|^2,$$

où $V(x_1, \ldots, x_n)$ est le déterminant de Van der Monde associé à $x_1, \ldots, x_n$, $V = [b_{ij}]$, $b_{ij} = x_i^{j-1}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$. Soit $P \in \mathscr{P}_{n-1}$, alors $V(x_1, \ldots, x_n)$ est encore égal au déterminant obtenu en remplaçant, dans la dernière colonne de V, x_i^{n-1} par $P(x_i)$. En développant cette dernière expression de V par rapport aux éléments de la dernière colonne, on voit que $V(x_1, \ldots, x_n) = \sum_i V_i P(x_i)$, où, au signe près, V_i est le déterminant de Van der Monde de $(x_1, \ldots, \check{x}_i, \ldots, x_n)$. Choisissons $x = (x_1, \ldots, x_n)$ de telle sorte que $g_n(x) \geqslant D_n(B)\,(1 - \varepsilon)$, on a :

$$(1 - \varepsilon)\, D_n(B) \leqslant n^2\, \|P\|_B^2\, D_{n-1}(B),$$

quel que soit $P \in \mathscr{P}_{n-1}$. On en déduit, comme plus haut :

$$(S_{n-1}(B))^2 \geqslant D_n(B)/n^2 D_{n-1}(B),$$

et : $$\underline{\lim}\, s_n(B) \geqslant d(B),$$

d'où la proposition.

COROLLAIRE 5.4.3. — *Soient* B *une partie bornée de* K, $d(B)$ *son diamètre transfini,* $\varepsilon > 0$ *et* $r > 1$; *il existe un entier* n *et un polynôme* $P \in \mathscr{P}_n$ *tels que :*

$$B \subseteq \{x \in K \mid |P(x)| \leqslant (d(B) + \varepsilon)^n r\}.$$

En effet, pour n assez grand, $s_n(B) \leqslant d(B) + \varepsilon$, $S_n(B) \leqslant (d(B) + \varepsilon)^n$; en choisissant un tel n, il existe $P \in \mathscr{P}_n$ tel que $||P||_B \leqslant r S_n(B)$.

EXEMPLE 5.4.4. — Supposons K non archimédien et algébriquement clos, la LEMNISCATE $B = B(P, M)$ définie par un polynôme unitaire P de degré $q \geqslant 1$ et une constante M a un diamètre transfini $d(B) = M^{1/q}$. En effet, $||P^k||_B = M^k \geqslant S_{qk}(B)$, donc $d(B) \leqslant M^{1/q}$. D'autre part, si Q est un polynôme unitaire de degré kq, soit :

$$Q = Q_0 + Q_1 P + \ldots + Q_k P^k, \quad \text{où} \quad \deg Q_i < q$$

(cf. 4.8.4), alors :

$$Q_k = 1, \quad \text{et} \quad ||Q||_B \geqslant ||Q||_0 \geqslant ||Q_k||_0 M^k = M^k,$$

donc $S_{nq}(B) = M^k$ et $d(B) = M^{1/q}$.

EXERCICE 5.4.5. — Soient A une partie bornée de K (K non archimédien et algébriquement clos), P un polynôme unitaire de degré $q \geqslant 1$, et $B = P(A) = \{P(x) \mid x \in A\}$. Alors $d(B) = d(A)^q$.

Soit B′ un ouvert de $\mathbf{P}_1(\mathbf{C})$ dont le complémentaire est borné, on notera $H_0(B')$ l'espace des fonctions holomorphes sur B′ nulles à l'infini et continues sur la frontière de B′. Nous traitons au § 5.5 les quelques propriétés des fonctions holomorphes dans **C** sur le complémentaire d'une lemniscate qui nous sont utiles pour la démonstration du théorème ci-dessous.

THÉORÈME 5.4.6 *(Polya-F. Bertrandias)* [30]. — *Soient* K *un corps de nombres,* $f(X) = \sum_{n \geqslant 1} a_n / X^n$ *une série de Laurent à coefficients dans* K. *S'il existe une partie finie* $P_1(K)$ *de* $P(K)$ *telle que :*

(i) *pour* $\mathfrak{P} \notin P_1(K)$ *et* $n \geqslant 1$, $|a_n|_{\mathfrak{P}} \leqslant 1$;

(ii) *pour chacune des* $r + s$ *places infinies de* K, f *définit dans* **C** *une fonction prolongeable dans un domaine connexe* B_i *dont le complémentaire est borné et a un diamètre transfini* d_i;

(iii) *pour* $\mathfrak{P} \in P_1(K)$, f *définit dans* $\mathbf{C}_{\mathfrak{P}}$ *une fonction prolongeable en un élément analytique sur une partie* $B_{\mathfrak{P}}$ *de* $\mathbf{C}_{\mathfrak{P}}$ *dont le complémentaire est une partie bornée de diamètre transfini* $d_{\mathfrak{P}}$;

(iv) *le produit* $d = (\prod_{i=1}^{r+s} d_i^{N(i)}) \times (\prod_{\mathfrak{P} \in P_1(K)} d_{\mathfrak{P}})$ *satisfait* $d < 1$,

alors f *est une fraction rationnelle.*

Remarquons que le théorème de Borel-Dwork est un corollaire de celui-ci, car si $f(X) = \sum_{n \geqslant 0} a_n X^n$ satisfait les hypothèses du théorème de Borel-Dwork, on vérifie très facilement que $g(X) = f(1/X) - a_0$ satisfait les hypothèses de 5.4.6.

Le principe de démonstration est tout à fait analogue à celui utilisé pour le théorème de Borel-Dwork, mais ici nous majorerons les valeurs absolues des déterminants de Kronecker associés à la suite des coefficients a_k, au lieu d'utiliser les déterminants de Hankel. Les remarques suivantes vont permettre de ramener la démonstration du théorème au cas particulier où les domaines B_i et $B_{\mathfrak{P}}$ sont des complémentaires de lemniscate.

(1) Soit $\mathfrak{P} \in P_1(K)$, notons $T_{\mathfrak{P}}$ le complémentaire de $B_{\mathfrak{P}}$, et soit $d'_{\mathfrak{P}} > d_{\mathfrak{P}}$. Il existe un entier n tel que $S_n(T_{\mathfrak{P}}) < d'^n_{\mathfrak{P}}$. Un tel n étant choisi, il existe $P \in \mathscr{P}_n$ tel que $||P||_{T_{\mathfrak{P}}} \leqslant d'^n_{\mathfrak{P}}$. Alors $B'(P, d'^n_{\mathfrak{P}}) \subseteq B'_{\mathfrak{P}}$, et f y définit un élément analytique. On voit donc que, sous l'hypothèse (iii), quel que soit $d'_{\mathfrak{P}} > d_{\mathfrak{P}}$, il existe une lemniscate de diamètre transfini $d'_{\mathfrak{P}}$ dans le complémentaire de laquelle f est prolongeable en un élément analytique.

(2) De même, pour une place finie, quel que soit $d'_i > d_i$, il existe une lemniscate de diamètre transfini d'_i telle que f soit prolongeable en une fonction holomorphe dans le complémentaire de cette lemniscate.

Quitte à remplacer les quantités d_i et $d_{\mathfrak{P}}$ par des nombres strictement supérieurs satisfaisant encore la condition (iv), on peut donc supposer que les domaines B_i et $B_{\mathfrak{P}}$ sont définis par des inégalités polynomiales du type $B_i = \{x \in C \mid |P_i(x)| \geqslant d_i^{dg(P_i)}\}$.

LEMME 5.4.7. — *Soient* C *un corps complet pour une valeur absolue et algébriquement clos (par exemple* $C = \mathbf{C}$ *ou* $C = \mathbf{C}_{\mathfrak{P}}$*) et* $f(X) = \sum_{k \geqslant 1} a_k X^k$, $a_k \in C$. *Soient* $P \in C[X]$, $q = dg\, P \geqslant 1$, $d > 0$, *et* $B'(P, d^q) = B' = \{x \in C \mid |P(x)| \geqslant d^q\}$, *si* f *est prolongeable en une fonction de* $H_0(B')$:

$$\overline{lim}\, |D_1^k|^{2/k^2} \leqslant d.$$

Soit $\Gamma = \{x \in C \mid |P(x)| = d^q\}$, on sait (par 4.8.7 si C est non archimédien et 5.5.3 si $C = \mathbf{C}$) qu'il existe une constante $M(f)$ telle que, pour tout polynôme Q :

$$|a_1(fQ)| \leqslant M(f)\, ||Q||_\Gamma.$$

Soient $P_1, \ldots, P_k$ des polynômes unitaires, $P_k \in \mathscr{P}_{k-1}$. Par définition, $D_1^k = [a_{ij}]$, où $a_{ij} = a_{i+j-1}$, $i = 1, \ldots, k$, $j = 1, \ldots, k$. Par une combinaison linéaire des colonnes de D_1^k, on voit que, si :

$$P_j(X) = X^{j-1} + p_{j1} X^{j-2} + \ldots + p_{j,j-1},$$

et :
$$P_j f = \sum_{k > -j} b_{kj} X^k,$$

on a aussi $D_1^k = [b_{ij}]$, $i = 1, \ldots, k$, $j = 1, \ldots, k$. En faisant une combinaison analogue sur les lignes de D_1^k, on voit que $D_1^k = [a_1(P_i P_j f)]$, $i = 1, \ldots, k$, $j = 1, \ldots, k$. Posons $p_i = ||P_i||_\Gamma$, il existe une constante $M(f)$ telle que $|a_1(P_i P_j f)| \leqslant M(f)\, p_i p_j$.

Posons $S_k = \mathrm{Max}\,(p_1, \ldots, p_k)$ si C est non archimédien et $S_k = (p_1^2 + \ldots + p_k^2)^{1/2}$ si $C = \mathbf{C}$. En appliquant l'inégalité de Hadamard, on obtient :

$$|D_1^k(f)| \leqslant M(f)^k\, p_1 \ldots p_k (S_k)^k.$$

Choisissons $P_1, \ldots, P_k$ de telle sorte que $p_k \leqslant (d + \varepsilon)^k$, pour k assez grand (ce qui est possible, cf. 5.4.3). Supposons d'abord $d < 1$, et notons L une constante (qui peut ne pas être la même d'une inégalité à la suivante); alors, en choisissant ε assez petit pour que $d + \varepsilon < 1$, on a :

$$S_k \leqslant kL, \quad p_1 \ldots p_k \leqslant L(d + \varepsilon)^{k(k-1)/2},$$

d'où :

$$2/k^2 \,\mathrm{Log}\, |D_1^k(f)| \leqslant L/k + \mathrm{Log}\,(d + \varepsilon) + (\mathrm{Log}\, k)/k + L.$$

Lorsque $k \to +\infty$, on en déduit $\overline{\lim}\, |D_1^k|^{2/k^2} \leqslant d + \varepsilon$. Si $d < 1$, le lemme est démontré. Or, soit $\lambda \in K$, et soit $f_\lambda(X) = f(\lambda X)$, f_λ est prolongeable en un élément de $H_0\left(\frac{1}{\lambda} B'\right)$, où $\frac{1}{\lambda} B'$ est l'image de B' dans l'homothétie de centre O et de rapport $1/\lambda$. Il est clair que :

$$D_1^k(f_\lambda) = \lambda^{-k^2} D_1^k(f) \quad \text{et} \quad d\left(\frac{1}{\lambda} B'\right) = \frac{1}{|\lambda|}\, d$$

on en déduit que si le lemme est vrai pour $d < 1$, il est vrai pour tout $d > 0$.

PREUVE DU THÉORÈME 5.4.6. — Pour $x \in K$, notons $||x|| = \prod_{i=1}^{r+s} |x|_i^{N(i)} \times \prod_{\mathfrak{P} \in P(K)} |x|_{\mathfrak{P}}$, le produit de toutes les valeurs absolues normalisées de x. Soit d le produit des diamètres transfinis figurant dans la condition (iv). Soit $\mathfrak{P} \notin P_1(K)$, alors $|D_1^k(f)|_{\mathfrak{P}} \leqslant 1$. Soit :

$$N = r + 2s + \mathrm{Card}\,(P_1(K)),$$

choisissons $\varepsilon > 0$ de telle sorte que $d(1 + \varepsilon)^N < 1$. Il existe des entiers k_i et $k_{\mathfrak{P}}$ ($i = 1, \ldots, r + s$, $\mathfrak{P} \in P_1(K)$) tels que, pour $k \geqslant k_i$ (resp. $k \geqslant k_{\mathfrak{P}}$), on ait :

$$|D_1^k(f)|_i \leqslant (d_i(1 + \varepsilon))^{k^2}$$

(resp. $|D_1^k(f)|_{\mathfrak{P}} \leqslant (d_{\mathfrak{P}}(1+\varepsilon))^{k^2}$). Soit K le maximum des k_i et $k_{\mathfrak{P}}$, alors, pour $k \geqslant K$:

$$\|D_1^k(f)\| \leqslant (d(1+\varepsilon)^N)^{k^2} < 1.$$

Donc, pour un tel k, $D_1^k(f) = 0$, et, d'après le corollaire 5.2.3, f est rationnelle.

REMARQUES. — Les deux critères de rationalité que nous avons prouvés donnent des conditions suffisantes pour qu'une série (formelle) soit rationnelle. Ces conditions sont aussi nécessaires puisque, d'une part, une fraction rationnelle n'ayant qu'un nombre fini de pôles, elle définit une fonction méromorphe dans tout disque, et un élément analytique dans le complémentaire de tout fermé ayant ses pôles comme points intérieurs (on trouve de tels fermés de diamètre transfini aussi petit que l'on veut); d'autre part, les seuls idéaux premiers $\mathfrak{P}$ pour lesquels il existe des indices n tels que $|a_n|_{\mathfrak{P}} > 1$ sont ceux auxquels appartient le terme constant (resp. le coefficient du terme de plus haut degré) d'un polynôme Q tel que $f = P/Q$, P et Q étant à coefficients dans l'anneau des entiers de K : il n'y a qu'un nombre fini de tels $\mathfrak{P}$, et les conditions (i) des deux théorèmes sont satisfaites si f est rationnelle.

EXERCICE 5.4.8. — Soient p un nombre premier et :

$$f(X) = \sum_{k \geqslant 0} p^k X^{p^k}, \quad g(X) = f(1/X) - 1.$$

(i) Déterminer les rayons de convergence de f dans $\mathbf{C}$, $\mathbf{C}_p$, $\mathbf{C}_{p'}$, $p' \neq p$.

(ii) En calculant les déterminants $D_n^j(f)$ pour n et j bien choisis, montrer que f n'est pas rationnelle.

(iii) Soit $D = \{x \in \mathbf{C} \mid |x| < 1\}$, on admettra que si Ω est un ouvert contenant strictement D, $d(\Omega) > 1$; en déduire que f n'est prolongeable dans aucun ouvert Ω', connexe, et contenant strictement D.

(iv) Montrer que, dans $\mathbf{C}_p$, il n'existe aucune lemniscate de diamètre transfini strictement inférieur à 1, telle que g soit prolongeable en un élément analytique sur le complémentaire de cette lemniscate.

(v) Soit $f(X) = \sum_{n \geqslant 0} a_n X^n$, on dit que f est lacunaire si, quel que soit $k > 0$, il existe n tel que $a_n = a_{n+1} = \ldots = a_{n+k} = 0$. Montrer qu'une telle série n'est pas rationnelle.

(vi) Soit f une série lacunaire à coefficients entiers, montrer que, s'il existe un nombre premier p tel que le rayon de convergence de f dans $\mathbf{C}_p$ soit strictement supérieur à 1, le rayon de convergence de f dans $\mathbf{C}$ est strictement inférieur à 1.

5.5. LEMNISCATES DANS LE PLAN COMPLEXE

Soit $P \in \mathbf{C}[X]$ un polynôme unitaire de degré $q \geqslant 1$, $M > 0$, on note :

$$B(P, M) = \{z \in \mathbf{C} \mid |P(z)| \leqslant M\},$$
$$B^0(P, M) = \{z \in \mathbf{C} \mid |P(z)| < M\},$$
$$B'(P, M) = \{z \in \mathbf{C} \mid |P(z)| \geqslant M\}$$

et : $$C(P, M) = B(P, M) \cap B'(P, M);$$

si aucune confusion n'est possible on abrégera ces notations en B, B^0, B′ et C.

PROPOSITION 5.5.1. — *La lemniscate* $B^0(P, M)$ *a au plus* q *composantes connexes* $B_1^0, \ldots, B_h^0$, $h \leqslant q$, *chaque* B_i^0 *contient un zéro de* P *et est simplement connexe. La frontière* C_i *de* B_i^0 *est une courbe fermée simple,* $C = C_1 \cup \ldots \cup C_h$.

Montrons que toute composante connexe de B^0 contient un zéro de P : leur nombre est alors majoré par q. Si D est une composante connexe de B^0, soit Γ un cercle contenu dans D : d'après le principe du maximum, si I(Γ) est l'intérieur de Γ, on a :

$$\operatorname{Max}\{|P(z)| \mid z \in I(\Gamma)\} = \operatorname{Max}\{|P(z)| \mid z \in \Gamma\} \leqslant M,$$

donc $I(\Gamma) \subset D$, et D est simplement connexe. Soit F(D) la frontière de D : pour $z \in F(D)$, $|P(z)| \leqslant M$ (par continuité), mais, s'il existe $z \in F(D)$ tel que $|P(z)| < M$, il existe un voisinage de z contenu dans B^0; soit V un tel voisinage de z, alors $V \cup D \neq D \subseteq B^0$, et D n'est pas une partie connexe maximale de B^0. Donc $|P(z)| = M$ pour tout $z \in F(D)$. Enfin P a au moins un zéro dans D, sinon $1/P$ serait holomorphe dans tout voisinage fermé

assez petit de D : soit D' un tel voisinage, alors, d'après le principe du maximum, pour $z \in D$:

$$1/M \leqslant |1/P(z)| \leqslant \mathrm{Max}\{|1/P(t)| \; t \in F(D)\} = 1/M;$$

alors P serait constant sur D, ce qui est impossible. Soient donc $B_1^0, \ldots, B_h^0$, $h \leqslant q$, les composantes connexes. Pour j fixé, choisissons un zéro b de P dans B_j^0, notons, pour $\theta \in \mathbf{R}$, $f_\theta(r) = P(b + re^{i\theta})$, et $r(\theta)$ la borne supérieure des $r' > 0$ tels que $|f_\theta(r'')| \leqslant M$ pour $0 \leqslant r'' \leqslant r'$. Il est clair que $r(\theta)$ est une fonction continue de θ et que $\theta \to r(\theta)$, $\theta \in [0, 2\pi]$ est un paramétrage de la frontière C_j de B_j^0 : C_j est donc une courbe fermée simple.

Nous noterons $\vec{C}_j$ la courbe orientée dans le sens positif du plan associée à C_j (*i.e.* l'orientation est telle que, pour $b \in B_j^0$, $n(b, \vec{C}_j) = 1/2i\pi \int_{\vec{\partial}_j} dz/z - b = +1$) et $\vec{C} = \vec{C}_1 + \ldots + \vec{C}_h$.

LEMME 5.5.2. — *Soit* $f(z) = \sum_{k \geqslant k_0} a_k/z^k$ *une série de Laurent définissant une fonction holomorphe dans* $B' - \{\infty\}$, *alors :*

$$a_1 = \frac{1}{2i\pi} \int_{\vec{\partial}} f(z)\, dz.$$

Soit en effet Γ un cercle orienté dans le sens positif du plan et contenant B dans son intérieur $I(\Gamma)$. Alors f est holomorphe dans le domaine borné $B' \cap I(\Gamma)$ et continue au bord : il en résulte aisément que :

$$\int_{\vec{\Gamma} - \vec{\partial}} f(z)\, dz = 0.$$

Choisissons $\vec{\Gamma}$ de telle sorte que, pour $z \in \Gamma$, $|a_k|\,|z|^k$ soit sommable. Pour $k \neq 1$:

$$\int_{\vec{\Gamma}} dz/z^k = 0, \quad \text{et} \quad \int_{\vec{\Gamma}} dz/z = 2i\pi.$$

Donc $\int_{\vec{\Gamma}} f(z)\, dz = 2i\pi a_1 = \int_{\vec{\partial}} f(z)\, dz$, d'où le lemme.

COROLLAIRE 5.5.3. — *Soit f une fonction analytique sur B' et nulle à l'infini, il existe une constante $M(f)$ telle que, pour tout polynôme Q, $|a_1(Qf)| \leqslant M(f)\, ||Q||_0$.*

En effet, d'après 5.5.2, $a_1(Qf) = 1/2i\pi \int_{\vec{\partial}} Q(z) f(z)\, dz$. Soit L la longueur de C, on a, d'après l'inégalité de Cauchy :

$$|a_1(Qf)| \leqslant L/2\pi\, ||Q||_0\, ||f||_0 = M(f)\, ||Q||_0.$$

EXERCICE 5.5.4. — 1. Déterminer le nombre de composantes connexes de la lemniscate $B^0(P, M)$, où $P(z) = z^2 - 1$ en fonction de M.

2. Soient plus généralement P un polynôme unitaire de degré $q \geqslant 1$ et $h(P, M)$ le nombre des composantes connexes de $B^0(P, M)$. Montrer que la fonction $M \to h(P, M)$ est non croissante, que $\lim_{M \to +\infty} h(P, M) = 1$, que h est continue par intervalles, et que les valeurs M_i où elle n'est pas continue sont les modules des zéros du polynôme $Q(y)$ numérateur du discriminant de $P(X) - y$.

BIBLIOGRAPHIE

OUVRAGES DE RÉFÉRENCE

[1] BACHMAN (G.), *Introduction to p - adic numbers and valuation theory*, New York-London, 1964.

[2] BOREVITCH (Z. I.) et CHAFAREVITCH (I. R.), *Théorie des nombres*, Paris, 1967.

[3] BRUHAT (F.), *Lectures on some aspects of p - adic analysis*, Bombay, 1963.

[4] HASSE (H.), *Zahlen-theorie*, Berlin, 1969.

[5] HENSEL (Kurt), *Zahlentheorie*, Berlin, 1913.

[6] LANG (Serge), *Algebraic Number Theory*, New York, 1970.

[7] SAMUEL (Pierre), *Théorie algébrique des nombres*, Paris, 1967.

[8] SERRE (Jean-Pierre), *Corps locaux*, Paris, Hermann, 1962.

[9] SERRE (Jean-Pierre), *Cours d'arithmétique*, Paris, P.U.F., 1970.

[10] WEIL (André), *Basic Number Theory*, Berlin, Springer-Verlag, 1967.

ARTICLES ET AUTRES OUVRAGES

I. — *Espaces de Banach et espaces de fonctions continues*

[11] AMICE (Yvette), Interpolation p - adique, *Bull. Soc. Math. France*, 92 (1964), p. 117-180.

[12] CARPENTIER (Jean-Pierre), Semi-normes et ensembles convexes dans un espace vectoriel sur un corps valué ultramétrique, *Sem. Choquet*, Paris, 1964-1965.

[13] GRUSON (Laurent), Catégories d'espaces de Banach ultramétriques, *Bull. Soc. Math. France*, 94 (1966), p. 287-299.

[14] MAHLER (Kurt), *Introduction to p - adic numbers and their functions*, Cambridge, 1973.

[15] MONNA (A. F.), *Analyse non archimédienne*, Berlin, Springer-Verlag, 1970,

[16] PUT (Marius van der), Algèbres de fonctions continues p - adiques. *Proc. Kon. Ned. Akad. v. Wetensch.*, A 71 (1968), p. 401-420.

[17] PUT (Marius van der), Espaces de Banach non archimédiens, *Bull. Soc. Math. France*, 97 (1969), p. 309-320.

[18] SERRE (Jean-Pierre), Endomorphismes complètement continus des espaces de Banach p - adiques, *Publ. Math. I.H.E.S.*, n° 12, Paris, 1962, p. 69-85.

II. — *Théorie classique des fonctions analytiques*

[19] Lazard (Michel), Les zéros d'une fonction analytique d'une variable sur un corps valué complet, *Publ. Math. I.H.E.S.*, nº 14.
[20] Schnirelman (L.), Sur les fonctions dans les corps normés et algébriquement fermés, *Izvestia Akad. Nauk S.S.S.R.*, Ser. Math., 2, p. 487-498 (en russe).
[21] Schöbe (W.), *Beitrage zur Funktionenetheorie in nichtarchimedisch bewerteten Körpern*, thèse Sc. Math., Univ. Münster, 1930.

III. — *Prolongement analytique*

[22] Durix (Marie-Claude), Prolongement multiforme des fonctions analytiques dans les corps valués non archimédiens, *Sem. Delange-Pisot-Poitou*, nº 20, Paris, 1966-1967.
[23] Escassut (Alain), *Algèbres de Banach d'éléments analytiques au sens de Krasner*, thèse 3e cycle, Bordeaux, 1970.
[24] Escassut (Alain), Algèbres de Banach ultramétriques et algèbres de Krasner-Tate, *Astérisque*, nº 10 (1973), p. 1-107 (Paris, Soc. Math. Fr.).
[25] Krasner (Marc), Prolongement analytique uniforme et multiforme, *Colloque C.N.R.S. nº 143, Clermont-Ferrand, 1963*, Paris, Ed. C.N.R.S., 1966, p. 97-141.
[26] Robba (Philippe), Prolongement analytique pour les fonctions de plusieurs variables sur un corps valué complet, *Bull. Soc. Math. France*, 101 (1973), p. 193-217.
[27] Robba (Philippe), Fonctions analytiques sur les corps valués ultramétriques complets, *Astérisque*, nº 10 (1973), p. 109-218 (Paris, Soc. Math. Fr.).
[28] Tate (John), Rigid analytic spaces, *Inventiones Math.*, 1971, p. 257-289.

IV. — *Fonctions spéciales, rationalité*

[29] Amice (Yvette) et Fresnel (Jean), Fonctions zéta p - adiques des corps de nombres abéliens réels, *Acta Arith.*, XX (1972), p. 353-384.
[30] Bertrandias (Françoise), Diamètre transfini dans un corps valué, application au prolongement analytique, *Sem. Delange-Pisot*, nº 3, Paris, 1963-1964.
[31] Dwork (Bernard), On the rationality of the zeta function of an algebraic variety, *Amer. J. of Math.*, 82 (1960), p. 631-648.
[32] Dwork (Bernard), On the zeta function of a hypersurface, *Publ. Math. I.H.E.S.*, nº 12, 1962.
[33] Dwork (Bernard), On the rationality of zeta functions and L series, *Proc. Conf. on local fields*, Driebergen, 1966, p. 40-55.
[34] Fresnel (Jean), Nombres de Bernoulli et fonctions L p - adiques, *Ann. Inst. Fourier, Grenoble*, 17 (1967), p. 281-333.

[35] Iwasawa (Kenkichi), *Lectures on p - adic L-functions*, Princeton, 1972.
[36] Kubota (T.) und Leopoldt (H. W.), Eine p - adische Theorie der Zetawerte, *Jour. für die reine u. angewandte Math.*, Bd 214-215 (1964), p. 328-339.
[37] Mahler (Kurt), Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, *Proc. Ned. Akad. v. Wetensch.*, A 38 (1935), p. 50-60.
[38] Pisot (Charles), Familles compactes de fractions rationnelles et ensembles fermés de nombres algébriques, *Ann. Sc. Ec. Normale Sup.*, 3e série, t. 81, 1964, p. 165-188.
[39] Roquette (Peter), *Analytic theory of elliptic functions over local fields*, Göttingen, 1970.
[40] Serre (Jean-Pierre), Formes modulaires et fonctions zéta p - adiques, *Modular functions of one variable*, Summer School Antwerp, 1972, III, Berlin, 1973, p. 191-268.

On trouvera aussi une série d'articles sur l'analyse p - adique dans :

[41] *Table ronde du C.N.R.S. sur l'analyse non archimédienne*, Paris, 1972, Mémoires Soc. Math. France.

INDEX TERMINOLOGIQUE

1975. — Imprimerie des Presses Universitaires de France. — Vendôme (France)
ÉDIT. N° 33 528 IMPRIMÉ EN FRANCE IMP. N° 24 705